Теория групп: примеры и задачи

А.И. Корчагин

В литературе и Интернете на фоне изобилия теоретического материала практически отсутствуют систематизированные учебники по практической составляющей теории групп, где бы разбирались решения типовых и классических задач по всем основным входящим в стандартную программу темам. И в данном пособии я сделал попытку восполнить этот пробел: в нем собраны решения ключевых задач теории групп - от элементарных до достаточно сложных, требующих нетривиального подхода.

Первая часть книги строится вокруг практической части курса теории групп МФТИ. Ее основу составляет разбор типовых и классических задач, но помимо этого включены краткие теоретические комментарии и задачи повышенной сложности, способствующие более глубокому пониманию предмета.

Вторая часть посвящена более сложным темам, выходящим за рамки стандартной программы. Я считаю эти темы крайне важными для всех математиков, чьи исследования прямо или косвенно связаны с теорией групп. Из-за того, что эти темы не покрываются стандартной программы и в силу их повышенной наукоемкости - большой акцент сделан на теорию, и практических задач там существенно меньше чем в первой части.

По моему глубокому убеждению математики должны мыслить конкретными примерами - а потому на них в этом пособии сделан основной акцент. Кроме того, изложение сопровождается подробными и обширными комментариями, которые, по моему мнению, помогут взглянуть на теорию групп с разных сторон и заметно упрощают восприятие. Также рекомендую последовательное изучение материала, поскольку часто по ходу изложения будут отсылки к более ранним сюжетам. Математика - это не прогулка в парке, и преодоление трудностей остается неотъемлемой частью научного роста, и это пособие призвано сделать более осознанным и интересным путь к покорению новых вершин в теории групп.

Оглавление

Часть I

Часть II

Общие связанные с группами вопросы

Группой называется множество G с введенной на нем ассоциативной операцией, допускающей обратный и нейтральный элемент. Обычно эту операцию обозначают $a \cdot b$ или просто ab. Если $ab = ba$ для любых a, b - то группу называют абелевой. В абелевой группе иногда операцию обозначают $a + b$ дабы подчеркнуть абелевость. Существует много других алгебраических структур: поле, кольцо, векторные пространства, моноиды, группоиды - но группы занимают центральное место в этой иерархии, так как с одной стороны они не очень абстрактны, что обеспечивает богатый инструментарий, но при этом и не очень специальны, что обеспечивает им богатое разнообразие (скажем, тех же линейных пространств очень мало (к примеру с точностью до изоморфизма над конкретным полем существует всего одно n-мерное линейное пространство), но у них много хороших свойств (даже слишком хороших), тогда как моноидов слишком много, но свойства для них верны только самые общие: и группы в некотором смысле являются золотой серединкой). Сразу хочется сказать, что в отличие от линала, где все линейные пространства в некотором смысле сильно похожи друг на друга - группы более разнообразны и многогранны, среди них выделяются разные классы групп с принципиально различающимися свойствами а также методами работы с ними - а потому здесь будет меньше алгоритмов и больше творчества; и чтобы освоить этот предмет - нужно много размышлять, решать задачи, заходить на сайт mathoverflow (или же mathstackexchange) и разбирать научные статьи - и обдумывать и записывать в тетрадочку пóтом добытые добытые там приемы - и чтобы в конечном счете начать "чувствовать" группы. Это очень красивая наука, я понял это после того, как закончил университет, надеюсь, вы поймете раньше. Также теория групп богата на приложения, причем не только в других областях математики, но и в химии, теоретической физике, криптографии и в других науках.

Базовые примеры групп, с которых мы начнем наше обучение - следующие (они зачастую будут выступать в роли тестовых, которыми мы будем иллюстрировать новые понятия):

$$\boxed{\mathbb{Z}, \mathbb{Z}_n, GL_n(F), SL_n(F), S_n, S(X)}$$

Здесь и далее $GL_n(F)$ и $SL_n(F)$ это соответственно множество обратимых матриц и матриц, с определителем равным единица, в этих примерах F - поле, хотя из формулы для обратной матрицы вытекает, что $SL_n(F)$ является группой даже когда F просто кольцо. На $\mathbb{Z}$ и $\mathbb{Z}_n$ групповая операция это сложение (и сложение по модулю n), на матрицах - матричное умножение, а на перестановках - операция композиции. Что касается списка множеств с операциями, которые не являются группами - то стоит отметить:

$$(\mathbb{N}, +), (\mathbb{R}, \cdot), (GL_n(\mathbb{Z}), \cdot)$$

здесь $(\mathbb{N}, +)$ не является группой как минимум потому, что нет нейтрального элемента; в $(\mathbb{R}, \cdot)$ нейтральный есть $(=1)$, но у 0 нет обратного (но при этом $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ с операцией умножения уже является группой). И наконец $(GL_n(\mathbb{Z}), \cdot)$ не является группой, так как опять-таки не у каждого элемента есть обратный (у обратной матрицы могут быть нецелочисленные коэффициенты).

Первая группа задач - на работу с элементарными соотношениями, которые обычно решаются игрой с соотношениями до тех пор, пока задача не решится, причем с опытом стремительно растет скорость решения подобных задач. В последующих темах мы с вами изучим группы, заданные копредставлениями, и эта техника очень пригодится.

Утверждение

Доказать, что в группе существует единственный нейтральный и единственный обратный элемент.

Делается это с помощью стандартного приема, который все должны знать: пусть у группы есть два нейтральных e_1 и e_2, и два обратных b, c к a. Тогда:

$$e_1 = e_1 e_2 = e_2$$

$$b = b(ac) = (ba)c = c$$

Задача

Доказать, что если для элементов $a, b \in G$ некоторой группы выполнены соотношения

$$a^5 = b^3 = 1 \qquad\qquad b^{-1}ab = a^2$$

то $a = 1$.

Сопряжение уважает степени: $(x^{-1}yx)^n = x^{-1}y^n x$, что легко проверяется: $(x^{-1}yx)^n = (x^{-1}yx)(x^{-1}yx)\dots(x^{-1}yx) = x^{-1}y^n x$, так как все промежуточные xx^{-1} сокращаются.

А потому имеем:

$$a = b^{-3}ab^3 = b^{-2}(b^{-1}ab)b^2 = b^{-2}a^2b^2 = b^{-1}(b^{-1}ab)^2 b = b^{-1}a^4 b = a^8$$

Значит

$$a^7 = 1 \qquad\qquad a^5 = 1$$

А значит для любых целых чисел n, m имеем $a^{5m+7n} = 1$. Так как наибольший общий делитель 5 и 7 равен 1, то из теоремы о линейном представлении наибольшего общего делителя найдутся целые m и n, что $5m+7n = 1$, а потому получаем $a = 1$. Для таких маленьких чисел можно найти конкретное представление: $a = a^1 = a^{5\cdot 3-7\cdot 2} = 1$.

Задача

Доказать, что если $g^2 = 1$ для любого $g \in G$, то группа G абелева.

Два элемента коммутируют тогда и только тогда когда коммутатор тривиален:

$$ab = ba \qquad \Longleftrightarrow \qquad [a, b] := aba^{-1}b^{-1} = 1$$

В некоторых задачах удобно проверять само условие коммутирования, а в некоторых пользоваться коммутатором: в принципе, подходы эквивалентны, но один из них обычно оказывается проще как технически, так и для восприятия. В этой задаче воспользуемся помощью коммутатора:

$$[a, b] = aba^{-1}b^{-1} = abab = (ab)^2 = 1$$

так как если $g^2 = 1$ для любого g, тогда $g = g^{-1}$.

Замечание:

Не забывайте, что в неабелевой группе нужно быть очень аккуратным с соотношениями. На первых порах после чисто коммутативной линейной алгебры хочется писать что-то вроде $(ab)^2 = a^2b^2$, но так нельзя.

Задача

Описать все группы G, такие что $|G| = 3$.

Группа - это множество с операцией (или правильнее сказать операциями, так как взятие обратного элемента - это тоже операция). А потому группа полностью определяется своей таблицей умножения (взятие обратного тоже зашито в этой таблице, так как оно определяется местами, где стоит нейтральный элемент: на пересечении x-строки и y-столбца стоит элемент xy, если он равен e, то $y = x^{-1}$). Кроме нейтрального элемента e в группе есть еще два, которые мы назовем a и b.

	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

Умножение слева на любой элемент группы - это биекция; а потому в каждой строчке должны присутствовать все элементы группы в некотором порядке.

Подумаем, чему может быть равно ab.

• Случай $ab = a$ отпадает, иначе умножая это равенство слева на a^{-1} получим $b = e$.

• Случай $ab = b$ тоже отпадает, так как умножая уже на b^{-1} и справа получим $a = e$

Поэтому $ab = e$, а значит $a^{-1} = b$, откуда $ba = e$. Оставшиеся две клеточки заполняются автоматически из наблюдения, что в каждой строчке и в каждом столбце таблицы умножения должны быть представлены все элементы группы. Таким образом таблица умножения имеет вид:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Замечания:

Советую потренироваться, стартовав с анализа значения a^2 вместо ab - подумайте, как отсеивание происходит в этом случае. Полученная нами группа изоморфна $\mathbb{Z}_3$. С теоремой Лагранжа задача существенно упрощается, но полезно уметь решать ее без этой мощной теоремы, чтобы лучше прочувствовать групповое умножение. Отмечу, что хотя трехэлементных множеств, с заданными на них бинарными операциями вообще без каких либо свойств, сказочно много: 3^9, аксиомам групп удовлетворяет лишь одна таблица умножения, как мы только что убедились.

• **Домашнее задание**: описать в лоб (т.е. без теоремы Лагранжа и "более поздних" теорем) все группы из 4 элементов.

Порядок элемента

Порядок элемента - самая важная и вместе с тем самая простая характеристика элемента группы (думайте о нем как о своего рода следе или определителе), которая позволяет очень многое сказать как о свойствах этого элемента, так и о структуре всей группы в целом, если понять элементы каких порядков в ней существуют (количество элементов заданного порядка чуть ли не самый мощный инструмент для проверки на изоморфность конечных групп малого порядка, к примеру если в группе A существует всего 3 элемента порядка 4, а в группе B их 5, то группы неизоморфны. Даже множество допустимых порядков элементов очень многое скажет вам о группе).

Определение

Порядком $\mathrm{ord}(x)$ *элемента* $x \in G$ *называется минимальное число* n *(∞, если такого числа нет), что* $g^n = 1$ *(иногда нейтральный элемент группы я буду обозначать* 1*, иногда* e*).*

Замечание:

Не путайте порядок элемента с порядком группы, который общепризнано определяется как мощность группы. Такое совпадение терминологий почти никогда не приводит к недоразумениям или неясностям, но все равно остается осадочек.

Основные свойства порядка:

• $\mathrm{ord}(x) = \mathrm{ord}(y^{-1}xy)$ - доказательство очень простое: достаточно заметить, что операция сопряжения "уважает" произведение (с этим вы часто на линале сталкивались), т.е.

$$(y^{-1}xy)^n = y^{-1}xyy^{-1}xy\dots y^{-1}xy = y^{-1}x^ny$$

Таким образом $(y^{-1}xy)^n = 1$ iff $y^{-1}x^ny = 1$ iff $x^n = 1$. Ясно, что если $y^{-1}x^ny = 1$, то после домножения слева на y и справа на y^{-1} мы получим, что $x^n = 1$ и обратно. Свойство это естественно: при операции сопряжение структура элемента не меняется и, выражаясь терминами линала, он просто рассматривается "в другом базисе".

• $\mathrm{ord}(xy) = \mathrm{ord}(yx)$ - очевидно вытекает из первого, т.к. $yx = y(xy)y^{-1}$.

• $n = \mathrm{ord}(a)$, тогда $a^k = 1 \iff k$ делится на n.

$\Leftarrow$ Если $k = nm$, то $a^k = (a^n)^m = 1$.

$\Rightarrow$ Алгоритм Евклида (он же делением столбиком). Поделим с остатком $k = mn + r$. Тогда $a^k = (a^n)^m a^r$, а значит $a^r = 1$, а значит n не минимальная степень.

Это свойство позволяет вычислять порядки элементов в

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$$

(эту группу довольно часто удобнее записывать в мультипликативной форме $\mathbb{Z}_n = \{1, a, a^2, \dots, a^{n-1}\}$ и $a^n = 1$, при перемножении таких элементов степени складываются по модулю n, изоморфизм между аддитивной и мультипликативной формой задается $k \leftrightarrow a^k$). Здесь мы будем использовать мультипликативную запись, и найдем $\mathrm{ord}(a^k)$ в $\mathbb{Z}_n$. По определению, это минимальный m, что $a^{km} = 1$. По свойству получаем, что это выполняется iff km делится на n. Из основных теоретико-числовых теорем вытекает, что минимальный m с таким условием равен $m = \frac{n}{(n,k)}$ (минимальность m фактически означает минимальность km, т.е. иными словами нам нужно найти минимальное число, которое делится и на n и на k - а это НОК, из теории чисел вытекает, что $mk = \mathrm{НОК}(n,k) = \frac{nk}{(n,k)}$). Значит:

$$\mathrm{ord}(a^k) = \frac{n}{(n,k)}$$

Задача

Пусть $[a,b] = 1$. Доказать, что НОК$(\mathrm{ord}(a), \mathrm{ord}(b))$ делится на $\mathrm{ord}(ab)$.

Пусть $N = \mathrm{НОК}(\mathrm{ord}(a), \mathrm{ord}(b))$. Так как a, b коммутируют, то $(ab)^N = a^N b^N = 1$. Из третьего свойства вытекает, что N делится на $\mathrm{ord}(ab)$.

Замечание:

• *Если a, b - суперкоммутирующие элементы, тогда можно поставить равенство $\mathrm{ord}(ab) = НОК(\mathrm{ord}(a), \mathrm{ord}(b))$. Например, это верно в случае, когда a, b независимые циклы, или когда $a = (g, 1), b = (1, h) \in G \times H$, т.е. в случаях, когда не только они коммутируют, но и когда из $a^n b^m = 1 \;\Rightarrow\; a^n = 1$ и $b^m = 1$.*

В общем случае равенство не всегда достигается, например, в случае $b = a^{-1}$. Здесь $\mathrm{ord}(ab) = 1$, но при этом НОК$(\mathrm{ord}(a), \mathrm{ord}(b)) = \mathrm{ord}(a)$

• *Если a, b некоммутирующие, то не только делимости может не быть, но и порядок произведения может быть бесконечным. Примеры нужно искать среди*

бесконечных групп, где они встречаются очень часто и в некотором смысле даже скорее типичны чем аномальны.

Построим два примера, когда $\mathrm{ord}(a) = \mathrm{ord}(b) = 2$, *но при этом* $\mathrm{ord}(ab) = \infty$.

1) *Аналитический пример*

Рассмотрим $a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $b = M^{-1}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}M$ *в любой матричной группе (групповая операция = умножение матриц). Если* $[a, M] = 1$, *то примера построить не получится, т.к. тогда* $[a, b] = 1$ *и мы находимся в условии задачи. Но если взять некоммутирующую с* a *матрицу, например* $M = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$, *то в этом случае получим*

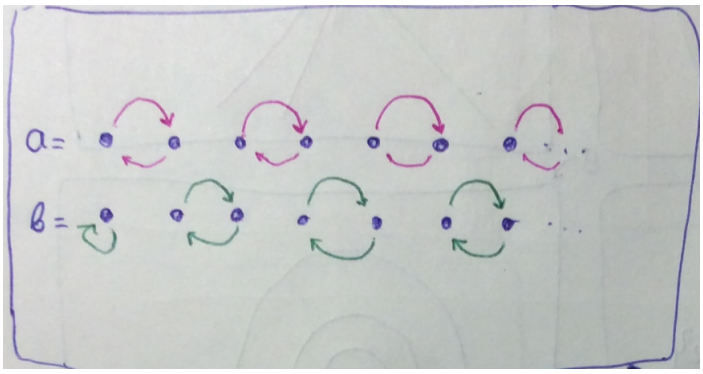
$$ab = \begin{pmatrix} 1 & 2\lambda \\ 0 & 1 \end{pmatrix}$$

такой выбор матрицы обусловлен в первую очередь тем, что пока мы не поняли какие именно к M *нужно выдвигать требования - ее лучше брать максимально простой, а умножение на матрицах подобного вида очень просто устроено: при перемножении просто складываются элементы, стоящие в правом верхнем углу. Нетрудно заметить, что* $(ab)^N = \begin{pmatrix} 1 & 2N\lambda \\ 0 & 1 \end{pmatrix}$, *а значит* $\mathrm{ord}(ab) = \infty$.

Хорошее упражнение: верно ли, что в описанном выше случае $\mathrm{ord}(ab) = \infty$ *для любой некоммутирующей с* a *матрицы* M, *а не только для жордановой клетки?*

2) *Геометрический пример.*

Рассмотрим $a, b \in S(\mathbb{N})$, *равные* $a = (12)(34)\ldots$, $b = (23)(45)\ldots$. *Графически эти биекции удобно задать графом, где стрелочками отмечается какой элемент в какой переходит.*



Ясно, что $a^2 = b^2 = 1$, *но при этом давайте посмотрим, как действует* $(ba)^N$ *на первый элемент 1. После первой итерации 1 перейдет по красной стрелочке в 2, а затем по зеленой в 3, применяя* ba *еще раз - мы сначала сдвинемся под действием* a *в 4, а затем в 5. Повторяя такую итерацию* N *раз мы приходим к тому, что* $(ba)^N(1) = 2N + 1$. *Таким образом* $(ba)^N \neq \mathrm{id}$, *потому что отличаются их значения как минимум на 1 (как функций, это же биекции из* $\mathbb{N}$ *в себя), так как для тождественной перестановки верно* $\mathrm{id}(1) = 1$. *Значит и в этом случае* $\mathrm{ord}(ab) = \mathrm{ord}(ba) = \infty$.

Оба примера поучительны даже не сколько в понимании, как порядок ведет при произведении, сколько ценными методами работы в этих группах и идеями построения контрпримеров к другим задачам, так как методы работы с этими группами довольно простые: $S(\mathbb{N})$ это фактически точки и стрелочки, а матрицы - это фактически жордановы формы, которые все на первом курсе проходили. Но эти группы имею чрезвычайно богатую внутреннюю структуру, и часто вопрос про произвольную группу можно редуцировать либо к матрицам, либо к перестановкам. Например $S(\mathbb{N})$ содержит в себе все конечные группы - одна и все сразу (потому что она содержит любое S_n, в некоторое из которых вкладывается произвольная конечная группа по теореме Кэли). Матричные группы тоже имеют богатейшую структуру, например, в GL_n при $n \geq 3$ можно построить парадоксальные множества в смысле Банаха-Тарского (это разбиение ведет к понятию аменабельных групп, о которых мы поговорим во второй части методички), т.е. это такое множество A, которое конгруэнтно двум своим непересекающимся подмножествам (иными словами существуют $c, b \in G$, что $B = bA, C = cA, B \sqcup C \subset A$). Например, для $\mathbb{R}^3$, на котором изометриями действует группа $O_3(\mathbb{R})$ ортогональных матриц, этот парадокс означает, что существует множество $M \subset \mathbb{R}^3$ и два его непересекающихся подмножества $A, B \subset M$, с каждым из которых M можно совместить вращениями. Конечно же, если бы допускались произвольные преобразования пространства - то такой конструкции - грош цена, и сгодилось бы любое бесконечное множество. Пафос именно в том, что совмещается оно с помощью изометрий. Самое интересное, что в $\mathbb{R}^2$ такое множество построить невозможно. Одно из следствие всего этого, что в $\mathbb{R}^3$ не существует конечно аддитивной меры (инвариантной относительно движений), определенной на всех множествах (для счетно аддитивных мер, насколько вы помните, ответ зависит от того, принимаем ли мы аксиому детерминированности). А в $\mathbb{R}$ и $\mathbb{R}^2$ такая мера существует и называется мерой Хаусдорфа. И причина такого разделения в том, что группа $O_2(\mathbb{R})$ - аменабельна, тогда как $O_n(\mathbb{R})$ неаменабельна при $n \geq 3$. Возможно, этот факт про меры, полноценно раскрывающийся в призме именно теории групп, будет лишним аргументов пользу того, насколько важны группы в математической жизни.

Задача

Пусть $|G| < \infty$. Доказать, что $\mathrm{ord}(g) < \infty$ для любого $g \in G$.

Пусть $\mathrm{ord}(g) = \infty$. Тогда все элементы $e, g, g^2, g^3, \ldots$ различны, потому что если бы два совпали $g^n = g^m$, то $g^{n-m} = e$ и получаем противоречие с бесконечностью порядка. Но бесконечное число попарно различных элементов не поместятся в конечное множество G. Приходим к противоречию.

Группы перестановок

Определение

Группой перестановок S_n *называется* $S(\{1, 2, \ldots, n\})$ *группа биекций* n*-элементного множества.*

Группа эта очень важная, так как с одной стороны любая конечная группа в группу перестановок вкладывается. С другой стороны, структура элементов и их произведений очень прозрачная, все можно потрогать руками, при необходимости подробно расписать любое множество, любое комбинаторное условие на элементы. Так что группы перестановок всегда будут для нас центральным примером конечных групп.

Любой элемент группы перестановок - это функция из n-элементного множества в себя, такую функцию удобнее всего задавать одним из следующих трех способов:

1) Табличкой: в первой строчке выписываем все аргументы, а в нижней куда они соответственно переходят.

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 4 & 7 & 6 & 8 \end{pmatrix}$$

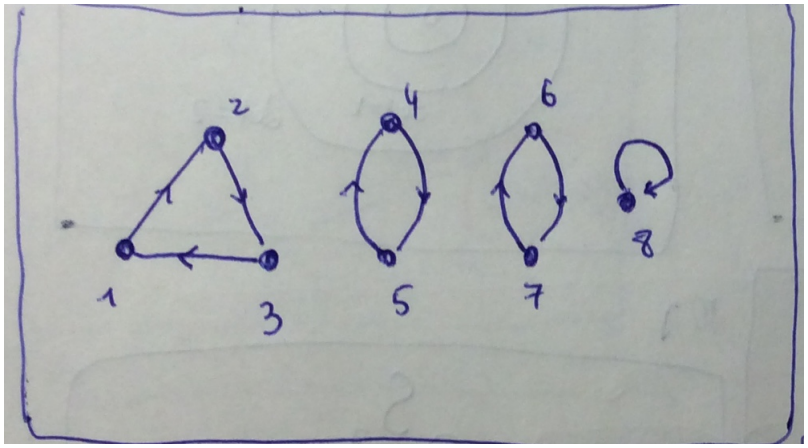
2) Независимыми циклами: в одну строчку выписываем аргументы так, что каждый предыдущий переходит в последующий, когда цикл замыкается - выделяем соответствующую группу аргументов круглыми скобочками. Например, упомянутая выше перестановка в независимых циклах запишется:

$$a = (123)(45)(67)$$

Циклы длины 1 соответствуют неподвижным элементам и обычно опускаются (будем считать, что на элементах, которые не попали в запись, перестановка действует тождественно). Так как носители независимых циклов не пересекаются - то они коммутируют, а сама перестановка равна групповому произведению всех независимых циклов, причем порядок циклов не важен. Также не важно, с какого элемента цикл начинался. Например, упомянутую выше перестановку можно записать и так: $a = (54)(67)(231)$. Если перемножить две перестановки, заданные в виде произведения независимых циклов - полученное разложение хотя и будет произведением циклов, но они не обязаны быть независимыми (т.е. иметь непересекающиеся носители) - и как следствие они не обязаны коммутировать. И когда в данном случае хотят подчеркнуть границу между перестановками (где заканчиваются независимые циклы одной перестановки и начинаются циклы другой: главном образом из эстетических соображений, чтобы это произведение было воспринимаемое) - то обычно обрамляют перестановки в квадратные скобочки.

Циклический тип перестановки - это "скелет" перестановки, а именно информация о количестве независимых циклов заданной длины, без уточнения, какие аргументы в эти циклы входят. Для циклического типа много обозначений, каждое из которых легко расшифровывается, но обычно используют одно из 4 стандартных, которые мы проиллюстрируем на примере нашей тестовой перестановки: $3 * 2 * 2$, или $3 * 2^2$, или $3 + 2 + 2$, или $(* * *)(**)(**)$ - смысл в каждой ситуации понятен, и можно использовать более приглянувшийся способ записи. Циклический тип чем-то отдаленно напоминает сигнатуру из линала.

3) С помощью графа: визуализация независимых циклов, когда аргументы отмечаем точками, а стрелочками отмечаем, какой аргумент в какой переходит.



Нужен для понимания структуры перестановок тем, кто картинки воспринимает лучше формул, а также отлично подойдет для теоретических задач, с условиями на *область определения перестановок*. В математике обычно чем больше для математического объекта форм записи и интерпретаций - тем лучше: и нужно пользоваться, что для перестановок есть три хорошие формы записи. И перед решением задачи прикинуть, какой способ подойдет для задачи лучше всего: хотя они и эквивалентны, но их интерпретация и восприятие очень различны: к примеру, порядок перестановки и запись в виде таблички на уровне восприятия почти несовместимы.

==========

Произведения в группе перестановок = композиция, а потому умножать перестановки нужно как композицию: *справа налево*.

Пример

Перемножить перестановки $a = (13)(57)(246)$ *и* $b = (135)(24)(67)$.

Есть два стандартных способа перемножения перестановок: неоптимальный и сложный, когда перестановки записываются табличками, причем так, чтобы нижняя строка первой совмещалась с верхней строкой второй:

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 2 & 1 & 7 & 6 \end{pmatrix}$$

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 1 & 6 & 7 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 4 & 5 & 2 & 1 & 7 & 6 \\ 1 & 6 & 7 & 4 & 3 & 5 & 2 \end{pmatrix}$$

А дальше нужно "совместить" таблички - и результат умножения будет перестановка, переводящая аргументы самой верхней строчки в соответствующие аргументы самой нижней строчки:

$$ab = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 7 & 4 & 3 & 5 & 2 \end{pmatrix}$$

Мне этот способ не нравится, так как он трудоемкий и плохо отражает структуру элементов и их произведения.

Второй способ - простой, структурно понятный и быстрый = это отвечать себе на вопрос, куда под действием композиции переходит каждый аргумент, потом его

образ, образ образа и т.д. например, для произведения

$$ab = [(13)(57)(246)][(135)(24)(67)]$$

спросим: куда переходит 1? Сначала b его отправит в 3, а затем a полученную 3 отправит в обратно в 1. Получили цикл длины 1. Берем следующую жертву: 2 под действием b перейдет в 4, а 4 уже под действием a в 6, таким образом $2 \mapsto 6$ под действием ab. Теперь то же самое нужно проделать с 6, с его образом, образом образа и т.д., пока мы обратно не вернемся в 2 и получим новый независимый цикл, в данном случае это будет (2657). Проделав такую операцию со всеми аргументами получим:

$$ab = [(13)(57)(246)][(135)(24)(67)] = (2657)$$

Запись тоже, кстати говоря, более компактной получилась.

Замечания:

Чтобы от элемента взять обратный - в табличке нужно поменять местами верхнюю и нижнюю строчки, а в случае записанного с помощью независимых циклов элемента - просто пустить циклы "в обратную сторону", т.е. к примеру, если $a = (1235)(64)$, *то* $a^{-1} = (5321)(46)$ *- думаю, это должно быть понятно.*

Произведение в группе перестановок некоммутативно, что типично для композиций отображений. Для построения контрпримера подойдет почти любая рандомная пара, но самый просто пример следующий:

$$(12)(23) = (123)$$

$$(23)(12) = (132)$$

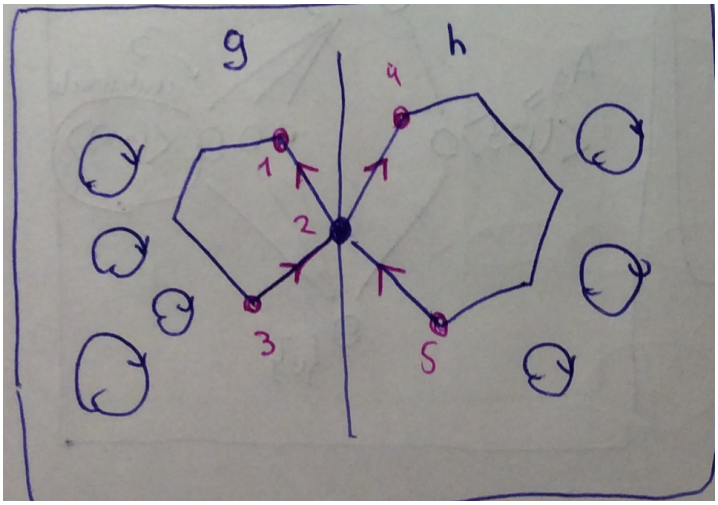
Отмечу, что группы S_1 *и* S_2 *все же являются абелевы - для неабелевости нужны минимум три аргумента, чтобы нашлись циклы с непересекающимися носителями.*

Что касается произведений, то подумайте над следующим вопросом: давайте введем на множестве перестановок $(S_n, \circ)$ *новую операцию* $a \circ b = ba$, *т.е. это обычное умножение, но в обратном порядке. Иными словами эти странные перестановки перемножаются не как композиции справа налево, а слева направо. Разберитесь, будет ли это группой, а если да, то будет ли* S_n *с этим экзотическим умножением изоморфна обычной группе перестановок, а если да, то можно ли построить явный изоморфизм?*

Задача

Даны две перестановки $g, h \in S_n$, *такие, что* $\sharp\{supp(g) \cap supp(h)\} = 1$ *(здесь* $\sharp$ *- мощность множества, а* $supp(g) = \{i : g(i) \neq i\}$ *носитель перестановки, т.е. множества тех аргументов, которые передвигаются под действием* g *- это общематематическое понятие. Требуется доказать, что* $ghg^{-1}h^{-1} = (***)$.

Здесь будем пользоваться геометрической интерпретацией перестановок: аргументы, которые не попали в носители ни g, ни h вообще не будем рассматривать - так как на них любая полученная из g, h комбинация будет действовать тождественно. Оставшиеся аргументы разделим линией на те, кто попадает в носитесь g, а кто в носитель h. Пересекаются они по одному элементу. Обозначим числами стоящий на пересечении аргумент, а также всех его соседей по графу.



Ясно, что на всех, кроме этих пяти элементов, перестановка $ghg^{-1}h^{-1}$ действует тождественно (например, если взять такой аргумент из носителя, скажем, h, то с помощью h^{-1} он "не дотянется" до носителя g, а значит g и g^{-1} в данном случае будут действовать тождественно).

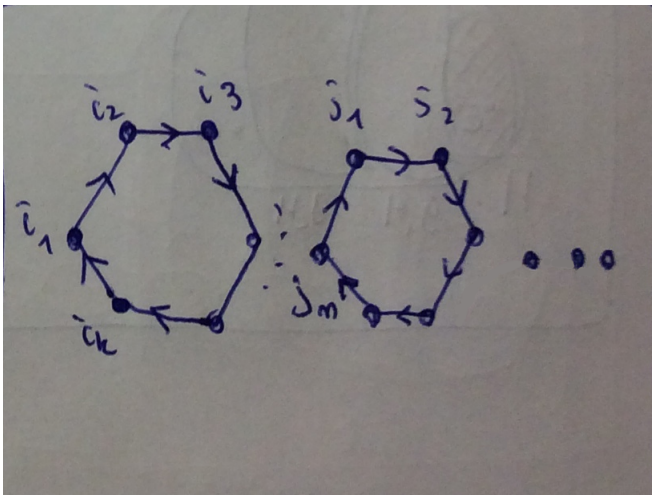
Для отмеченной же пятерки непосредственно находим их образы под действие коммутатора, и получаем, что

$$ghg^{-1}h^{-1} = (421)$$

==========

Порядок перестановок из S_n

Пусть $\sigma = (i_1, \ldots, i_k)(j_1, \ldots, j_m)\ldots$, соответствующий граф будет такой:



Нетрудно заметить, что в N-степени σ становится тождественной iff когда "замыкаются" все ее циклы, а именно:

$$\sigma^N = 1 \iff \begin{cases} N \text{ делится на } k \\ N \text{ делится на } m \\ \quad \ldots \end{cases} \iff N \text{ делится на } \mathrm{HOK}(k, m, \ldots)$$

Минимальное N с таким условием равно в точности $\mathrm{ord}(\sigma) = \mathrm{HOK}(k, n, \ldots)$.

Задача

Доказать, что

- *В S_6 нет элементов порядка 7.*
- *В S_8 найти элемент порядка 15.*
- *$x^6 = 1$ для любых $x \in S_3$.*
- *$[x^2, y^2] = 1$ для любых $x, y \in S_3$.*

---

1) Порядок элементов в S_n - это НОК длин независимых циклов. Так как 7 простое число, то в перестановке должен быть независимый цикл длины 7, что невозможно в S_6.

2) В отличие от первого пункта 15 уже составное число, равное $15 = \text{НОК}(3, 5)$. Таким образом порядок 15 имеет перестановка с циклическим типом:

$$(***)(*****)$$

Нетрудно заметить, что перестановки с другими циклическими типами не могут иметь порядок 15, т.к. 15 раскладывается в НОК только двумя способами (либо $= \text{НОК}(3, 5)$, либо $= \text{НОК}(15, 1)$, но последний случай не соответствует никаким перестановкам в S_8).

3) Нетривиальные циклические типы в S_3 сводятся к двум:

$$(**) \qquad (***)$$

В обоих случаях в 6-ой степени они становятся тождественными.

4) При возведении в квадрат перестановок из предыдущего пункта мы получим только один возможный для квадратов циклический тип: $(***)$. Всего перестановок с таким циклическим типом две: (123), (132). Непосредственно проверяется, что они коммутируют. В случае совпадающих $x^2 = y^2$ очевидно, что перестановка коммутирует сама с собой.

Комбинаторная задача

Найти количество элементов порядка 6 в S_7.

Аналогично второму пункту предыдущего примера для перестановок порядка 6 допустимы лишь три циклических типа:

$$(******) \qquad (**)(***) \qquad (**)(**)(***)$$

1) Для подсчета таких перестановок в первом случае заметим, что перестановка без учета порядка однозначно определяется единственным остающимся неподвижным аргументом (а их всего 7), упорядоченных способов расположить оставшиеся элементы 6!, причем для перестановки неважно, с какого номера начинается перестановка - а значит должны поделить на 6 (можно было рассуждать и так: берем произвольный элемент - возможностей для его образа 5 штук, для последующего образа - 4 штуки, и т.д., опять-таки придем к 5!). Это можно резюмировать в следующее наблюдение: *циклов длины k на фиксированных k элементах всего $(k-1)!$ штук.*

Таким образом:

$$N_1 = 7 \cdot \frac{6!}{6} = 840$$

2) Для подсчета перестановок второго типа - заметим, что возможностей выбрать пару элементов $= C_7^2$, согласно упомянутому выше наблюдению на выбранной паре можно организовать 1! различных циклов (что естественно: ведь существует только одна транспозиция на множестве из двух элементов). Из оставшихся нужно 3 элемента, на которых цикл запускается $2! = 2$ способами: (abc) и (acb), имеем:

$$N_2 = C_7^2 \cdot 1 \cdot C_5^3 \cdot 2 = 420$$

3) В последнем случае рассуждения аналогичные: комбинаторно вычисляем сколькими способами можем набрать аргументы для выбранного цикла длины k и умножаем на $(k-1)!$, лишь уточню, что в этом случае нужно еще поделить на два, т.к. в перестановке не важно в каком порядке идут два цикла $(**)$:

$$N_3 = \frac{C_7^2 \cdot 1 \cdot C_5^3 \cdot 2 \cdot C_2^2 \cdot 1}{2} = 210$$

естественно, их получилось в 2 раза меньше, чем предыдущего типа: потому что каждой паре перестановок $(ab)(***)$ и $(cd)(***)$ - предыдущего типа (таких, что $\{a, b, c, d, *, *, *\} = \{1, 2, 3, 4, 5, 6, 7\}$) соответствует одна перестановка третьего типа $(ab)(cd)(***)$. Итого получаем, что всего перестановок порядка 6:

$$N = N_1 + N_2 + N_3 = 1470 \approx 29,2\%$$

такими комбинаторными приемами по подсчету количества перестановок с определенными свойствами должны владеть абсолютно все.

==========

Сопряжение в группе S_n

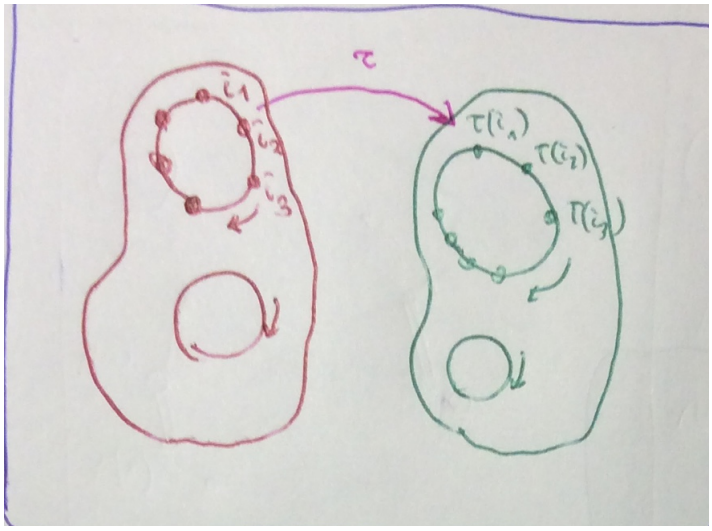
Для сопряжения перестановок есть очень простая и удобная для применений формула (я бы сказал, что это чуть ли не самая важная формула на перестановки): пусть $\sigma = (i_1, \ldots, i_k)(j_1, \ldots, j_m)\ldots$. Тогда:

$$\boxed{\tau\sigma\tau^{-1} = (\tau(i_1), \ldots, \tau(i_k)(\tau(j_1), \ldots, \tau(j_m)\ldots}$$

проверяется это очень просто: перестановки совпадают, когда совпадают их действия на произвольных аргументах: имеем

$$\tau\sigma\tau^{-1} : \tau(i_p) \mapsto \tau(i_{p+1 \ mod \ k})$$

т.е. действие в точности такое же, как и у правой части доказываемого равенства. Ясно, что в других циклах точно такая же картина - значит они равны. Визуализировать это хочется следующей картинкой:



Фактически, перестановки σ и $\tau\sigma\tau^{-1}$ отличаются не структурой, а только "угла", с которого вы на эту перестановку смотрите; формула CAC^{-1} должна навеивать ностальгические воспоминания про линальный переход к другому базису. Можно сказать, здесь это же и происходит, если отождествлять i с базисным вектором e_i а перестановку σ с соответствующей матрицей перестановки T_σ, действующей на базисных векторах $T_\sigma(e_i) = e_{\sigma(i)}$.

Отмечу также, что эта формула очень эффективна для вычислений, с ее помощью вычисляется не только результат сопряжений, но даже обычные произведения пытаются максимально сводить к сопряжениям для упрощения выкладок, иногда даже ценой кажущегося вычислительного усложнения. К примеру, при вычислении коммутатора перестановок $[g,h] = ghg^{-1}h^{-1} = (ghg^{-1})h^{-1}$ оптимально сначала вычислить сопряжение ghg^{-1} (так как оно выписывается с ходу), а потом его умножить на h^{-1}, т.е. фактически вычисление коммутатора сводится к одному! умножению вместо трех. Не забывайте про этот трюк.

Также отмечу, что упомянутая формула - это формула для $\tau\sigma\tau^{-1}$, а не $\tau^{-1}\sigma\tau$ - довольно легко перепутать порядок. Но нужно либо запомнить, либо придумать какое-нибудь мнемоническое правило для запоминания, либо всякий раз эту формулу выводить, пока она намертво не запомнится. Лично я, зная какая формула должна получиться, задаю себе вопрос: куда перейдет аргумент $\tau(i_p)$. Ясно, что образ его будет "хорошим" при действии $\tau\sigma\tau^{-1}$ и плохим при $\tau^{-1}\sigma\tau$. Если нужно вычислить $\tau^{-1}\sigma\tau$ - то можно вычислить τ^{-1} и свести к исходной формуле. Если в задаче есть альтернатива, какое именно сопряжение использовать - то старайтесь выбирать сопряжение, где обратный стоит справа, так как именно в этом случае получаем молниеносную формулу.

В частности из этой архиполезной формулы вытекает следующее:

Наблюдение

Две перестановки в S_n сопряжены iff у них одинаковый циклический тип

$\Longrightarrow$ Очевидно вытекает из формулы.

$\Longleftarrow$ Если циклические типы совпадают - то можно построить биекцию Ω между циклами первой и второй перестановки, а дальше определить τ так, чтобы она отправляла элементы из каждого независимого цикла в элементы соответствующего при биекции Ω цикла с сохранением порядка. Типично, что осуществляющая сопряжение перестановка τ не единственна: произвол заключается в:

1) В выборе начального элемента цикла: например, если τ должна отправить (123) в (456), то 1 можно отправить в 4, 5 или 6, а после этого выбора τ на остальных элементах определяется однозначно.

2) Перемешивании циклов одинаковой длины

В частности, перестановки σ, такие что $\sigma\tau\sigma^{-1} = \tau$ сопрягающие перестановку τ с собой состоят в точности из перестановок, коммутирующих с τ. В частном случае $\tau = \mathrm{id}$ - любая перестановка годится в роли сопрягающей.

Пример

Сопряжены ли перестановки $\sigma_1 = (123)(45)$ и $\sigma_2 = (345)(12)$, а если да, то найти какую-нибудь сопрягающую перестановку

У них одинаковый циклический тип - значит они сопряжены. Если $\sigma_2 = \tau\sigma_1\tau^{-1}$, то по упомянутой выше формуле имеем:

$$(345)(12) = (\tau(1)\tau(2)\tau(3))(\tau(4)\tau(5))$$

Ясно, что в качестве сопрягающей подойдет:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

Всего возможных сопрягающих перестановок будет 6 штук - так как цикл длины 3 (2 соответственно) должен перейти в цикл длины 3 (2 соответственно). В рамках цикла длины 3 у нас три возможности отображения с сохранением порядковой структуры (для первого элемента цикла у нас 3 возможности, но после этого выбора образы остальных элементов определяется однозначно), для цикла длины 2 всего 2 возможности. Например, в качестве сопрягающей сгодится и такая перестановка:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}$$

==========

Порождающие элементы для S_n

Нетрудно заметить, что

$$(12)(23)\dots(n-1,n) = (123\dots n)$$

(для этого рассмотрим произвольный аргумент i. Под действие правой перестановки он перейдет в $i+1$, под действием большого произведения он будет неподвижен, пока не дойдем до сомножителя $(i, i+1)$, потом перейдет в $i+1$, и дальше останется неподвижным. Отдельно нужно рассмотреть, что происходит с образом n - в обоих случаях он перейдет в 1)

Комбинаторное утверждение

Доказать, что S_n порождается каждым из следующих наборов.

- $\{(k, k+1)\}$
- $\{(1, k)\}$
- $\{(12), (123\dots n)\}$

---

1) Докажем, что любую перестановку σ можно представить как произведение набора транспозиций вида $(k, k+1)$. Разложим перестановку в произведение независимых циклов:

$$\sigma = (i_1, i_2, \dots, i_k)(j_1, j_2, \dots, j_m)\dots$$

На основании замечания выше имеем:

$$(12)(23)\dots(n-1, n) = (123\dots n)$$

Таким образом при должной перенумерации индексов каждый независимый цикл можно представить в виде произведения транспозиций (i, j) (замечу, что транспозиции не обязаны иметь вид $(i, i+1)$ с последовательно идущими аргументами, так как в независимых циклах аргументы не обязаны быть последовательными).

Для доказательства осталось доказать, что любая транспозиция (i, j) представляется как произведение транспозиций вида $(i, i+1)$, что легко вытекает из следующего равенства (здесь мы используем формулу для сопряжения перестановки; можно считать, что $i < j$):

$$(i, i+2) = (i+1, i+2, \dots, j)(i, i+1)(i+1, i+2, \dots, j)^{-1}$$

$$(i, i+3) = (i+1, i+2, \dots, j)^2(i, i+1)(i+1, i+2, \dots, j)^{-2}$$

$$\dots\dots\dots\dots$$

$$(i, j) = (i+1, i+2, \dots, j)^{j-i-1}(i, i+1)(i+1, i+2, \dots, j)^{-(j-i-1)}$$

В цикле все аргументы идут подряд, а потому цикл можно породить транспозициями вида $(i, i+1)$. Итог: любую перестановку можно породить транспозициями вида $(i, i+1)$.

---

2) Используя первый пункт достаточно породить не произвольную перестановку, а перестановки, которые любую перестановку порождают, а именно транспозиции вида $(k, k+1)$. Порождение для них вытекает из формулы для сопряжения (очевидно, что $(i, j)^{-1} = (i, j)$):

$$(k, k+1) = (1, k+1)(1, k)(1, k+1)^{-1}$$

---

3) Пусть $a = (12)$, $b = (123\dots n)$, тогда используя конструкцию из первого пункта получаем:

$$(1, k) = b^{k-2}ab^{-(k-2)}$$

из чего вытекает, что любая перестановка g выражается через a, b, т.е. представляется как произведение $g = g_1 g_2 \dots$, где $g_i \in \{a, b\}$.

Замечания:

Последний пункт кажется весьма удивительным, так как любая S_n порождается всего двумя перестановками, хотя является универсальным вместилищем всех конечных групп. Из этого наблюдения в частности вытекает, что подгруппы типично имеют большее минимальное число порождающих элементов, чем объемлющие их группы, хотя в линале с пространствами все было с точностью до наоборот: размерность подпространства была всегда меньше размерности всего пространства.

Также отметьте себе универсальный прием при работы с порождающими, которым мы воспользовались при решении этой задачи: что два набора порождают одну и ту же группу (пространство, алгебру и т.д... это работает для любой алгебраической структуры) iff каждый элемент из одного набора выражается через элементы другого набора. Иногда при должном старании это позволяет уменьшить число порождающих (как получилось у нас сейчас при успешном прохождении через все три пункта задачи - массу порождающих мы свели лишь к двум), либо свести к другим порождающим, связанными менее сложными соотношениями.

Замечу, что по определению группа G порождается элементами $x, y, \ldots$, если любой $g \in G$ представим как $g = g_1^{\pm 1} g_2^{\pm 1} \ldots$, где $g_i \in \{x, y, \ldots\}$. Однако если группа конечна, то как мы уже поняли у любого элемента конечный порядок, а значит $g^{-1} = g^n$ для любого g при некоторой степени n. Таким образом, в конечных группах элементы $\{x, y, \ldots\}$ порождают G, если всякий элемент допускает представление $g = g_1 g_2 \ldots$, где $g_i \in \{x, y, \ldots\}$, т.е. где все фигурирующие степени положительны. В бесконечных группах это, разумеется, неверно: например группа $\mathbb{Z}$ порождается 1, тогда как без взятия обратного с помощью этой 1 вы не сможете получить отрицательные числа. Множество всевозможных произведений, где допускаются исключительно положительные степени называется полугруппой, порожденной данным множеством. У полугрупп своя нетривиальная и красивая теория.

==========

Четность перестановок

Четность перестановки - это очень важный инвариант, сохраняющийся при сопряжении и уважающий групповое умножение. Четность перестановки является очень хорошим *препятствием* для реализации некоторых соотношений или конструкций в перестановках, позволяя во многих случаях почти сразу сказать твердое и элегантное "нет", тогда как лобовой подход приводил бы к очень весомым выкладкам. Четность перестановки является прямой групповой аналогией линального определителя, или же ориентации преобразования пространства. Важность ее усиливается еще и тем, что в группах перестановок нет аналога следа матриц: потому что на матрицах определено умножение и сложение, а на перестановках только умножение, и четность вынуждена в перестановках отдуваться сразу за двоих.

Определение

Четностью называется отображение $\tau : S_n \to \mathbb{Z}_2$, заданное на $\sigma = (i_1, \ldots, i_k)(j_1, \ldots, j_m)\ldots$ формулой:

$$\boxed{\tau(\sigma) = (k-1) + (m-1) + \ldots \mod 2}$$

т.е. фактически четность суммы уменьшенных на 1 длин всех независимых циклов.

Для четности есть вторая альтернативная формула:

$$\tau(\sigma) = \text{число инверсий } \sigma \mod 2$$

где число инверсий вычисляется по следующей формуле: берем и записываем перестановку σ в виде таблички с первой упорядоченной строкой, а дальше проходим нижнюю строку и для каждого аргумента вычисляем количество аргументов больше его и при этом стоящих левее.

Например, для

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$$

проходим по второй строчке: у 4,5,6 слева от каждого стоят только числа меньшие их. Для 1 инверсиями являются 4,5,6, для 2 и 3 тоже 4,5,6. Таким образом по второй формуле $\tau(\sigma) = 3 + 3 + 3 \mod 2 = 1$. Для того, чтобы воспользоваться первой формулой раскладываем перестановку в произведение независимых циклов: $\sigma = (14)(25)(36)$, тогда по первой формуле $\tau(\sigma) = 1 + 1 + 1 \mod 2 = 1$. И хотя количество инверсий не совпадает с суммой уменьшенных на 1 длин всех независимых циклов, но по модулю 2 они совпадают.

Сразу скажу, что удобнее пользоваться первой формулой, так как она и вычислительно проще (сложить тройку чисел проще, чем перебирать множество всевозможных пар), да и в жизни перестановки чаще встречаются в виде произведения независимых циклов, нежели заданные таблицей; но в реальности обе формулы нужны, и наличие для некоторого математического объекта двух формул его вычисления всегда лучше одной.

Свойства четности

1) $\tau(\mathrm{id}) = 0$

2) $\tau(xy) = \tau(x) + \tau(y) \mod 2$

Отсюда вытекает, что четность не меняется при сопряжении: нетрудно заметить, что перестановки x и x^{-1} имеют одинаковый циклический тип для любой перестановки x, а значит из первой формулы получаем, что $\tau(x) = \tau(x^{-1})$, а значит:

$$\tau(xyx^{-1}) = \tau(x) + \tau(y) + \tau(x^{-1}) = \tau(x) + \tau(y) + \tau(x) = \tau(y) \mod 2$$

Также отмечу, что из второго свойства также вытекает, что если перестановка $x = a_1 a_2 \ldots a_k$ представлена в виде произведения транспозиций a_i, то $\tau(x) = k \mod 2$, так как четность каждой транспозиции равна 1. Забегая вперед скажу, что эти два свойства фактически означают, что отображение четности является гомоморфизмом групп $\tau : S_n \to \mathbb{Z}_2$.

Определение

Перестановки σ, четность которых равна 0, называются четными, а у которых равна 1 называются нечетными. Множество четных перестановок с операциями из S_n является группой и обозначается:

$$A_n = \{\sigma \in S_n : \tau(\sigma) = 0\}$$

Задача

Найти порядок группы A_n.

Стандартное доказательство фактически имитирует разбиение на смежные классы из теоремы Лагранжа: рассмотрим произвольную нечетную перестановку, например $\sigma = (12)$. Тогда нетрудно заметить, что:

$$S_n = A_n \sqcup \sigma A_n$$

Действительно, эти два множества не пересекаются, т.к. для $x \in A_n$ перестановка $\sigma x \notin A_n$ (так как $\tau(\sigma x) = \tau(\sigma) + \tau(x) = 1 + 0 = 1$). Более того, для любой $x \notin A_n$ верно $x \in \sigma A_n$ так как $x = \sigma(\sigma^{-1}x)$, где $\sigma^{-1}x \in A_n$ потому что $\tau(\sigma^{-1}x) = \tau(\sigma)+\tau(x) = 1 + 1 = 0$ (хотя $\sigma = \sigma^{-1}$ для выбранной нами $\sigma = (12)$, рассуждения я провел так, чтобы они проходили и для любой другой нечетной перестановки).

Далее замечаем, что отображение $\lambda_\sigma : S_n \to S_n$, $\tau \mapsto \sigma\tau$ является биекцией (проверьте это), а значит в частности $\#A_n = \#\sigma A_n$. Таким образом:

$$\#S_n = \#(A_n \sqcup \sigma A_n) = 2\#A_n$$

Таким образом $\#A_n = \frac{n!}{2}$.

Задача

Существуют ли перестановки x, y, z с циклическим типом $(***)$, такие что $xyz = (12)$?

Предположим, что такие перестановки существуют - тогда вычислим четность от обеих частей:

$$1 = \tau(12) = \tau(xyz) = \tau(x) + \tau(y) + \tau(z) = 0 + 0 + 0 = 0$$

Приходим к противоречию.

Пример

Сопряжены ли в A_4 перестановки (123) и (132)? Сопряжены ли они в A_5?

Мы помним, что две перестановки сопряжены в S_n iff у них одинаковый циклический тип, но в A_n эта теорема не работает, так как сопрягающие две четные перестановки не обязаны сами быть четными перестановками. И пример из задачи классический, когда нельзя выбрать четную сопрягающую.

Пусть $\sigma_1 = (123)$, $\sigma_2 = (132)$ и $\sigma_1 = \tau\sigma_2\tau^{-1}$ для некоторой $\tau \in A_4$. Вспоминаем волшебную формулу для сопряжения и получаем:

$$(123) = \tau(132)\tau^{-1} = (\tau(1)\tau(3)\tau(2))$$

Ясно, что $\tau(4) = 4$. Возможно, в этом случае можно было придумать какое-нибудь наблюдение, уменьшившее бы перебор до минимума, но так как нужно перебрать всего 3 перестановки - то просто сделаем это: перестановка τ полностью восстанавливает после того, как мы выбрали образ для фиксированного аргумента, для которого существует 3 варианта. Таким образом существует лишь 3 возможности для τ:

$$\begin{cases} \tau(1) = 1 \\ \tau(3) = 2 \\ \tau(2) = 3 \end{cases} \implies \tau = (23) \qquad \begin{cases} \tau(1) = 2 \\ \tau(3) = 3 \\ \tau(2) = 1 \end{cases} \implies \tau = (12) \qquad \begin{cases} \tau(1) = 3 \\ \tau(3) = 1 \\ \tau(2) = 2 \end{cases} \implies \tau = (13)$$

Во всех возможных случаях сопрягающая перестановка оказывает нечетной, значит исходные перестановки не сопряжены в A_n.

В A_5 же эти перестановки оказываются сопряженными и в качестве сопрягающей можно взять, к примеру, $\tau = (13)(45)$ - перестановка (13) как мы уже поняли являются сопрягающей, и так как $\{4, 5\}$ и $\{1, 2, 3\}$ не пересекаются, то с одной стороны добавление цикла (45) никак не повлияет на результат сопряжения, а с другой стороны превратит сопрягающую перестановку в четную. Ясно, что в A_n при $n \geq 5$ они тоже являются сопряженными.

Утверждение

Доказать, что A_n порождается тройными циклами при $n \geq 3$.

Вспоминаем, что в одном из предыдущих примеров мы уже поняли, что любая перестановка представляется как произведение более простых, и даже построили 3 порождающих множества. Лучше всего для этой задачи подойдет порождение под пунктом 2, а именно, что любая перестановка представляет собой произведение транспозиций вида $(1, i)$. Рассмотрим подобное представление для произвольной четной перестановки:

$$\sigma = (1, i_1)(1, i_2)(1, i_3)(1, i_4)\dots$$

Так как перестановка σ четная, то количество транспозиций в этом разложении четное число, а значит они естественным образом по своему порядку в этом произведении разбиваются на пары: 1-ая и 2-ая, 3-ья и 4-ая и т.д. Нетрудно заметить, что произведение одной такой пары это тройной цикл: $(1, i)(1, j) = (1, j, i)$, таким образом и вся исходная перестановка раскладывает в произведение тройных циклов:

$$\sigma = (1, i_2, i_1)(1, i_4, i_3)\dots$$

Замечания:

Изначально, можно было использовать более слабую версию теоремы о порождающем множестве, к примеру, факт, что любая перестановка раскладывается в произведение транспозиций без каких-либо дополнительных ограничений на транспозиции - этот факт доказывается практически даром, но тогда доказательство, что A_n порождается тройными циклами, стало бы чуть более технически сложным: дословно повторяя рассуждения с разбиениями на пары - мы бы пришли к необходимости доказывать, что двойное произведение $(i, j)(k, l)$ порождается тройными циклами, и это чуть более сложный факт, так как нужно рассматривать всевозможные случаи взаимного расположение аргументов i, j, k, l относительно друг друга.

Замечу также, что мы не просто доказали, что A_n порождается тройными циклами, а даже более сильное утверждение: что оно порождается тройными циклами вида $(1, i, j)$.

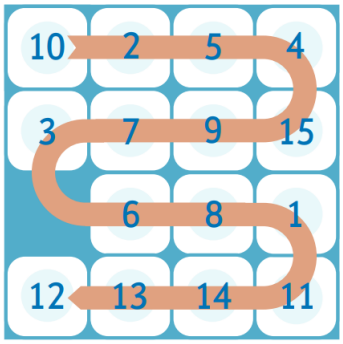
Историческая задача

Предположим, что один безумный стоматолог с понятными только ему целями полтора века назад дает в газету объявление, что он даст крупное денежное вознаграждение любому, кто сможет в игре "Пятнашка" переставить 14 и 15 местами, при этом остальные костяшки должны вернуться на свои изначальные места. Доказать, что это сделать невозможно.

Напомню суть игры в "Пятнашку": в квадрат 4×4 помещают пронумерованные 15 квадратных 1×1 костяшек, упорядоченных слева направо, а при заполнении строчки - переходя на следующую строчку. Клетка с координатами $(4, 4)$ остается пустующей. В этой игре можно делать ход, смещая в пустую клетку соседнюю с ней костяшку, иными словами если считать пустое место невидимой костяшкой - то переставляя эту невидимую костяшку с некоторой с ней соседствующей. Перед игрой обычно нужно хаотично подвигать костяшки и сбить изначальный порядок, и цель игры (подобно игре в кубик Рубика): вернуть изначальное расположение костяшек.

В задаче же нужно показать, что невозможно движениями костяшек из начального состояния попасть в чуть измененное, где лишь костяшки 14 и 15 поменялись местами:

Для доказательства невозможности, каждому расположению костяшек сопоставим заданную таблицей перестановку из S_{15}, где в нижней строке образа выписываются все номера костяшек, перечисляемые вдоль змейки, игнорируя пустое место; к примеру игровой ситуации:



будет соответствовать перестановка:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 2 & 5 & 4 & 15 & 9 & 7 & 3 & 6 & 8 & 1 & 11 & 14 & 13 & 12 \end{pmatrix}$$

Утверждается, что в процессе игры четность соответствующих игровым ситуациям перестановок не меняется, а потому так как перестановка, соответствующая ситуации из задачи, получается из "стартовой" перестановки умножением на транспозицию $(14, 15)$: то у них разные четности и такое расположение костяшек не может быть получено.

Итак докажем сохранение четности: если костяшка сдвигается влево-вправо - то соответствующая перестановка вообще не меняется - а значит и четность не меняется. Если же костяшка сдвигается вверх-вниз - то на уровне табличного задания перестановки соответствующее сдвигаемой костяшке число сдвигается в нижней строчке на *четное число шагов* влево или вправо, подвигая остальные числа (оно может сдвигаться и на 0 шагов, если этот сдвиг происходит вдоль змейки, как например в нашей ситуации при сдвиге костяшки 3). К примеру, для нашей тестовой ситуации при сдвиге костяшки 12 в пустое место - в перестановке она сдвигается на 6 шагов, сдвигая блок $(6, 8, 1, 11, 14, 13)$, то есть соответствующая новой ситуации перестановка будет равна:

$$\sigma_{new} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 2 & 5 & 4 & 15 & 9 & 7 & 3 & 12 & 6 & 8 & 1 & 11 & 14 & 13 \end{pmatrix}$$

И новая перестановка получается из старой умножением на цикл длины 7 (в общем случае на некоторый цикл нечетной длины, возможно даже длины 1 как в случае со сдвигом вдоль змейки, который не меняет перестановки), а именно:

$$\sigma_{new} = (6, 12, 13, 14, 11, 1, 8)\sigma$$

так как в реальности в раскрашенном блоке у вас все прокрутилось по циклу на один шаг. Так как цикл нечетной длины является четной перестановкой, то:

$$\tau(\sigma_{new}) = \tau(\sigma)$$

Сложно представить сколько суммарно нервных клеток читателей этой газеты было принесено в жертву математике.

==========

Задачи для самостоятельной работы

- *Выяснить, как изменяется разложение перестановки в произведение независимых циклов при ее умножении на некоторую транспозицию.*
- *Порождается ли S_n всевозможными циклами длины 4 при $n \geq 4$?*
- *Порождается ли S_n всевозможными циклами длины 5 при $n \geq 5$?*
- *Порождается ли A_n всевозможными тройными циклами вида $(1, 2, i)$ при $n \geq 3$?*
- *Доказать, что для любой перестановки $\sigma \in S_n$ существуют перестановки $\alpha, \beta \in S_n$, такие что $\sigma = \alpha\beta$ и $\alpha^2 = \beta^2 = \mathrm{id}$.*

Подгруппы

Определение

Подмножество $H \subset G$ называется подгруппой (писать в таком случае мы будем $H < G$), если

1) $e \in H$

2) $h^{-1} \in H$ для любого $h \in H$

3) $h_1 h_2 \in H$ для любых $h_1, h_2 \in H$

Иными слова подгруппой называется подмножество, замкнутое относительно всех групповых операций (это общекатегорная конструкция: вспомните, к примеру, подпространства, являющиеся подмножествами, замкнутыми относительно двух операций в линейном пространстве (сложение и умножение на скаляр)). Если H непусто, то первое условие выводится из второго и третьего: так как $e = hh^{-1} \in H$. Но все равно обычно записывают первое условия вместо уточнения непустоты H: так как ценой краткости такой подход более идеологически правильный, так как он подчеркивает, что подгруппа уважает всю групповую структуру (так же как пишут 8 аксиом линейного пространства, тогда как можно обойтись 7 аксиомами). Вторую аксиому выкинуть нельзя: например, $\mathbb{N} \subset \mathbb{Z}$ не замкнуто относительно второй аксиомы, при это для него выполняются аксиомы 1,3. Подгруппа сама является группой: аксиомы группы выполняются для любого подмножества, тогда как аксиомы 1-3 подгруппы обеспечивают корректность групповых операций: что они не выбивают за рамки нашего множества.

Пример

Пусть G - некоторая группа, $g \in G$ произвольный элемент. Тогда

$$\langle g \rangle = \{g^k\}_{k \in \mathbb{Z}} < G$$

и она называется *циклической подгруппой, порожденной g*. Легко понять, что

$$\langle g \rangle \cong \begin{cases} \mathbb{Z}_n, & \mathrm{ord}(g) = n \\ \mathbb{Z}, & \mathrm{ord}(g) = \infty \end{cases}$$

Циклические группы являются важнейшим и самым простым примером подгрупп, любой анализ подгрупп я советую начинать именно с них.

Пример

Далеко идущим обобщением циклической подгруппы является подгруппа, порожденная некоторым набором элементов (в нашем курсе в большинстве случаев конечным):

$$\langle g_1, g_2, \ldots, g_n \rangle = \{g_{i_1}^{\alpha_1} g_{i_2}^{\alpha_2} \ldots\} < G$$

Замечания:

• *Стоит отметить, что $H = \langle g_1, g_2, \ldots \rangle$ является в точности минимальной подгруппой $G(S)$, содержащей множество $S = \{g_1, g_2, \ldots\}$. Действительно, очевидно, что $G(S) < H$, так как $G(S)$ минимальна. С другой стороны $H < G(S)$, так как $\{g_1, g_2, \ldots\} \subset G(S)$ и раз $G(S)$ подгруппа, то всевозможные обратные и произведения этих элементов будут также лежать в $G(S)$, а это по определению H означает $H < G(S)$.*

• *Стоит отметить, что таким образом можно получить любую подгруппу произвольной группы G (правда в таком случае мощность порождающего множества не обязана быть конечной). Действительно, для произвольной*

подгруппы $H < G$ рассмотрим подгруппу $\langle H \rangle$ порожденную H (как множеством). Нетрудно понять, что $H = \langle H \rangle$. Отмечу, что из этого равенства вытекает, что любая подгруппа конечной группы оказывается конечно-порожденной: так как в качестве порождающего множества всегда можно рассмотреть всю подгруппу.

Также эта конструкция помогает в некотором смысле понять, каким образом устроена произвольная подгруппа: самые "элементарные" подгруппы - это циклические подгруппы $\langle g \rangle$. Дальше мы смотрим, какие группы получаются, если к описанным выше циклическим группами мы будем добавлять один дополнительный порождающий, таким образом мы получим все двухпорожденные группы $\langle g, h \rangle$; добавляя к двухпорожденным одну дополнительную порождающую мы получим трехпорожденные и т.д. Ясно, что этим процессом мы исчерпаем все подгруппы. Другое дело этот процесс очень неалгоритмизирован, и зачастую довольно сложно описывать даже подгруппы, порожденные фиксированной парой элементов. Обычно для описание всех подгрупп применяются дополнительные соображения (вроде теоремы Лагранжа, после мы рассмотрим конкретные примеры).

Утверждение

Доказать, что любая подгруппа $\mathbb{Z}$ циклическая и изоморфна $\mathbb{Z}$.

В этой задаче будем использовать мультипликативную форму записи. Пусть $H < \mathbb{Z} = \langle g \rangle$ и $H = \{g^{k_1}, g^{k_2}, \ldots\}$ (если кому-то некомфортна мультипликативная запись, то в аддитивной записи $H = \{k_1, k_2, \ldots\}$, считаем все k_i ненулевыми). Тогда рассмотрим $k = \min\{|k_1|, |k_2|, \ldots\}$ (у любого подмножества натуральных чисел всегда есть минимальный элемент, даже у бесконечного). Ясно, что $\langle g^k \rangle < H$, так как $g^{\pm k}$ содержится в H. С другой стороны $H < \langle g^k \rangle$ так как если какой-нибудь $g^m \in H$ не входит в $\langle g^k \rangle$, то поделив с остатком $m = dk + r$, $|r| < k$ мы получим, что $g^r = g^m g^{-dk} \in H$, что противоречит тому, что k выбирался минимальным. Таким образом $H = \langle g^k \rangle$ или в аддитивной записи $H = k\mathbb{Z}$.

Таким образом мы получили полную классификацию подгрупп $\mathbb{Z}$, полностью задающихся соответствующим множителем в аддитивной записи.

Утверждение

Пусть $G = \mathbb{Z}_n = \langle g \rangle$. Доказать, что:

- *Для любой $H < G$ выполняется $H = \langle g^k \rangle$ для некоторого k.*
- *Для любого k, такого что n делится на k, существует единственная $H < G$ с $|H| = k$. Более того $H = \langle g^{\frac{n}{k}} \rangle$.*

---

1) Пусть $H = \{g^{k_1}, g^{k_2}, \ldots\}$. Нетрудно заметить, что $H = \langle g^k \rangle$, где $k = \text{НОД}(k_1, k_2, \ldots)$. Действительно, по теореме о представлении НОД имеем $k = m_1 k_1 + m_2 k_2 + \ldots$, а значит:

$$g^k = g^{m_1 k_1} g^{m_2 k_2} \ldots \in H$$

и $\langle g^k \rangle < H$. С другой стороны ясно, что раз $k = \text{НОД}$, то $k_i = m_i k$, а значит $g^{k_i} \in \langle g^k \rangle$ и $H < \langle g^k \rangle$ так как $H = \{g^{k_1}, g^{k_2}, \ldots\}$.

2) Рассмотрим произвольную подгруппу $H = \langle g^\beta \rangle$ порядка $|H| = k$ (по первому пункту она обязана быть циклической, также можно считать, что β это минимальная положительная степень среди всех таких возможных порождающих H).

Рассмотрим $r = \text{НОД}(n, \beta)$. Из линейности представления НОД'а вытекает, что $g^r \in H$, а значит g^r порождает H (потому что r делит β, а потому g^β выражается через g^r, но g^β порождающий для H). В силу минимальности выбора β получаем, что $r = \beta$, иными словами

$$\beta = \text{НОД}(n, \beta) = \frac{n}{m}$$

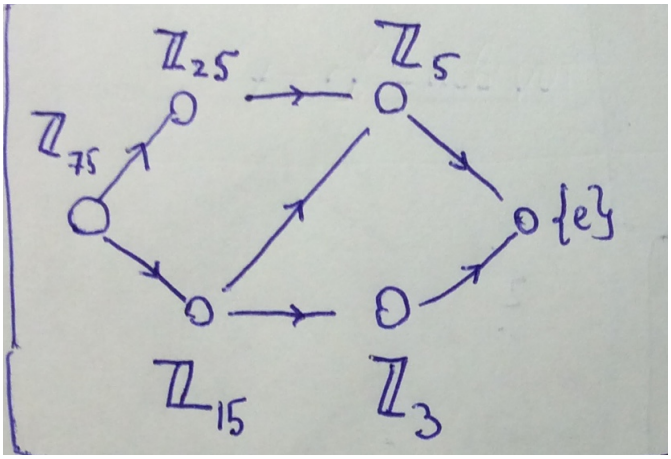
для некоторого m. Нетрудно понять, что в таком случае $H = \{e, g^\beta, g^{2\beta}, \ldots, g^{(m-1)\beta}\}$, то есть состоит из m элементов, таким образом в случае $|H| = k$ мы получаем $m = k$, а значит $\beta = \frac{n}{k}$, и $H = \langle g^{\frac{n}{k}} \rangle$.

Резюмируя, получаем, что структура подгрупп конечной циклической группы совпадает со структурой делителей порядка группы, причем каждому делителя соответствует в точности одна подгруппа. Вообще, это большой подарок судьбы, обычно для произвольной группы структура подгрупп очень сложная.

Пример

Описать граф подгрупп для группы $\mathbb{Z}_{75}$.

Направленный граф подгрупп - это граф, вершинами которого являются подгруппы, а направленным ребром соединяются подгруппы, вложенные друг в друга и между которыми нет промежуточных подгрупп. На самом деле для произвольной группы множество подгрупп наделяется не просто структурой направленного графа, но даже решетки: то есть частично упорядоченного множество (порядок здесь задается вложением подгрупп), где каждое двухэлементное множество $\{A, B\}$ имеет как супремум (в данном случае это будет подгруппа $\langle A, B \rangle$, порожденная A и B) и инфинум (в данном случае им будет $A \cap B$). Как следует из предыдущего утверждения - структура подгрупп полностью восстанавливается по набору делителей, а значит граф подгрупп будет следующим (каждый следующий уровень - это делители, у которых в разложении на один простой сомножитель меньше - потому что именно в этом случае нет промежуточных делителей):



Утверждение

Доказать, что произвольная конечно-порожденная подгруппа $H < \mathbb{Q}$ группы рациональных чисел является циклической.

Доказательство очень похоже на доказательство цикличности подгруппы циклической группы, но немного отличается. Пусть $H = \langle \frac{m_1}{n_1}, \ldots, \frac{m_k}{n_k} \rangle$. Здесь сложно переходить к НОД'у или НОК'у дробей, потому что неясно, что это такое. Зато можно рассмотреть $N = \text{НОК}(n_1, \ldots, n_k)$ и заметить, что

$$H < \left\langle \frac{1}{N} \right\rangle$$

Таким образом $H \cong \mathbb{Z}$ как подгруппа циклической группы $\left\langle \frac{1}{N} \right\rangle$ (хотя мы и не смогли получить явной формы для порождающего элемента).

Замечания:

• *Мастерам теории чисел предлагается подумать над тем, можно ли получить явную формулу для порождающего элемента в таком случае.*

• *Также стоит отметить, что несмотря на то, что в $\mathbb{Q}$ и в $\mathbb{Z}$ одинаковые конечно-порожденные подгруппы (каждая такая подгруппа циклическая в обеих группах) - сами они неизоморфны: $\mathbb{Q} \ncong \mathbb{Z}$ хотя бы потому, что в группе рациональных чисел есть "деление" на любое натуральное число (скажем, 2 для определенности), а группе $\mathbb{Z}$ такое деление возможно не для всех элементов. Пусть вас не пугает операция деления, несмотря на то, что в абелевой записи есть только операция сложения: ведь операцию умножения на натуральное число можно записать в терминах сложения, а операция деления - обратная к умножению, более формально: различающим инвариантом в данном случае является разрешимость уравнения $x + x = y$ для любого y (при использовании аддитивной записи, в мультипликативной записи это уравнение будет выглядеть как $x^2 = y$, иными словами в группе можно извлекать квадратные корни); из анализа разрешимости этого уравнения также вытекает, что группа $\mathbb{Q}$ с операцией сложения неизоморфна группе $\mathbb{Q}^*$ ненулевых рациональных чисел с операцией умножения: опять-таки, потому что в $\mathbb{Q}$ уравнение $x+x = y$ разрешимо для любого y, тогда как его мультипликативная форма $x^2 = y$ в $\mathbb{Q}^*$ неразрешима для $y = 2$. Разрешимость некоторых уравнений как инвариант очень сильный, особенно в абелевом случае. К примеру, есть набор очень похожих на $\mathbb{Q}$ групп:*

$$\mathbb{Z}\left[\frac{1}{N}\right] = \left\{ \frac{m}{N^k} : m, k \in \mathbb{Z} \right\}$$

операция в этой группе - сложение. Ясно, что по построению группа $\mathbb{Z}\left[\frac{1}{N}\right]$ допускает деление на N, однако не допускает деления, скажем, на $N + 1$, иными словами, невозможно найти такой $x \in \mathbb{Z}\left[\frac{1}{N}\right]$, чтобы $(N + 1)x = 1$, а значит неизоморфна группе $\mathbb{Q}$, несмотря на то, что очень сильно на нее похожа. Из этих же соображений, в частности, вытекает, что:

$$\mathbb{Z}\left[\frac{1}{2}\right] \ncong \mathbb{Z}\left[\frac{1}{3}\right]$$

• *В теории групп есть такое немаловажное понятие как ранг Прюффера, обычным рангом $d(H)$ называется минимальное число порождающих группы H, а рангом Прюффера называют:*

$$\mathrm{rk}(G) = \sup_H d(H)$$

где супремум берется по всем конечно-порожденным подгруппам $H < G$. Предыдущее утверждение фактически показывает, что $\mathrm{rk}(\mathbb{Q}) = 1$. То есть несмотря на то, что сама группа является бесконечно-порожденной, но в некотором смысле она очень похожа на однопорожденную.

• *Также хочу предостеречь от напрашивающейся аналогии ранга $d(G)$ с размерностью из линейной алгебры. Хотя размерность линейного подпространства всегда меньше размерности объемлющего пространства и хотя кажется, что $d(G)$ - это мерило того, насколько группа "большая" (что логично: чем больше порождающих - тем больше группа) - но такие доводы в корне неверные, даже типично, что ранг подгруппы больше ранга объемлющей группы. Например, мы с вами помним, что S_n порождается двумя перестановками для любого n, и при этом, как мы покажем далее, любая конечная группа вкладывается в S_n для некоторого n. Тогда если взять некоторую группу ранга k, например, $G = \mathbb{Z}_2^k$ (для того, чтобы понять почему $d(G) = k$ нужна теория конечных абелевых групп, но если в двух словах - то эта группа одновременно является и линейным пространством потому что $\mathbb{Z}_2$ это поле, а потому для нее $d(G) = \dim(G) = k$), но при этом она вкладывается в S_{2^k}, для которой $d(S_{2^k}) = 2$.*

Но несмотря на это, из определения очевидно вытекает, что ранг Прюффера подгруппы всегда не превосходит ранга Прюффера объемлющей группы, а потому его можно считать более разумным и естественным аналогом размерности в теории групп. Попробуйте вычислить ранг Прюффера для известных вам групп, например, для S_n при небольших n.

Задача

Пусть $H_i < G$. Верно ли, что следующие множества являются подгруппами:

- *$H_1 \cap H_2 < G$?*
- *$H_1 \cup H_2 < G$?*
- *$H_1H_2 = \{gh : g \in H_1, h \in H_2\} < G$?*

---

1) Ответ ДА. Если рассмотреть произвольные $x, y \in H_1 \cap H_2$, то раз они лежат в H_1, то и $xy \in H_1$. Так как здесь H_1 и H_2 равноправны, то $xy \in H_2$. Таким образом $xy \in H_1 \cap H_2$. Замкнутость относительно взятия обратного проверяется аналогично. Также ясно, что $e \in H_1 \cap H_2$, если $e \in H_i$.

2) Ответ НЕТ. В этом случае контрпримеры лежат на каждом углу, рассмотрим дл я определенности $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ и $H_1 = \mathbb{Z}_2 \times \{0\}$, $H_2 = \{0\} \times \mathbb{Z}_2$. Тогда $H_1 \cup H_2 = \{(0,0), (1,0), (0,1)\}$, что не является подгруппой, так как $(1,0) + (0,1) = (1,1) \notin H_1 \cup H_2$.

3) Ответ НЕТ. Первый разумный шаг - это рассмотреть произвольные $x, y \in H_1H_2$, то есть $x = g_1h_1$, $y = g_2h_2$, но для произведения $xy = g_1h_1g_2h_2$ мы не сможем переставить местами h_1 и g_2, чтобы слева все было из H_1, а справа из H_2. Но в этом случае контрпример будет построить чуть сложнее, так как в случае, если одна из подгрупп нормальна, то H_1H_2 будет подгруппой (потому что если, скажем, H_1

нормальна, то $xy = g_1(h_1g_2h_1^{-1})h_1h_2$ и $g_1(h_1g_2h_1^{-1}) \in H_1$, а $h_1h_2 \in H_2$). Поэтому отбрасываем в сторону надежды на абелевы группы и рассмотрим, к примеру, $G = S_3$, и пусть $H_1 = \langle(12)\rangle$, $H_2 = \langle(13)\rangle$. Тогда $|H_i| = 2$, значит $|H_1H_2| \leq 4$ (так как всевозможных пар всего 4, но некоторые соответствующие парам произведения могут совпасть). Но при этом, если бы H_1H_2 было подгруппой G, то вместе с каждым набором элементов в H_1H_2 лежало бы их произведение. Однако мы помним, что (12) и (13) порождают S_3, значит $S_3 = H_1H_2$, то есть $|H_1H_2| = 6$ - противоречие.

Подумайте над тем, можно ли придумать пример подгрупп $H_i < G$, чтобы теоретико-множественное произведение H_1H_2 не было замкнуто относительно взятия обратного (в предыдущем пункте мы построили пример незамкнутости относительно умножения, что достаточно для того, чтобы H_1H_2 не была подгруппой). Сгодится ли этот же пример?

Утверждение

Пусть $|G| = 2n$. Доказать, что найдется $g \in G$, такой что $g^2 = e$.

Классическая задачка: рассмотрим разбиение G на пары $\{x, x^{-1}\}$ по всевозможным x. Для e это множество состоит из одного элемента. Таким образом:

$$|G| = 1 + \sum_{x \neq e} \#\{x, x^{-1}\}$$

Таким образом, раз порядок группы четен, то найдется такой x, что $\#\{x, x^{-1}\} = 1$, иными словами $x = x^{-1}$ или что то же самое $x^2 = e$.

==========

Теорема Лагранжа

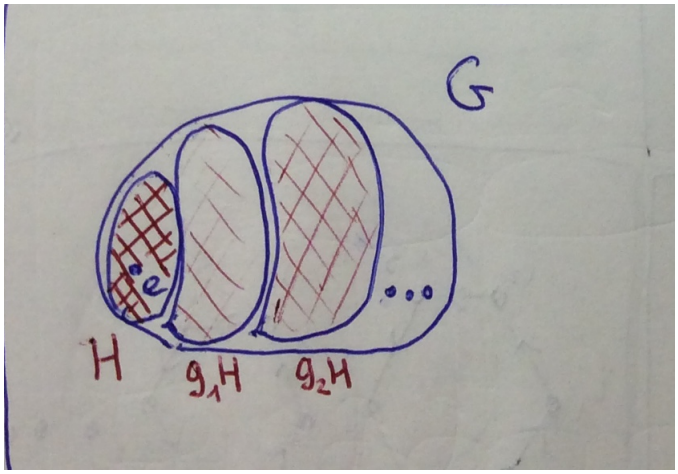
Эта теорема вместе со связанной с ней конструкцией разбиения группы на смежные классы - одна из ключевых во всей теории групп, которая в некотором смысле означает что вместе с групповыми операциями на любой группе есть некоторая скрытая структура (ее можно понимать по разному - это и связь структуры подгрупп с делителями порядка группы, это и в некотором смысле естественное действие группы на множестве левых смежных классов: конструкция, которая работает даже в случае бесконечных групп). Все это дает возможность делать заключительные мазки в общей картине любого доказательства или совершать в ней существенный идейный рывок.

Теорема Лагранжа базируется на наблюдении, что если $H < G$, то для любых $x, y \in G$ множества xH и yH либо не пересекаются, либо совпадают. Действительно, пусть $xH \cap yH \neq \emptyset$. Пусть $g \in xH \cap yH$, тогда $g = xh_x = yh_y$ для некоторых $h_x, h_y \in H$. А значит $x = yh_yh_x^{-1}$ и $xH = yh_yh_x^{-1}H = yH$ так как $hH = H$ для любого $h \in H$. Аналогично рассуждая мы приходим к элементарному и очень важному утверждению, которое будем многократно использовать в дальнейшем:

$$\boxed{xH = yH \qquad \Longleftrightarrow \qquad y^{-1}x \in H}$$

Мы только что доказали $\Rightarrow$, докажем $\Leftarrow$. Действительно, так как $x \in yH$, то $xH \subset yH \cdot H = yH$. С другой стороны $x = yh$ для некоторого $h \in H$, то есть $y = xh^{-1}$, а значит $yH = xh^{-1}H \subset xH$.

Таким образом для произвольной $H < G$ вся группа G как множество разбивается на непересекающиеся множества вида xH, которые называются *левыми смежными классами по* H:



Группу также можно разбить на *правые смежные классы*, а именно на множества вида Hx, их теорию можно построить в дословной аналогии, их свойства дублируют свойства левых смежных классов, хотя иногда в конкретных задачах принципиально с правыми или левыми смежными классами мы работаем, а иногда приходится работать одновременно с обоими (например, в задаче про нормальность подгруппы индекса два). Множество левых смежных классов обозначается

$$G/H = \{xH\}_{x\in G}$$

множество правых смежных классов $H\backslash G = \{Hx\}_{x\in G}$. Есть еще такое понятие, как двойные смежные классы: это множества вида xHy.

Нетрудно заметить, что левое умножение $\lambda_g : G \to G$, $\lambda_g(x) = gx$ является биекцией, а потому $|gH| = |H|$ (два множества имеют одинаковые мощности; отметим, что это утверждение информативно и в случае бесконечного $|H|$, иными словами не может быть одно счетно, а другое - несчетно). Таким образом мы приходим к:

$$|G| = |G/H||H|$$

Мощность множества смежных классов по H называют *индексом подгруппы* H и обозначают $[G : H] = |G/H|$. В случае конечной G мы получаем:

Теорема (Лагранжа)
Пусть $|G| < \infty$*, тогда порядок любой подгруппы* $H < G$ *делит порядок группы* G*.*

Важное следствие из теоремы Лагранжа
Порядок конечной группы G *делится на порядок любого элемента* $g \in G$*. Это следует из того факта, что* $\mathrm{ord}(g)$ *совпадает с порядком циклической подгруппы* $\langle g\rangle$*.*

Эти два утверждения накладывают очень жесткие ограничения на порядки элементов и порядки подгрупп; при необходимости описать все подгруппы подобно ситечку теорема Лагранжа оставляет для анализа лишь отдельные случаи. С частным случаем этой теоремы мы встречались раньше: когда изучали структуру подгрупп конечной циклической группы и показали, что не только порядок каждой

подгруппы делит порядок группы $\mathbb{Z}_n$, но и для каждого делителя n существует (и даже единственная) подгруппа с заданным порядком. В общем случае такое обращение теоремы Лагранжа неверно: к примеру в A_4 не существует подгруппы порядка 6, хотя 6 и является делителем порядка группы.

Замечание:

К понятию порядка группы очень идейно близко понятие экспоненты группы (или периода группы), определяемое как:

$$\exp(G) = \min\{n : g^n = e \text{ для любого } g \in G\}$$

И если бы мощность не называлась в теории групп порядком, то именно эту величину логично и осмысленно было назвать порядком группы. Легко понять, что $\exp(G) = HOK\{\mathrm{ord}(g)\}_{g\in G}$ *(так как чтобы при возведении в степень любого элемента мы получали единицу - эта степень должна делиться на порядок этого элемента, т.е. быть кратным порядку каждого элемента группы. Если мы хотим получить наименьшее такое n - то это в точности HOK). Таким образом, раз* $|G|$ *делится на* $\mathrm{ord}(g)$ *для любого* g*, то* $|G|$ *делится на* $\exp(G)$*. Экспонента не обязана совпадать с порядком: например,* $|S_4| = 24$*, тогда как* $\exp(S_4) = 12$ *(перебором всех циклических типов получаем, что в 12 степени любая перестановка становится тривиальной). Или более простой пример* $G = \mathbb{Z}_2 \times \mathbb{Z}_2$*, где* $|G| = 4$*, но при этом* $\exp(G) = 2$*.*

Задача

Описать левые смежные классы по подгруппе (и найти индекс) в следующих случаях:

- S_3 *по* $\langle(12)\rangle$*.*
- S_n *по* A_n*.*
- $\mathbb{C}^*$ *по* $\mathbb{R}^*$ *(ненулевые комплексные и вещественные числа по умножению).*
- $GL_n(F)$ *по* $SL_n(F)$ *(где* F *- некоторое поле).*

---

1) Из формулы $|G| = |G/H||H|$ получаем, что $[S_3 : \langle(12)\rangle] = 3$, а потому достаточно просто найти три различных левых смежных класса - и из этой формулы получится, что других быть не может. Одним из смежных классов всегда является исходная подгруппа. Умножая этот цикл на рандомные перестановки находим еще два отличных от этого левых смежных классов:

$$e\langle(12)\rangle = \{e, (12)\}$$

$$(13)\langle(12)\rangle = \{(13), (123)\}$$

$$(23)\langle(12)\rangle = \{(23), (132)\}$$

Замечу, что вычисление $(23)\langle(12)\rangle$ фактически можно было не проводить, так как всегда $g \in gH$, а значит раз (23) не было в предыдущих двух классах, то $(23)\langle(12)\rangle$ искомый последний третий класс, который состоит в точности из всех оставшихся перестановок. Такой вот крошечный лайфхак.

2) Так как $|S_n| = n!$, а $|A_n| = n!/2$, то $[S_n, A_n] = 2$, а потому:

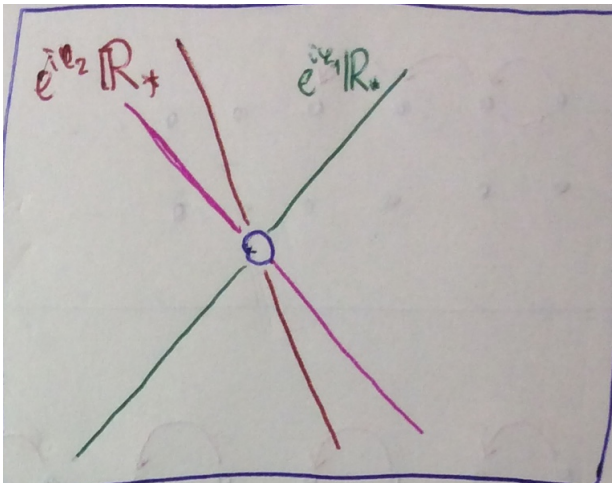
$$S_n = A_n \sqcup (12)A_n$$

потому что всего два класса, а A_n и $(12)A_n$ не могут совпадать, так как $(12) \notin A_n$.

3) Следующие два пункта решаются немного по-другому: вместо перебора до тех пора, пока не накопим смежных классов в количестве индекса - у нас будет возможность структурно описать эти классы, и мы ею воспользуемся:

$$x\mathbb{R}^* = re^{i\varphi}\mathbb{R}^* = e^{i\varphi}\mathbb{R}^* = \{z \neq 0 : \arg(z) = \varphi \text{ или } \varphi + \pi\}$$

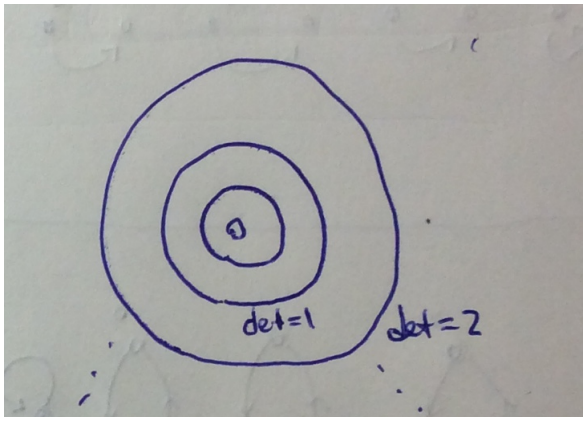
где $x = re^{i\varphi}$, таким образом в данном любой смежный класс - это проходящая через 0 прямая без 0. Индекс будет равен мощности $[0, \pi)$, т.е. континуальный.



4) Докажем следующее равенство.

$$gSL_n(F) = \{x \in GL_n(F) : \det(x) = \det(g)\}$$

Ясно, что если $x = gs$, где $s \in SL_n(F)$, то $\det(x) = \det(g)\det(s) = \det(g)$, то есть верно $\subset$. Теперь пусть $x \in \{x \in GL_n(F) : \det(x) = \det(g)\}$. Заметим, что $x = g(g^{-1}x)$, где $\det(g^{-1}x) = \det(g^{-1})\det(x) = 1$, таким образом $g^{-1}x \in SL_n(F)$, то есть доказали $\supset$. Таким образом, произвольный левый смежный класс в данном случае является множеством обратимых матриц с фиксированным определителем. Геометрически это можно представлять как расслоение пространства без 0 на сферы.



Индекс в данном случае будет равен $[GL_n(F) : SL_n(F)] = |F^*| = |F| - 1$. Действительно: любая обратимая матрица имеет ненулевой определитель. И обратно: для любого ненулевого числа $f \neq 0$ существует обратимая матрица с таким определителем, например $g = \mathrm{diag}(f, 1, \ldots, 1)$. Таким образом классов столько же, сколько и ненулевых чисел.

Задача

Описать все группы G порядка 1000000007.

Поверите вы или нет, но $q = 1000000007$ является простым числом. Рассмотрим произвольный неединичный $g \in G$. По теореме Лагранжа $\mathrm{ord}(g)$ делит порядок группы. Так как этот порядок является простым числом, то либо $\mathrm{ord}(g) = 1$, что невозможно, так как рассматривали неединичный элемент, либо $\mathrm{ord}(g) = q$, но тогда циклическая подгруппа $\langle g \rangle$ имеет такой же порядок как и G, а значит совпадает со всей группой, то есть:

$$G = \langle g \rangle \cong \mathbb{Z}_{1000000007}$$

Замечание:

Отмечу, что эти рассуждения, разумеется, работают для любого простого числа, а не только этого. Запомните, это очень важный факт: что группа простого порядка обязана быть циклической.

Вызовем на сцену и попросим представиться и рассказать немного о себе нашего нового друга:

==========

Группа Кватернионов

==========

Группа состоит из 8 элементов:

$$Q_8 = \begin{Bmatrix} 1 & i & j & k \\ -1 & -i & -j & -k \end{Bmatrix}$$

таблица умножения строится так, что ± 1 коммутируют с любым элементом, $i^2 = j^2 = k^2 = -1$ и $ijk = -1$. Из этих соотношений можно вывести любое другое соотношение между элементами (что можно более строго сформулировать, как задание группы копредставлением, что мы подробно будем разбирать чуть позже):

$$G = \left\langle -1, i, j, k | (-1)^2 = 1, [(-1), i] = [(-1), j] = [(-1), k] = 1, i^2 = j^2 = k^2 = ijk = -1 \right\rangle$$

Острой необходимости сейчас в копредставлении для группы кватернионов нет, так как в силу специфики группы (что 1 тождественен, а -1 со всеми коммутирует) групповое умножение достаточно задать лишь на буквах i, j, k, а их попарные произведения легко вычисляются с использованием "базисного" соотношения $ijk = -1$. Правда тогда остается вопрос, почему построенное умножение будет удовлетворять всем аксиомам группы: чтобы избежать большого перебора - проще всего реализовать группу кватернионов как подгруппу некоторой известной группы, для которой аксиомы уже проверены. Например, группу кватернионов можно реализовать как подгруппу $GL_2(\mathbb{C})$, где порождающими будут:

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$k \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Напомню, что комплексные числа можно реализовать вещественными матрицами:

$$a + bi \qquad \longleftrightarrow \qquad \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

так, что сумме и произведению комплексных чисел будет соответствовать сумма и произведение соответствующих матриц (пафос именно в произведении, так как если бы вы просто хотели, чтобы сумма уважалась - можно было бы рассмотреть простой вектор (a, b)). И здесь мы фактически следуем этой же идее но уже для группы кватернионов. Кстати, если каждое комплексное число в $GL_2(\mathbb{C})$ по этой конструкции заменить на вещественную 2×2 матрицу, то можно считать, что группу кватернионов мы реализовали в группе $GL_4(\mathbb{R})$.

Я покажу, как перемножать элементы, используя "базисные" соотношения, на двух примерах (по максимуму выделяя где это возможно ijk):

$$ij = -(ijk)k = k$$

$$ki = kijkk^{-1}j^{-1} = k(ijk)(-k)(-j) = -kkj = j$$

Некоторые свойства я советую запомнить: $\tau^3 = -\tau$ для любой буквы τ, а также, что произведение $\tau\lambda$ двух различных букв всегда равно плюс/минус оставшейся букве; причем произведение в другом порядке меняет знак, т.е.

$$\tau\lambda = \pm\delta$$

$$\lambda\tau = \mp\delta$$

Группа не является коммутативной, так как буквы не коммутируют.

Группа эта возникла как "скелет" кватернионного пространства

$$\mathcal{Q} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

являющегося обобщением комплексных чисел и играющего большую роль как в алгебре (есть теорема, что существует всего 3 конечномерных алгебры над $\mathbb{R}$ с делением: $\mathbb{R}$, $\mathbb{C}$ и $\mathcal{Q}$, а если пожертвовать ассоциативностью умножения, то в список добавится еще и алгебра октав $\mathcal{O}$); так и в геометрии: практика показывает, что в 3D-моделировании очень удобно повороты пространства выражать через кватернионы, так как композиции операторов соответствует произведение соответствующих кватернионов. Элементы i, j, k по понятным причинам называются мнимыми единицами.

Пример

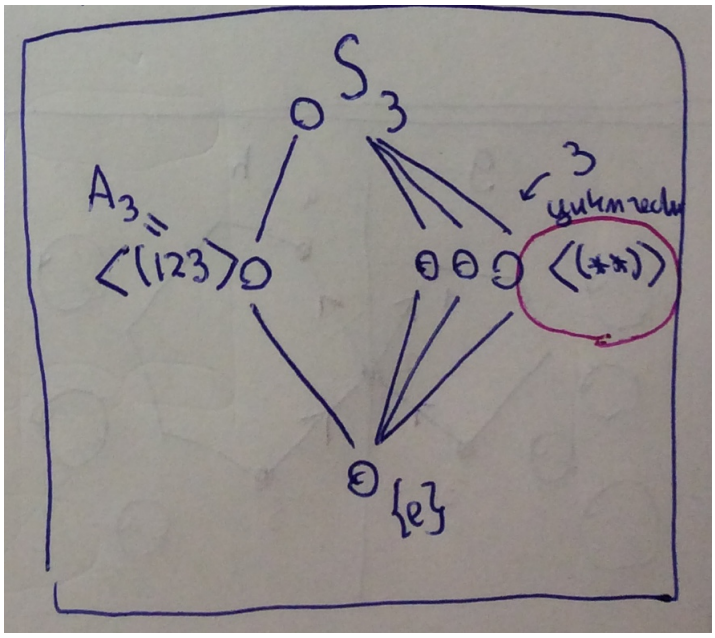
Найти все подгруппы для групп S_3, Q_8 и A_4 (и построить граф подгрупп).

Процесс поиска всех подгрупп не очень алгоритмизирован. Всегда есть две тривиальные подгруппы - единичная и вся группа. Дальше обычно перечисляют все циклические подгруппы - их проще всего найти - каждый элемент порождает свою циклическую подгруппу (они, правда, иногда совпадают). Имея колоссальные вычислительные мощности и возможности можно попытаться добавлять порождающие к уже имеющимся подгруппам и смотреть, какие новые подгруппы будут появляться, и продолжать этот переборного типа процесс, пока не доберемся до всей группы. Однако перебор там нечеловечески большой, обычно с помощью теоремы Лагранжа составляют набор допустимых порядков для подгрупп, приводят бросающиеся в глаза подгруппы заданного порядка, а дальше пытаются доказать, что нет других. Наиболее универсальный и полезный вопрос, с которого советую начинать поиск подгрупп заданного порядка: "а какие элементы могут лежать в нашей гипотетической подгруппе?".

1) В этом случае все совсем просто: $|S_3| = 6$, у 6 только два нетривиальных делителя 2 и 3, которые являются простыми числами, а значит любая нетривиальная подгруппа циклическая, а любая циклическая подгруппа имеет вид: $\{e, g, g^2, \ldots\}$. Таким образом полный список подгрупп следующий:

$$\{\{e\}, S_3, \langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle, \langle(123)\rangle\}$$

а граф подгрупп будет таким:



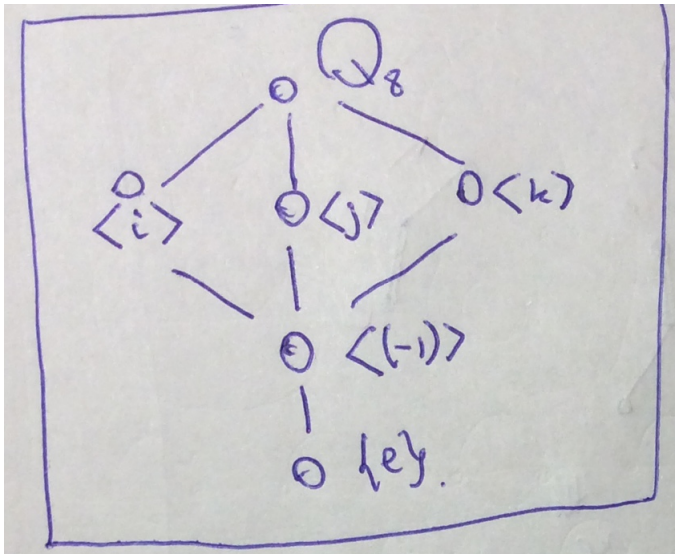
Замечу, что $\langle(123)\rangle = \langle(132)\rangle$, т.е. $a = (123)$ и $b = (132)$ порождают одну и ту же циклическую подгруппу, так как $a^2 = b, b^2 = a$, либо можно заметить, что $(132) \in \langle(123)\rangle$, а циклическую подгруппу простого порядка порождает любой ее неединичный элемент (это вытекает из теоремы Лагранжа: его порядок должен быть делителем порядка группы, а так как он простой, то совпадать с ним).

2) $|Q_8| = 8$, среди нетривиальных делителей есть не только простые числа, а потому не все так просто. Заметим, что по теореме Лагранжа порядок любой подгруппы может быть равен $1, 2, 4, 8$. Случай 1 и 8 - это тривиальные случаи. Далее: 2 - простое число, а потому могут быть только циклические подгруппы заданного порядка, эти подгруппы порождаются элементом порядка два, а он такой один - это (-1).

Осталось разобрать случай 4. Во-первых, есть циклические подгруппы порядка 4, их всего 3 штуки: $\langle i\rangle, \langle j\rangle, \langle k\rangle$. С другой стороны других подгрупп быть не может, действительно, пусть $H < Q_8$ и $|H| = 4$. Тогда в $|H|$ обязана лежать какая-нибудь мнимая единица $\pm\tau$ (так как всего 2 элемента, отличных от плюс/минус мнимых единиц - это 1 и (-1): и из них подгруппу порядка 4 не набрать). Но она тянет за собой всю порожденную собой подгруппу: $\{1, (-1), \tau, -\tau\}$, где уже 4 элемента. Значит кроме циклических подгрупп порядка 4 нет, и полный список подгрупп будет таким:

$$\{\{e\}, Q_8, \langle(-1)\rangle, \langle i\rangle, \langle j\rangle, \langle k\rangle\}$$

а граф подгрупп будет таким:



Интересно получается, что у нее все нетривиальные подгруппы циклические, т.е. она в некотором смысле напоминает циклическую группу (мы помним, что они тоже обладали этим свойством), но сама таковой не является.

3) $|A_4| = 12$, делители порядка группы - это 1,2,3,4,6,12. Случаи 1,12 - тривиальные ситуации. 2,3 - простые числа, а потому в этом случае возможны только циклические подгруппы, порожденные элементами порядков 2,3 соответственно.

Пусть теперь $H < A_4$ и $|H| = 4$. Заметим, что по теореме Лагранжа порядок любого элемента $h \in H$ должен быть степенью двойки. Значит H будет состоять из таких элементов, но в A_4 всего 4 элемента, у которых порядок является степенью двойки: e и 3 элемента с циклическим типом (**)(**). Таким образом других элементов в подгруппе H быть не может, а значит:

$$H = \{e, (12)(34), (13)(24), (14)(23)\}$$

Но на это анализ подгрупп порядка 4, разумеется. не заканчивается: нужно еще проверить, что это действительно подгруппа, т.е. что это множество замкнуто

относительно умножения: проверяем и убеждаемся. На самом деле перебор получится очень небольшой: так как в квадрате каждый такой элемент дает e и в силу равноправия ситуации при перемешивании чисел $\{1,2,3,4\}$ - достаточно лишь проверить, что произведение любых двух элементов даст третий. Для этой подгруппы есть специальное обозначение: V_4. Так как произведение любых двух нетривиальных элементов дает третий (вне зависимости от порядка), то V_4 - абелева, более того $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (так как у них совпадают таблицы умножения). Как самостоятельная группа а также как подгруппа A_4, группа V_4 является довольно хорошим источником вдохновения для построения самых разных контрпримеров.

И теперь самое сложное: докажем, что в A_4 нет подгрупп порядка 6. Есть несколько классических способов, как это можно сделать с помощью теории нормальных подгрупп, но мы пойдем с вами тяжелым путем применения кустарных методов. Пусть $H < A_4$ и $|H| = 6$. В H по-любому будет лежать e. Также в A_4 всего 4 элемента, не являющихся циклом длины 3 (это в точности элементы V_4), а потому в H будет лежать какой-нибудь цикл длины 3, можно перенумеровать индексы и считать, что это (123), вместе с ним и $(132) = (123)^2$. Осталось найти еще 3 элемента. Помним, что в группе четного порядке всегда есть элемента порядка 2, а значит присутствует и перестановка σ циклического типа $(**)(**)$, так как только у такого типа порядок равен 2. Рассмотрим теперь $\omega = \sigma(123)\sigma^{-1}$. По волшебной формуле для сопряжения $\omega = (\sigma(1)\sigma(2)\sigma(3))$, причем σ не оставляет на месте ни одного элемента, а потому в этом тройном цикле ω присутствует 4, таким образом $\{\omega, \omega^2\}$ - новые элементы, таким образом набрали необходимые 6 элементов:

$$H = \{e, (123), (132), \sigma, \omega, \omega^2\}$$

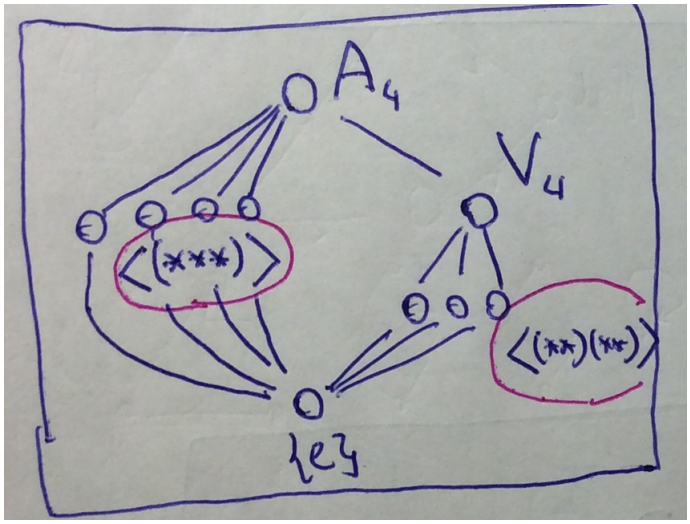
Докажем, что они не образуют подгруппу. И здесь я не вижу другого выхода кроме перебора. Так как элементов типа $(**)(**)$ меньше элементов типа $(***)$, то попробую перебирать элементы первого типа. Ясно, что $(123)\sigma(123) = \sigma$, так как при сопряжении циклический тип должен сохраниться с одной стороны, а другой стороны в нашей гипотетической подгруппе всего один элемент с таким циклическим типом, и это σ. Перебор:

$$\sigma = (12)(34) \qquad \Longrightarrow \qquad (123)\sigma(123)^{-1} = (23)(**) \neq \sigma$$

$$\sigma = (13)(24) \qquad \Longrightarrow \qquad (123)\sigma(123)^{-1} = (21)(**) \neq \sigma$$

$$\sigma = (14)(23) \qquad \Longrightarrow \qquad (123)\sigma(123)^{-1} = (24)(**) \neq \sigma$$

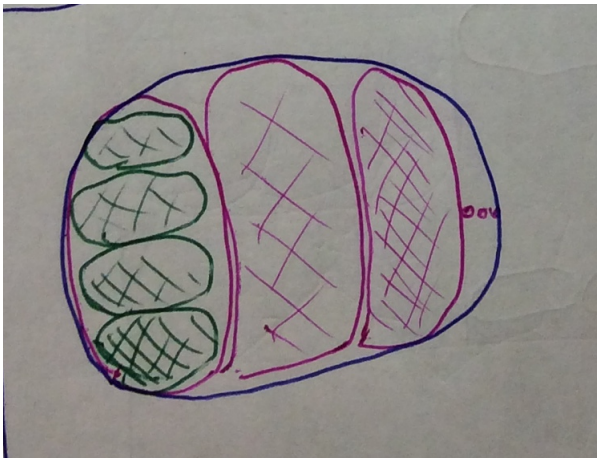
В каждой из ситуаций соответствующие перестановки различны из-за того, что они как минимум на одном элементе действуют различно. Также замечу, что перестановки из A_4 циклического типа $(**)(**)$ восстанавливаются по одному из своих циклов - так как второй цикл переставляет оставшиеся два элемента, так что звездочки можно моментально восстановить, хотя и в этом нет необходимости. Таким образом, приходим к противоречию, так как обнаружился седьмой элемент. Граф подгрупп таким образом будет следующий:



Утверждение

Доказать "tower law of subgroups", а именно если $[G : H] = n$, $[H : K] = m$, *то* $[G : K] = nm$.

Очень простое утверждение. Если неформально, то всего n штук H-сосисок, в каждой из которых умещается m штук маленьких K-сосисок, итого маленьких сосисок будет mn-штук.



Формально:

$$G = \coprod_i g_i H$$

$$H = \coprod_j h_j K$$

для некоторых задающих непересекающиеся смежные классы представителей g_i и h_j. Тогда:

$$G = \coprod_i g_i H = \coprod_i g_i \left(\coprod_j h_j K \right) = \coprod_{i,j} g_i h_j K$$

Все смежные классы из самой правой части равенства различны, так как если $g_i h_j K = g_I h_J K$, то $i = I$ (так как мы выбирали из каждого класса по одному

представителю, а значит $g_iH = g_IH$ iff $i = I$); таким образом $h_jK = h_JK$. Опять же в силу выбора по одному представителю из каждого класса получаем $j = J$.

Утверждение

Пусть $[G : H] = m$, $[G : K] = n$. *Доказать, что*

$$HOK(m, n) \leq [G : H \cap K] \leq nm$$

Докажем неравенство НОК $(m, n) \leq [G : H \cap K]$. Для этого применим tower law к двум башням $G > H > H \cap K$ и $G > K > H \cap K$:

$$[G : H \cap K] = m[H : H \cap K]$$

$$[G : H \cap K] = n[K : H \cap K]$$

Получается, что $[G : H \cap K]$ - некоторое кратное m, n, а так как НОК - это наименьшее общее кратное, то НОК $(m, n) \leq [G : H \cap K]$.

Второе неравенство: заметим, что $x(H \cap K) = xH \cap xK$. Так как $[G : H] = m$, а $[G : K] = n$, то всего mn возможных пар (xH, yK), ясно, что их всевозможных пересечений $xH \cap yK$ не больше mn (может быть меньше, потому что некоторые пары могут дать пустое пересечение. Замечу, что при условии непустоты из $xH \cap yK = \tilde{x}H \cap \tilde{y}K$ вытекает $xH = \tilde{x}H$ и $yK = \tilde{y}K$, так как смежные классы дизъюнктны), таким образом всевозможных $x(H \cap K) = xH \cap xK$ тем более не больше mn. Таким образом $[G : H \cap K] \leq mn$.

Замечания

• *Это довольно полезное утверждение, на практике его часто используют. В частности получается, что если* m, n- *взаимно просты, то* $HOK(m, n) = mn$, *а значит смежных классов* mn - *максимальное возможное, иными словами каждый* H-*класс пересекается с каждым* K-*классом. Интуитивно геометрически это означает, что* H *и* K *находятся в* G *в общем положении, т.е. практически как прямые сомножители. Интересно, что это наблюдение можно сделать лишь на основании взаимной простоты индексов без каких бы то ни было предположений касательно структуры группы или подгрупп.*

• *Чтобы понять, что бывают случаи, когда* $[G : H \cap K] \neq mn$ *достаточно рассмотреть случай* $H = K$. *В этом случае* $[G : H \cap K] = [G : H] = n \neq n^2$, *так что без дополнительных предположений улучшить границы этих неравенств невозможно.*

• *Из этого утверждения в частности вытекает, что пересечение любых смежных классов* $xH \cap yK$ *является некоторым смежным классом по* $H \cap K$ *в случае взаимной простоты индексов и конечной группы* G. *Действительно, рассмотрим:*

$$\Omega = \{xH \cap yK : xH \in G/H, yK \in G/K\}$$

Ясно, что раз $[G : H] = m$, $[G : K] = n$, *то* $|\Omega| \leq mn$. *С другой стороны, имеем* $x(H \cap K) = xH \cap yH$, *то есть* $G/(H \cap K) \subset \Omega$, *причем* $|G/(H \cap K)| = nm$ *согласно только что доказанному. Таким образом из соображений мощности получаем* $\Omega = G/(H \cap K)$, *т.е. каждое множество* $xH \cap yK$ *будет левым смежным классом по* $H \cap K$.

• *Отмечу, что в доказательстве последнего утверждения (и tower law тоже) мы нигде не использовали предположение конечности группы G, а потому эти утверждения верны и для бесконечных групп. Однако в случае конечной G можно пользоваться теоремой Лагранжа и существенно упростить доказательство tower law:*

$$[G:K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G:H][H:K]$$

Нормальные подгруппы

Определение

Подгруппа $H < G$ называется нормальной (обозначение $H \lhd G$), если $g^{-1}hg \in H$ для всякого $g \in G, h \in H$

Иными словами нормальными являются подгруппы замкнутые относительно сопряжения на элемент из объемлющей группы (выдерживание сопряжения на элементы из H вытекает из определения подгруппы, здесь требуется более сильное условие). Существует несколько эквивалентных почти тавтологически совпадающих определений нормальности:

$$H \lhd G \quad \Longleftrightarrow \quad g^{-1}Hg = H \text{ для всех } g \in G \quad \Longleftrightarrow \quad gH = Hg \text{ для всех } g \in G$$

Вторая эквивалентность получается домножением равенства $g^{-1}Hg = H$ слева на g и наоборот. Что касается первой эквивалентности, то $\Leftarrow$ очевидно, а для доказательства $\Rightarrow$ заметим, что $g^{-1}hg \in H$ для всех $g \in G, h \in H$ фактически означает, что выполнено $g^{-1}Hg \subset H$ для всех $g \in G$, а в частности $gHg^{-1} \subset H$, откуда получаем доказательство обратного вложения:

$$H = g^{-1}(gHg^{-1})g \subset g^{-1}Hg$$

Для проверки нормальности обычно пользуются определением, нежели этими двумя эквивалентными характеризациями, так как работать с элементами проще чем с подмножествами. Также хочется обратить внимание на последнюю характеризацию, которая дословно означает, что только для нормальных подгрупп правые смежные классы совпадают с левыми смежными классами. Для произвольных подгрупп несмотря на сходство и общность свойств правых и левых смежных классов - они различаются.

В отличие от произвольных подгрупп нормальные подгруппы являются более правильной параллелью с подпространствами из линала (мы помним, как разрушились наши представления о возможной аналогии подгрупп с подпространствами, когда мы вводили понятие *ранг подгруппы*), так как для $H \lhd G$ в некотором очень-очень приблизительном смысле $G \approx H \times G/H$, и изучение группы опять же в некотором смысле можно редуцировать к изучению двух групп меньшего

порядка, что в большинстве случаев упрощает исходную задачу. Связана эта возможность с тем, что для $H \lhd G$ множество левых смежных классов естественным образом наделяется структурой группы, о чем мы поговорим далее. Хочется также сделать стилистическое замечание, хорошо сформулированное Кострикиным в его книжке, что говорить "подгруппа не является нормальной" предпочтительнее нежели "подгруппа ненормальная".

Утверждение
Доказать, что если $H < G$ и G абелева, то $H \lhd G$.

Очень простая задача, проверка непосредственная: $g^{-1}hg = h \in H$ для любых $g \in G, h \in H$.

Задача
Доказать, что
- $SL_n(F) \lhd GL_n(G)$
- $A_n \lhd S_n$

---

1) Пусть $h \in SL_n(F), g \in GL_n(F)$, тогда

$$\det(g^{-1}hg) = \det(h) = 1$$

Таким образом, $g^{-1}hd \in SL_n(F)$, что доказывает ее нормальность.

2) Второй пункт доказывается полностью аналогично с заменой определителя det на четность τ.

Эти два примера лишь отголосок более общей картины: а именно, что ядра произвольных гомоморфизмов являются нормальными подгруппами, это мы докажем позже. Более того, любая нормальная подгруппа получается как ядро некоторого гомоморфизма (спойлер: канонического гомоморфизма $G \to G/H$).

У произвольной группы G существуют две естественные и очень важные нормальные подгруппы: это *центр* и *коммутант*:

$$\boxed{\begin{gathered} Z(G) = \{x \in G : xg = gx \text{ для всех } g \in G\} \lhd G \\ [G,G] = \{[x_1,y_1][x_2,y_2]\dots[x_n,y_n] : x_i, y_i \in G\} = \langle [x,y] \rangle_{x,y \in G} \lhd G \end{gathered}}$$

Покажем их нормальность, для центра $h \in Z(G), g \in G$:

$$g^{-1}hg = h \in Z(G)$$

Для коммутанта в первую очередь заметим, что

$$g^{-1}[x,y]g = g^{-1}(xyx^{-1}y^{-1})g = (g^{-1}xg)(g^{-1}yg)(g^{-1}xg)^{-1}(g^{-1}yg)^{-1} = [g^{-1}xg, g^{-1}yg]$$

А значит для произвольного $\omega = [x_1,y_1]\dots[x_n,y_n] \in [G,G]$ и $g \in G$ имеем:

$$g^{-1}\omega g = [g^{-1}x_1g, g^{-1}y_1g]\dots[g^{-1}x_ng, g^{-1}y_ng] \in [G,G]$$

Все это должно напомнить линейную алгебру, в которой, мы помним, сопряжение уважает все существующие операции и все свойства объектов, потому что

сопряжению соответствует переход в другой базис: объект остается тем же, только меняется угол зрения на него. Иногда используют обозначение $x^g = g^{-1}xg$ - это настоящая находка для компактификации текста, когда очень много сопряжений; но очень сильно режет глаза, когда в таком обозначении нет особой необходимости.

Замечание:

Интуитивно центр - это "стержень" группы, на который группа нанизывается как шашлык на шампур (причем в группах это заметно чуть менее, чем в других алгебраических структурах, во многих из которых любой объект представляет собой некоторое расслоение над своим центром, к примеру в C^*-алгебрах такая конструкция обеспечивается теоремой Даунса-Хофманна). Если коммутатор элементов - это мерило их некоммутативности, то коммутант группы - это мерило отклонения группы от абелевой, чем больше коммутант - тем менее группа абелева (в абелевом случае коммутант тривиален). Отмечу также, что коммутант - это именно подгруппа, порожденная коммутаторами, а не просто множество коммутаторов, которые обычно не образуют подгруппу, потому что нет никаких поводов, чтобы произведение коммутаторов было некоторым коммутатором - очень многие в этом делают ошибки. В связи с этим рассмотрим следующий:

Классический Пример (Cassidy, 1979)

Привести пример группы G, для которой $[G,G] \neq \{[x,y]\}$.

Пример является очень экзотической модификацией группы Гейзенберга (которой мы с вами еще коснемся, так что описанные далее выкладки не пропадут даром). Пусть F - произвольное поле, а $F[x,y]$ - кольцо многочленов от двух переменных, а $F[x], F[y]$ подкольца многочленов, зависящих только от одной из переменных. Тогда в качестве примера подойдет группа G матриц по умножению вида:

$$\begin{pmatrix} 1 & f(x) & h(x,y) \\ 0 & 1 & g(y) \\ 0 & 0 & 1 \end{pmatrix}$$

где $f \in F[x], g \in F[y], h \in F[x,y]$, такую матрицу мы будем отождествлять с вектором (f,g,h), состоящим из определяющих матрицу функций. Непосредственная проверка показывает, что:

$$(f,g,h)^{-1} = (-f,-g,fg-h)$$

$$(f,g,h)(a,b,c) = (f+a, g+b, h+c+fb)$$

$$[(f,g,h),(a,b,c)] = (0,0,fb-ga)$$

Тогда нетрудно заметить ($\alpha \in F$), что

$$[(\alpha x^k,0,0),(0,y^n,0)] = (0,0,\alpha x^k y^n)$$

А так как $(0,0,h)(0,0,c) = (0,0,h+c)$ умножение на матрицах такого вида есть просто сложение соответствующих многочленов, то раз все элементарные мономы являются коммутаторами, то и любой многочлен автоматически лежит в коммутанте, т.е. $[G,G] \subset \{(0,0,h) : h \in F[x,y]\}$. Обратное включение очевидно вытекает из

вышеупомянутой формулы для коммутатора произвольных элементов группы G. Таким образом:

$$[G, G] = \{(0, 0, h) : h \in F[x, y]\}$$

Однако $(0, 0, x^2 + xy + y^2)$ не является коммутатором, несмотря на то, что лежит в коммутанте. Проверим это, пусть найдутся $f, a \in F[x]$ и $g, b \in F[y]$ (заметим, что значение коммутатора не зависит от третьих координат), что:

$$[(f, g, h), (a, b, c)] = (0, 0, fb - ga) = (0, 0, x^2 + xy + y^2)$$

Пусть $f = \sum f_i x^i$ и $a = \sum a_i x^i$. Тогда, сравнивая многочленные коэффициенты при $1, x, x^2$, получаем:

$$\begin{cases} f_0 b(y) - a_0 g(y) = y^2 \\ f_1 b(y) - a_1 g(y) = y \\ f_2 b(y) - a_2 g(y) = 1 \end{cases}$$

Что невозможно, так как $\{1, y, y^2\}$ линейно независимы и не могут быть линейно выражены через 2 многочлена $g(y)$ и $b(y)$.

Замечание:

Читателям предлагается придумать другие примеры. Вообще, самым простым примером является свободная группа, к примеру $\mathbb{F}_4 = \langle a, b, x, y\rangle$, нетрудные комбинаторные рассуждения показывают, что $[a, b][x, y]$ не является коммутатором никаких элементов. но мы пока не добрались до свободных групп, плюс красивой идейной начинкой примера Cassidy, возможно, вы сможете воспользоваться в других задачах. Что касается конечных групп, то минимальный порядок группы, где такое возможно, равен 96. Причем, существует 2 неизоморфные группы порядка 96, с описанным выше свойством.

По аналогии с группами, порожденными некоторым набором элементов, вводится понятие *нормального замыкания*:

$$\langle\langle M\rangle\rangle = \langle\{g^{-1}mg\}\rangle_{g\in G, m\in M} \lhd G$$

То есть это подгруппа, составленная из всевозможных произведений сопряжений элементов из $M \cup M^{-1}$. нормальной она будет являться по построению. Нетрудно заметить, что $\langle\langle M\rangle\rangle$ является минимальной нормальной подгруппой, содержащей множество M: доказательство дословно копирует аналогичное доказательство для обычных подгрупп. Также любая нормальная подгруппа может быть получена таким образом, ведь для $H \lhd G$ верно $H = \langle\langle H\rangle\rangle$ - есть минимальная нормальная подгруппа, натянутая на H как множество. Однако не скажу, что эта конструкция прямо-таки упрощает картину мира: все-таки даже нормальное замыкание одного элемента $\langle\langle g\rangle\rangle$ устроено крайне сложно и очень далеко от циклических групп за исключением каких-нибудь очень простых случаев.

Пример

Верно ли, что если $K \lhd H$ и $H \lhd G$, то $K \lhd G$?

Несмотря на то, что так хочется ответить "Да", ответ отрицательный. Вообще говоря нет никаких аргументов в пользу того, чтобы нормальность была транзитивной: ведь при сопряжении лишь элементами из H мы не выходим за границу K, а если сопрягать произвольными элементами из G, то максимум,

что мы можем сказать - так это то, что мы не выберемся из H. Но подобных рассуждений в математике недостаточно - нужно приводить контрпример, если мы хотим опровергнуть какое-нибудь утверждение. И в отличие от примера, когда множество коммутаторов не равнялось коммутанту - здесь примеры лежат на самой поверхности: заметим, что $\langle(12)(34)\rangle \lhd V_4$ так как V_4 - абелева, и $V_4 \lhd A_4$ так как циклический тип сохраняется при сопряжении. Но при этом $\langle(12)(34)\rangle$ не является нормальной в A_4 хотя бы потому, что $(123)[(12)(34)](123)^{-1} = (23)(14) \notin \langle(12)(34)\rangle$.

Задача
Пусть $H_i \lhd G$, доказать, что $H_1 \cap H_2 \lhd G$.

То, что пересечение подгрупп является подгруппой - мы уже знаем, нормальность проверяется элементарно: пусть $g \in G$ и $h \in H_1 \cap H_2$, тогда $h \in H_1$, тогда из нормальности получаем $g^{-1}hg \in H_1$, аналогично $g^{-1}hg \in H_2$, значит $g^{-1}hg \in H_1 \cap H_2$.

Утверждение
Пусть $H < G$ и $[G : H] = 2$, доказать, что $H \lhd G$.

Классическая простая задачка: разобьем G на левые и правые смежные классы по H одновременно. Ясно, что $eH = He$. Рассмотрим произвольный $g \notin H$, тогда $gH = Hg$, так как при разбиении что на правые, что на левые смежные классы этот класс не может совпадать с H, а так как индекс равен 2, то и gH, и Hg совпадают с множеством оставшихся элементов $G \backslash H$. Если $g \in H$, то очевидно, что $gH = H = Hg$, таким образом $gH = Hg$ для всякого $g \in G$.
==========

Группа G/H

Как я уже говорил, одним из главных плюсов нормальных подгрупп является наличие групповой структуры на G/H. Если рассмотреть 2 смежных класса (неважно каких, потому что подгруппа нормальна) $xH, yH \in G/H$, тогда используя, что для нормальных подгрупп выполнено $gH = Hg$ для любого g, мы получаем:

$$(xH)^{-1} = Hx^{-1} = x^{-1}H$$

$$(xH) \cdot (yH) = x(Hy)H = xyHH = xyH$$

где операции понимаются как теоретико множественные, т.е. произведение двух множеств - это множество всевозможных произведений. Таким образом, раз операции на этих множествах xH задаются групповыми операциями на соответствующих им представителях x, а в группе выполнены аксиомы группы - то и операции на смежных классах тоже удовлетворяют аксиомам группы.

Фактор G/H может быть вычислен многими способами. Самый универсальный и относительно алгоритмический - с помощью теоремы о гомоморфизме. Для простых случаев иногда достаточно вычислить порядок и отбросить лишние варианты, перемножая бросающиеся в глаза смежные классы и тем самым добывая все новые и новые свойства изучаемой группы.

Важный вопрос: А что мешает для произвольной (не обязательно нормальной) подгруппы $H < G$ определить операции на G/H таким же образом, получится ли группа в таком случае? И несмотря на то, что все аксиомы группы будут выполняться, группой G/H не будет, так как таким образом определенные операции не будут корректными, так как их результат будет зависеть от выбора представителя в смежных классах. Если же для каждого смежного класса xH мы попытаемся намертво зафиксировать его представителя x, то не факт, что эти выборы будут согласованы с групповыми операциями, т.е. не факт, что для класса $(xH) \cdot (yH) = xyH$ мы изначально зафиксировали именно представителя xy. В случае нормальных подгрупп $H \lhd G$ этой проблемы не возникало, так как групповые операции на смежных классах естественно рождались из теоретико-множественных операций на множествах; и хотя корректность проверять не обязательно - я советую ее проверить чисто на групповом языке (т.е. независимость результата от выбора представителя) - так как это является хорошим упражнением на отработку техники работы с нормальными подгруппами.

Возможно, на первых порах психологически сложно будет привыкнуть, что элементы групп вида G/H - это множества, согласен, с этим сложно смириться в одночасье - но нужно привыкать, учиться и исследовать.

Утверждение

Доказать, что $G/[G,G]$ является абелевой группой для любой группы G.

Коммутативность можно проверять либо с помощью коммутаторов, либо с помощью проверки $xy = yx$, здесь удобно первым путем пойти: рассмотрим два произвольных смежных класса $x[G,G]$ и $y[G,G]$ и вычислим их коммутатор, вспоминая, что операции на смежных классов индуцируются групповыми операциями на их представителях:

$$[x[G,G], y[G,G]] = x[G,G]y[G,G](x[G,G])^{-1}(y[G,G])^{-1} = xyx^{-1}y^{-1}[G,G] = [G,G]$$

В G/H смежный класс H является нейтральным элементом, а потому $G/[G,G]$ является абелевой.

Замечания:

• *Группа $G_{ab} = G/[G,G]$ называется абеленизацией группы G и играет большую роль в описании произвольной группы. Например, если абеленизации разные, то и понятно, что группы неизоморфны; или, к примеру, есть много свойств групп, которые "пропускаются" через абеленизацию, а потому доказав свойство для нее - задаром получим ее для исходной группы. Теория абелевых групп не совсем тривиальная, но на порядок проще, чем теория неабелевых, а потому переход к абелевым группам - это колоссальный шаг к упрощению любой задачи.*

• *Также стоит отметить, что как и здесь, как и в линале, когда вы изучали фактор-пространства, так и во всей математике в целом любая факторизация - эта в некотором роде процедура "склейки" элементов, которые мы хотим сделать одинаковыми. Либо факторизацию можно алгебраически представлять как принуждение того, по чему мы факторизуем, быть в новом объекте тривиальным (когда мы дойдем до заданных копредставлениями групп эти соображения станут более формальными). Поэтому, неформально говоря, при факторизации $G/[G,G]$ мы принуждаем любые коммутаторы быть тривиальными, то есть заставляем*

коммутировать любые два элемента - а потому получается при факторизации абелева группа.

• *Вообще говоря есть много нормальных подгрупп $N \lhd G$, фактор по которым G/N абелев - на эту роль кроме $[G,G]$ подходит, к примеру, вся группа $N = G$. Но оказывается, что коммутант сильно выделяется в этом множестве, а именно верно утверждение, что коммутант - это минимальная нормальная подгруппа, фактор по которой абелев, формально: если $N \lhd G$ и G/N абелева, то $[G,G] < N$. Доказательство очень простое, запишем условие коммутации двух произвольных элементов из G/N, а именно для любых $g, h \in G$ выполнено:*

$$N = [gN, hN] = [g,h]N$$

а значит $[g,h] \in N$, а так как коммутант порождается множеством всевозможных коммутаторов, то и $[G,G] < N$. Интуитивно это можно понять так: чтобы получить абелеву группу - нужно как минимум заставить коммутировать все элементы, то есть профакторизовать по коммутаторам, факторизация по остальным элементам уже факультативна и не особо нужна для получения абелевого фактора.

Этот факт сильно помогает при описании коммутантов групп, так как обычно явно записать коммутатор произвольных двух элементов сложно, а потому вы можете достаточно явно записать коммутаторы лишь некоторых элементов (к примеру, вы можете записать коммутатор двух транспозиций (**), но выписать явно коммутатор произвольных перестановок из S_n уже не получится), и если H - нормальная подгруппа, порожденная некоторыми коммутаторами, то $H < [G,G]$. Наблюдение с минимальностью дает при условии абелевости G/H обратное вложение $[G,G] < H$, которое на вес золота. Например, это условие абелевости G/H автоматически выполнено, если $[G:H]$ является простым числом.

Задача

Пусть G не абелева, тогда $G/Z(G)$ не является циклической.

Это то же самое, что сказать, что если $G/Z(G)$ циклическая, то G - абелева, это утверждение полезное, и мы будем использовать его в дальнейшем. Итак, пусть $G/Z(G) = \langle gZ(G) \rangle$ циклическая и порождена некоторым $gZ(G)$. Рассмотрим произвольные $x, y \in G$. Так как G расслаивается на левые смежные классы, то x, y принадлежат некоторым смежным классам, а так как по предположению любой смежный класс равен $g^n Z(G)$ для некоторого n, то $x = g^k z_x$, $y = g^m z_y$ для некоторых $z_x, z_y \in Z(G)$ и $k, m \in \mathbb{Z}$. Так как центральные элементы коммутируют с любыми элементами группы, то получаем:

$$xy = g^k z_x g^m z_y = g^{k+m} z_x z_y$$

$$yx = g^m z_y g^k z_x = g^{k+m} z_x z_y$$

иными словами исходная группа G абелева.

Встречайте теперь нашего нового друга:

==========

Группы Диэдра

==========

Группа Диэдра состоит из движений плоскости, переводящих правильный n-угольник в себя (обозначается группа D_n, обычно считают, что $n \geq 3$). Алгебраически вершины правильного n-угольника удобно параметризовать $\sqrt[n]{1} = \{1, \omega, \omega^2, \dots \omega^{n-1}\} \subset \mathbb{C}$, где $\omega = e^{\frac{2\pi i}{n}}$ но нам с вами не нужна будет их алгебраическая природа, а потому мы просто перенумеруем вершины: $\{0, 1, \dots, n-1\}$. Очевидные и бросающиеся в первую очередь движения - это:

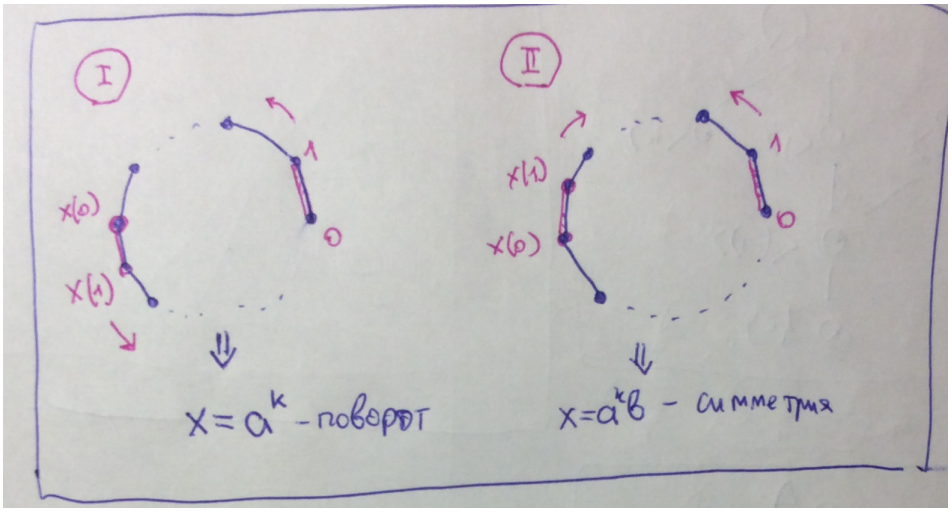
$$a = \text{ поворот на } \frac{2\pi}{n} \text{ по часовой стрелке}$$

$$b = \text{ симметрия относительно оси } O_x$$

Оказывается, произвольное движение порождается этими двумя, действительно: рассмотрим произвольный $x \in D_n$, оно переводит $0 \mapsto x(0)$ первую вершину в некоторую другую; и может возникнуть две ситуации (соседние вершины должны переходить в соседние, а всего есть два соседа у $x(0)$):

I) Либо $x(1) = x(0) + 1$ по модулю n, тогда при условии сохранения расстояний $x(2) = x(0) + 2$ (так как $x(2)$ должна быть сдвигом на 2 относительно $x(0)$ (но таких точек две: $x(0) + 2$ и $x(0) - 2$), но при этом она должна быть еще и сдвигом на 1 относительно $x(1)$), $x(3) = x(0) + 3$ и т.д.: то есть это движение обязано быть поворотом и $x = a^k$ для некоторого k.

II) Пусть $x(1) = x(0) - 1$, тогда легко понять из аналогичных соображений, что $x(2) = x(0) - 2$, $x(3) = x(0) - 3$ и т.д., таким образом это движение изменяет ориентацию, а значит является симметрией относительно некоторой прямой. Нетрудно понять, что в этом случае $x = a^k b$ - так как оба этих движения одинаково действуют на вершинах n-угольника. Действительно: $x(i) = x(0) - i$, $a^k b(i) = a^k(-i) = x(0) + (-i)$, если $k = x(0)$.



Для кого-то, возможно, более аргументировано будет услышать, что движение задается образом трех неколлинеарных точек, из соображений симметрии нетрудно заметить, что начало координат переходит в себя, а потому, если мы поняли, куда переходит 0 и 1, то мы восстанавливаем наше движение.

Таким образом $|D_n| = 2n$ из которых n движений сохраняют ориентацию, т.е. являются поворотами, а n движений меняют ориентацию, т.е. являются симметриями относительно некоторых прямых (в случае многоугольника с нечетным числом сторон - относительно прямых, проходящих через начало координат и вершины, а в случае многоугольника с четным числом сторон - относительно прямых, проходящих через начало координат и вершины, а также середины сторон: для простоты мыслите квадратами и пятиугольниками). Отмечу, что с помощью геометрического подхода очень сложно решать большинство задач, так как не очень ясны алгебраические соотношения между ними. Поэтому более плодотворных взгляд на эти вещи - алгебраический, с этой целью научимся перемножать эти движения и поймем, какими групповыми соотношениями они связаны.

Как уже отмечалось:

$$D_n = \begin{Bmatrix} e & a & a^2 & \dots & a^{n-1} \\ b & ab & a^2b & \dots & a^{n-1}b \end{Bmatrix}$$

В первой строчке все повороты, во второй - все симметрии. Ясно, что $a^n = b^2 = 1$, но кроме этих элементарных есть еще одно соотношение: $b^{-1}ab = a^{-1}$. Оказывается, это полный набор соотношений, т.е. любое соотношение между элементами может быть "выведено" из этих, на формальном языке это означает, что группа Диэдра задана копредставлением:

$$D_n = \langle a, b : a^n = b^2 = 1, b^{-1}ab = a^{-1} \rangle$$

Сейчас нам не обязательно уметь доказывать полноту этих соотношений, достаточно понимать, как произвольный элемент группы с помощью этих соотношений приводить к каноническому виду $a^k b^m$, где $0 \leq k \leq n-1, 0 \leq m \leq 1$. Последнее соотношение эквивалентно $ab = ba^{-1}$, и я для подобных соотношений использую неформальный термин "правило мясорубки": элементы a и b не коммутируют, но a можно "перетащить" сквозь b и после этого он "перемалывается" в a^{-1}. То есть все можно "перетащить" сквозь b, но ценой внутреннего изменения, здесь b играет роль мясорубки. После умножения мясорубочного тождества на a^{-1} слева и на a справа мы получим $a^{-1}b = ba$. Применяя несколько раз либо это, либо оригинальное тождество получаем для любого $n \in \mathbb{Z}$, что

$$a^n b = ba^{-n}$$

Покажу на примере, как это работает, приведя к каноническому виду следующий элемент группы Диэдра, скажем D_5 (алгоритм такой: нужно перекидывать так, чтобы все a оказались слева, а b справа; так что если видим какой-нибудь b, стоящий левее a - то применяем к этой паре мясорубочное тождество):

$$aba^8ba^2b = aba^8ba^2b = aba^8a^{-2}bb = aba^6 = aba^6 = aa^{-6}b = a^{-5}b = b$$

Пример

Вычислить $Z(G)$, $[G,G]$ и $G/[G,G]$ для S_n, A_n, Q_8, D_{2n}.

Подобного рода задачки вы должны щелкать как орешки, так как в них мало глубоких идей, а есть лишь требования к элементарным вычислительным навыкам. К тому же, это список пока для нас базовых групп, для которых нужно знать важнейшие характеристики, иначе будет сложно ориентироваться в сложных группах, если вы будете теряться в простейших примерах. По мере того, как расширяется известный вам список групп и базовых характеристик - не бездействуйте и тренируйтесь, вычисляя новые характеристики для новых групп (или просто описывайте их свойства, если явное вычисление невозможно). А для начала советую вам разобраться, чему равны эти базовые характеристики для D_{2n+1}; структура групп Диэдра для четных и нечетных индексов немного отличается.

Центр обычно вычисляется легко для групп, где можно хоть немного конструктивно задать любой элемент группы и выписать условие его коммутации со всеми остальными элементами.

Для вычисления коммутатора, в случае если можно записать относительно явную и простую формулу для произвольного элемента группы (например, в случае D_n), обычно вычисляют всевозможные коммутаторы - а дальше смотрят, какую они подгруппу порождают. Если явную формулу записать сложно (например, в случае S_n... вы начнете вспоминать про реализацию перестановки как произведение независимых циклов, но в такой форме нельзя написать прозрачной формулы для произведения перестановок) - то обычно получают некоторое семейство коммутаторов, строят ими порожденную подгруппу, а дальше хитрыми приемами пытаются доказать, что это весь коммутант. Очень часто в этом сильно помогает сформулированное ранее утверждение о том, что коммутант - это минимальная нормальная подгруппа, фактор по которой абелев.

$\boxed{S_n}$

Пусть существует нетривиальный $\sigma \in Z(S_n)$, а значит для некоторых $i \neq j$ выполнено $\sigma(i) = j$. Тогда рассмотрим произвольную перестановку $\omega \in S_n$, такую, что $\omega(j) = j, \omega(i) = k$, $k \neq i$ (и понятно, что $\sigma(k) \neq j$, потому что σ - биекция и в j уже переходит i под действием σ). Ясно, что такая перестановка ω существует, если $n \geq 3$. Тогда имеем:

$$\omega\sigma(i) = j$$

$$\sigma\omega(i) = \sigma(k) \neq j$$

Приходим к противоречию, поэтому $Z(S_n) = \{e\}$ при $n \geq 3$. При $n \leq 2$ группа S_n абелева, а значит совпадает со своим центром.

Если $n \leq 2$, то S_n абелева, а потому коммутант тривиален. Пусть $n \geq 3$. Тогда заметим, что

$$(ijk) = (kj)(ik) = (ij)(ik)(ij)^{-1}(ik)^{-1}$$

так как все (**) сопряжены, а значит для некоторой перестановки σ верно $(kj) = \sigma(ik)\sigma^{-1}$, а значит $(kj)(ik) = \sigma(ik)\sigma^{-1}(ik)^{-1} = [\sigma, (ik)]$, и в данном случае на эту роль подходит $\sigma = (ij)$, что легко понять из формулы для сопряжения перестановок. Таким образом все тройные циклы лежат в коммутанте, а значит и подгруппа ими порожденная, а мы знаем, что эта подгруппа совпадает с A_n, таким

образом получаем $A_n < [S_n, S_n]$. С другой стороны:

$$\tau(xyx^{-1}y^{-1}) = 0$$

то есть любой коммутатор лежит в A_n, а значит и $[S_n, S_n] < A_n$. Таким образом при $n \geq 3$:

$$[S_n, S_n] = A_n$$

$\boxed{A_n}$

В случае центра рассуждения почти дословно такие же как и для S_n, за той лишь разницей, что существование перестановки ω с описанными выше свойствами можно гарантировать лишь при $n \geq 4$: потому что $\omega = (j)(ik\ldots)$, и должен быть 4-ый элемент, чтобы превратить эту перестановку в четную: замкнуть цикл $(ik\ldots)$ до 3-цикла, или добавить еще каких-нибудь циклов. При $n = 3$ группа $A_3 = \mathbb{Z}_3$ является абелевой.

Касательно коммутанта, рассуждения опять же напоминают случай S_n, пусть $n \geq 5$, тогда (в данном случае 3-цикл уже нельзя представлять произведением двух транспозиций, так как они нечетны, нужно использовать циклы (**)(**), а также следить за тем, чтобы сопрягающая их перестановка была четной, ясно, что нам нужно много индексов, чтобы разгуляться - поэтому $n \geq 5$, все участвующие индексы предполагаются различными):

$$(ijk) = [(kj)(ab)][(ik)(ab)] = \sigma[(ik)(ab)]\sigma^{-1}[(ik)(ab)]^{-1}$$

здесь сгодится $\sigma = (ij)$, а дальше ее апгрейтим до четной: $\sigma = (ij)(ab)$; то есть фактически мы взяли конструкцию из S_n, где каждая перестановка была нечетной, а дальше к каждой перестановке добавляем независимый цикл (ab), превращая ее в четную и не нарушая при этом равенство. Таким образом:

$$Z(A_n) = \{e\} \quad \text{при } n \geq 4$$

$$[A_n, A_n] = A_n \quad \text{при } n \geq 5$$

В случае A_4 сначала заметим, что все перестановки циклического типа (**)(**) являются коммутаторами (пусть $V_4 = \{e, a, b, c\}$, нетрудно заметить, что все нетривиальные элементы V_4 сопряжены некоторым (***), а потому для некоторого 3-цикла g выполнено $gag^{-1} = b$, а потому $c = ab = agag^{-1} = [a, g]$, в силу того, что все $\{a, b, c\}$ равноправны получаем, что и остальные нетривиальные элементы V_4 являются коммутаторами), а значит $V_4 < [A_4, A_4]$. Дальше для доказательства $[A_4, A_4] = V_4$ можно пойти двумя путями: первый - сложный лобовой путь вычисления коммутатора произвольной пары элементов A_4, где допускаются лишь 2 циклических типа: (**)(**) и (***). Ясно, что любые два элемента вида (**)(**) коммутируют, а потому хитрыми комбинаторными приемами нужно показать, что коммутаторы $[(**)(**), (***)]$ и $[(***), (***)]$ имеют циклический тип (**)(**), а значит в таком случае $[A_4, A_4] < V_4$. Второй способ - элегантный и красивый с применением упомянутого ранее утверждения, что *коммутант - это минимальная нормальная подгруппа, фактор по которой абелев*. Так как $|A_4/V_4| = 3$, то $A_4/V_4 \cong \mathbb{Z}_3$ является циклической группой, а потому мы получаем $[A_4, A_4] < V_4$, избежав страшного комбинаторного перебора. Ясно, что в случаях общего положения $S_n/[S_n, S_n] = \mathbb{Z}_2$, так как $[S_n : A_n] = 2$ и существует лишь одна

группа порядка два, аналогично: $A_n/[A_n, A_n] = \{e\}$. В особых случаях абеленизация легко вычисляется: там либо все тривиально, либо порядок фактора простой - а значит фактор-группа циклическая. Например: $A_4/[A_4, A_4] \cong \mathbb{Z}_3$ так как она имеет порядок 3, а 3 простое число, значит существует лишь одна группа заданного порядка, или, к примеру, $[A_3, A_3] = \{e\}$, а потому $A_3/[A_3, A_3] \cong A_3 \cong \mathbb{Z}_3$.

$\boxed{Q_8}$

Из описанной выше таблицы умножения вытекает, что $Z(Q_8) = \{1, -1\}$. Посмотрим, чему равны $[x, y]$. Если или x, или y равен ± 1, то коммутатор тривиален, если x, y - это с точностью до знака одна и та же буква, то коммутатор опять тривиален. Значит единственный нетривиальный случай, это когда x, y - разные буквы (замечу, что умножение x или y на -1 не меняет коммутатора, а потому мы будем считать, что это буквы с плюсом), также помним, что для любых различных букв x, y выполнено $xy = \pm z$, где z - оставшаяся буква, и что $x^2 = -1$ для любой буквы x. Таким образом получаем:

$$[x, y] = xyx^{-1}y^{-1} = (-1)^2xyxy = (\pm z)(\pm z) = -1$$

Таким образом любой коммутатор равен или 1 или -1, а значит $[Q_8, Q_8] = \{1, -1\}$.

Заметим, что $V = Q_8/[Q_8, Q_8] = Q_8/Z(Q_8)$ не может быть циклической, так как Q_8 не абелева (помните эту задачку?). При этом V - абелева и $|V| = 4$. Когда мы пройдем теорию абелевых групп - такие ситуации будут легко разрешаться (из теоремы о классификации конечно-порожденных абелевых групп вытекает, что всего две абелевы группы порядка 4 - это $\mathbb{Z}_4$ и $\mathbb{Z}_2 \times \mathbb{Z}_2$), а пока попытаемся выкрутиться. Заметим, что любой нетривиальный элемент $x \in V$ имеет порядок 2 (должен делить 4, но 4 не может быть - иначе группа циклическая). Более того, если взять два нетривиальных несовпадающих $x, y \in V$, то xy не может равняться e (иначе они бы совпадали), не может ни x, ни y (иначе кто-нибудь из них был бы тривиальным), значит xy равен оставшемуся четвертому элементу. Это в точности таблица умножения $V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$.

$\boxed{D_{2n}}$

Рассмотрим произвольный $x \in Z(D_{2n})$. Заметим, что условие коммутации с произвольным элементом достаточно проверять лишь для порождающих группу элементов, т.е. в нашем случае для a, b, так как если коммутирует с порождающими, то и с любыми их произведениями.

Пусть $x = a^k$, тогда он очевидно коммутирует с a. Условие коммутации с b выглядит как:

$$e = [a^k, b] = a^kba^{-k}b = a^{2k}b^2 = a^{2k}$$

Таким образом $2k$ делится на $2n$, что означает, что в приводимой записи (где степени a неотрицательны и $< 2n$) допустимы $k = 0, n$.

Пусть теперь $x = a^kb$, запишем условие коммутации с a:

$$[a^kb, a] = a^kbaba^{-k}a^{-1} = a^kbba^{-1}a^{-k}a^{-1} = a^{-2} \neq e$$

Условие коммутации с b проверять не нужно, так как элемент этого типа даже с a не может коммутировать, а значит центральным ему не быть никогда.

Таким образом $Z(D_{2n}) = \{0, a^n\} \cong \mathbb{Z}_2$.

Вычислим коммутаторы $[x, y]$. Если и x, и y являются вращениями, то они коммутируют, а значит коммутатор тривиален.

Если один из них, скажем, $x = a^k$ - является вращением (меняя их местами мы покроем и случай, когда вращением является y), а второй: $y = a^m b$ - является симметрией, то:

$$[x, y] = [a^k, a^m b] = a^k a^m b a^{-k} b a^{-m} = a^{k+m} b b a^k a^{-m} = a^{2k}$$

И в случае, когда они оба являются симметриями: $x = a^k b$, $y = a^m b$ мы получаем:

$$[x, y] = [a^k b, a^m b] = a^k b a^m b b a^{-k} b a^{-m} = a^k b a^{m-k} b a^{-m} = a^k b a^{2m-k} b = a^{2k-2m} b b = a^{2k-2m}$$

Таким образом, в обоих случаях коммутаторы равны $a^{2k'}$, причем k' может быть любым целым числом (особенно хорошо это видно по первой формуле). Понятно, что порожденная ими подгруппа равна $[D_{2n}, D_{2n}] = \langle a^2 \rangle = \mathbb{Z}_n$. В этом случае, отмечу, множество коммутаторов совпадает с коммутантом группы.

Что касается $D_{2n}/[D_{2n}, D_{2n}]$, то как и в случае с Q_8 - это абелева группа порядка 4. Цикличный случай уже не так легко откинуть, так как в отличие от Q_8 здесь $[D_{2n}, D_{2n}] \neq Z(D_{2n})$. Но можно просто составить таблицу умножения: фактор группа состоит из $[D_{2n}, D_{2n}], a[D_{2n}, D_{2n}], b[D_{2n}, D_{2n}], ab[D_{2n}, D_{2n}]$. Ясно, что любой элемент в квадрате равен тождественному, плюс если перемножить любые два нетривиальных - то получится третий нетривиальный, значит и в этом случае $D_{2n}/[D_{2n}, D_{2n}] \cong V_4$.

Вообще, с помощью этих важнейших характеристик удобно проверять группы на изоморфность (или по крайней мере начинать проверку), так как если характеристики различаются, то и группы неизоморфны.

Пример

- *Изоморфны ли группы S_3 и D_3?*
- *Изоморфны ли группы A_4 и D_6?*
- *Изоморфны ли группы D_4 и Q_8?*

---

1) Разумеется, $S_3 \cong D_3$, так как движениями плоскости можно организовать любую перестановку вершин правильного треугольника.

2) Группы неизоморфны, так как несмотря на то, что они обе некоммутативные и имеют один и тот же порядок, но $Z(A_4) = \{e\}$, тогда как $Z(D_6) \cong \mathbb{Z}_2$. Коммутанты их также отличаются: $[D_6, D_6]$ - цикличный, а $[A_4, A_4] = V_4$.

3) С этими группами ситуация чуть сложнее, так как:

$$|D_4| = |Q_8|$$

$$Z(D_4) \cong \mathbb{Z}_2 \cong Z(Q_8)$$

$$[D_4, D_4] \cong \mathbb{Z}_2 \cong [Q_8, Q_8]$$

$$D_4/[D_4, D_4] \cong V_4 \cong Q_8/[Q_8, Q_8]$$

последняя строка выполняется потому, что в обоих случаях коммутант совпадает с центром, а фактор по центру не может быть циклическим в неабелевом случае. Так как порядки абеленизаций в обоих случаях равны 4, а есть только две абелевы группы порядка 4: V_4 и циклическая, то тогда наши абеленизации в обоих случаях изоморфны V_4.

Поэтому нужно искать более изощренный различающий их инвариант. Огромным потенциалом обладают инварианты:

$$N_k(G) = \#\{x \in G : x^k = e\}$$

$$\tilde{N}_k(G) = \#\{x \in G : \text{ ord}(x) = k\}$$

Эти инварианты различаются, хотя они и очень похожи и выражаются одни через другие, например: $N_4 = \tilde{N}_4 + \tilde{N}_2 + 1$. В данном случае поможет различить группы инвариант:

$$N_2(G) = \#\{x \in G : x^2 = e\}$$

Тогда нетрудно понять, что $N_2(D_4) = 1 + 1 + 4 = 6$ (тождественный, поворот на 180 градусов и 4 симметрии), тогда как $N_2(Q_8) = 2$ (только 1 и -1). Таким образом $D_4 \ncong Q_8$.

Пример

Описать все нормальные подгруппы S_3, A_4.

Описание всех нормальных подгрупп - как и все остальное в теории групп - неалгоритмично. Здесь существует два похожих, но идейно немного отличающихся подхода:

I) Стартуя с произвольного элемента $h \in H \lhd G$ мы замечаем, что его нормальное замыкание $\langle\langle h \rangle\rangle < H$ (нормальное замыкание - это всевозможные сопряжения и их произведения - как правило множество получается очень тучным). Значит H или совпадает с $\langle\langle h \rangle\rangle$, либо больше. В последнем случае берем произвольный элемент $x \in H$ не входящий в нормальное замыкание h - и проделываем ту же процедуру для $\langle\langle h, x \rangle\rangle$. Добавляем к нормальному замыканию элементы до тех пор, пока наше нормальное замыкание не сравняется со всей подгруппой. Процесс этот довольно тяжеловесен (фактически, нужно перебирать нормальные замыкания всех! элементов группы. Хотя часто наблюдение, что в нормальном замыкании вместе с любым элементом лежат и все к нему сопряженные, помогает существенно упросить перебор: к примеру, в случае S_n фактически достаточно перебирать не элементы, а их циклические типы); но несомненное преимущество этого подхода в том, что он всегда работает и теоретически даже для бесконечных групп.

II) В теории групп важным является понятие *класса сопряженности*, по определению это

$$[x] = \{g^{-1}xg\}_{g \in G}$$

множество всевозможных сопряжений фиксированного элемента. Ясно, что любой элемент лежит в нормальной подгруппе вместе со всем своим классом сопряженности, т.е. любая нормальная подгруппа - это объединение некоторого количества классов сопряженности. И алгоритм такой: мы разбиваем группу на классы сопряженности, а дальше рассматриваем случаи, когда мощность объединения нескольких классов сопряженности является делителем порядка группы - и проверяем, будет ли выбранное объединение классов подгруппой. Если да, то она автоматически будет нормальной.

Замечу, что процесс описания всех подгрупп заданной группы намного более сложный, нежели процесс описания всех нормальных подгрупп, так как последних намного меньше.

==========

Проиллюстрируем оба способа на простом примере группы S_3.

1) Пусть $H \lhd S_3$ - нетривиальная (т.е. отличная от $\{e\}$ и S_3) подгруппа. Вопрос: какие циклические типы возможны для перестановок из H?

Если в H есть транспозиция $\sigma = (ij)$, тогда в H лежат все перестановки циклического типа (**), а так как транспозиции порождают S_3, то и $H = S_3$.

Если в H транспозиций нет, но есть $\sigma = (ijk)$, тогда есть и обе перестановки циклического типа (***). Как известно, они порождают A_3. Поэтому, $H = A_3$, так как если H строго больше A_3, то в ней есть отсутствующая по предположению транспозиция. Рассуждать можно и по-другому: мы получили, что $A_3 \subset H \subset S_3$, но нетривиальных промежуточных групп быть не может по теореме Лагранжа, так как $|S_3| = 6$ и $|A_3| = 3$ отличается в простое число раз - и между ними нельзя строго вставить некоторый делитель 6, одновременно являющийся кратным 3. Таким образом полный список нормальных подгрупп исчерпывается $\{e\}, A_3, S_3$.

2) Опишем все нормальные подгруппы вторым способом, разбив для этого S_3 на классы сопряженности, причем нам здесь не так будет важна структура классов, сколько их мощность. Имеем:

$$[e] = \{e\} \qquad \# = 1$$

$$[(12)] = \{(**)\} \qquad \# = 3$$

$$[(123)] = \{(***)\} \qquad \# = 2$$

Замечу, что $\{e\}$ обязательно должен быть в подгруппе. Единственным способом "набрать" нетривиальный делитель 6 с условием обязательного включения класса $[e]$ - это 1+2, т.е. $[e] \cup [(123)]$. Далее убеждаемся, что это подгруппа, потому что эти элементы образуют в точности A_3. Таким образом никаких других нетривиальных подгрупп у нас не будет.

==========

Теперь A_4.

Воспользуемся здесь вторым подходом, а именно опишем классы сопряженности и поймем, каким образом можно их набрать, чтобы получить делитель 12. Для этой цели нам понадобится очень важное и нужное для других задач утверждение.

Очень важное утверждение

Пусть $\sigma \in A_n$, а $[\sigma]_{A_n}$ и $[\sigma]_{S_n}$ - ее классы сопряженности в A_n и S_n соответственно. Тогда:

$$[\sigma]_{S_n} = [\sigma]_{A_n} \qquad \Longleftrightarrow \qquad \left[\begin{array}{r} \textit{в разложении } \sigma \textit{ есть цикл четной длины} \\ \textit{в разложении } \sigma \textit{ есть 2 цикла одинаковой длины} \end{array} \right.$$

В противном случае (т.е. когда σ состоит лишь из независимых циклов различной нечетной длины) $[\sigma]_{S_n}$ распадается на 2 класса сопряженности A_n одинаковой мощности.

Иными словами, если у двух четных перестановок с одинаковым циклическим типом выполнено одно из тех двух условий, то они сопряжены в A_n, в противном случае перестановки этого циклического типа делятся на два множества, в каждом из которых все элементы попарно сопряжены в A_n.

Докажем $\Leftarrow$. Предположим, что выполнено одно из тех двух условий и рассмотрим произвольные 2 четные перестановки $\hat{\sigma}, \sigma \in A_n$ с одинаковой

циклической структурой. Так как их циклическая структура совпадает, то найдется $g \in S_n$, что $\hat{\sigma} = g\sigma g^{-1}$. Если $g \in A_n$ - то мы победили. Если нет, то заметим, что выполнение одного из тех двух условий влечет существование такой нечетной $h \in S_n \backslash A_n$, что $[h, \sigma] = 1$. Если есть цикл четной длины, то в качестве в качестве h мы можем взять этот цикл, если есть два нечетных цикла одинаковой длины $(i_1, \dots, i_k)$ и $(j_1, \dots, j_k)$, то можно положить $h = (i_1, j_1) \dots (i_k, j_k)$ - ясно, что это будет нечетная коммутирующая с σ перестановка. Таким образом

$$\hat{\sigma} = (gh)\sigma(gh)^{-1}$$

и в отличие от g перестановка gh уже будет четной, а значит σ и $\hat{\sigma}$ оказываются сопряженными даже в A_n.

Докажем $\Rightarrow$. Пусть теперь не выполнены оба упомянутых выше условия, т.е. в перестановке σ только циклы различных нечетных длин. Так как $S_n = A_n \sqcup A_n(12)$, то

$$[\sigma]_{S_n} = [\sigma]_{A_n} \cup [(12)\sigma(12)^{-1}]_{A_n}$$

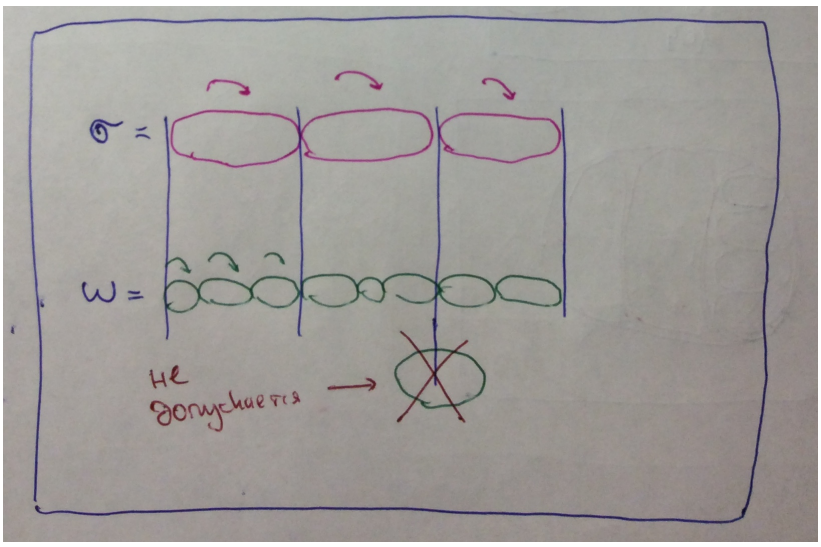
и предположим, что классы сопряженности справа пересекаются, иными словами, найдутся $g, h \in A_n$, что

$$g\sigma g^{-1} = h(12)\sigma(12)^{-1}h^{-1}$$

это равенство удобно переписать как $\omega\sigma\omega^{-1} = \sigma$, где $\omega = (12)h^{-1}g$. Заметим, что ω - нечетная перестановка и докажем, что σ не может в принципе коммутировать с нечетными перестановки. Пусть $\sigma = (i_1, \dots, i_{2k+1})(j_1, \dots, j_{2m+1}) \dots$ Вспоминая волшебную формулу для сопряжения, получаем, что

$$\omega\sigma\omega^{-1} = (\omega(i_1), \dots, \omega(i_{2k+1}))(\omega(j_1), \dots, \omega(j_{2m+1})) \dots = (i_1, \dots, i_{2k+1})(j_1, \dots, j_{2m+1}) \dots$$

И теперь самый идейно насыщенный и красивый шаг в доказательстве: так как длины всех циклов различны, то ω должна каждый индекс не выводить за пределы его цикла из σ, таким образом циклическая структура ω должна "накладываться" на циклическую структуру σ в том смысле, что каждый цикл из ω "живет" в некотором цикле из σ. Отсюда нетрудно понять, что каждый цикл ω коммутирует с каждым циклом из σ, и задача свелась к на порядок более простой - теперь нужно проверять условие коммутации не произвольных перестановок, а лишь двух циклов.



Хочу доказать, что хотя циклические структуры σ и ω могут быть разными, циклическая структура ω "внутри" каждого цикла σ_0 перестановки σ будет совпадать с σ_0^k для некоторого k, а так как все циклы σ были нечетной длины, то все циклы (а значит и их степени) будут четными перестановками, а значит и ω будет четной перестановкой, что будет противоречием с тем, что ω - нечетная.

Действительно, пусть ограничение ω на присутствующие в цикле σ_0 аргументы равно $\omega_0 = \omega|_{\text{аргументы из цикла } \sigma_0}$ (зеленая перестановка, действующая внутри одной розовой сосиски). Получили обыкновенную задачу поиска централизатора цикла максимальной длины, т.е. докажем, что $\omega_0 = \sigma_0^k$ для некоторого k. Есть два стандартных способа это доказать:

• Первый - правильная трактовка волшебной формулы для $\omega_0\sigma_0\omega_0^{-1} = \sigma_0$; с помощью перенумерации можно считать, что $\sigma_0 = (12\dots k)$. Таким образом получаем, что $(\omega_0(1)\omega_0(2)\dots\omega_0(k)) = (12\dots k)$. И если $\omega_0(1) = i$, то из условия сохранения порядка следования образы всех оставшихся аргументов однозначно восстанавливаются: $\omega_0(j) = (j-1) + i$ по модулю n, а значит легко понять, что $\omega_0 = \sigma_0^{i-1}$.

• Второй способ - с помощью действий, о которых речь пойдет далее: рассмотрим действие сопряжением $\mathrm{Ad} : S_k \curvearrowright S_k$. Как и прежде путем перенумерации считаем, что $\sigma_0 = (12\dots k)$. Легко понять, что множество коммутирующих с данной перестановок есть в точности стабилизатор действия сопряжением (его обычно называют централизатором). Тогда по формуле для орбит получаем:

$$\frac{|S_k|}{|\operatorname{St}(\sigma_0)|} = |\operatorname{Orb}(\sigma_0)|$$

Ясно, что орбита в данном случае имеет мощность $(k-1)!$, так как орбитой сопряжения являются все перестановки, сопряженные заданной, т.е. имеющие такой же циклический тип, а таких в точности $(k-1)!$, потому что есть $k!$ способов расставить упорядоченно k чисел, а дальше делим на k, потому что неважно с какого элемента цикл берет старт. Таким образом по формуле орбит получаем $\operatorname{St}(\sigma_0) = k$. Но все степени σ_0^k коммутируют с σ_0, а их k штук. Значит из формулы орбит получаем, что других нет.

Таким образом классы $[\sigma]_{A_n}$ и $[(12)\sigma(12)^{-1}]_{A_n}$ не пересекаются. Докажем, что у них одинаковые мощности. С этой целью заметим, что нормальность A_n обеспечивает $A_n(12) = (12)A_n$, откуда мы получаем, что:

$$[(12)\sigma(12)^{-1}]_{A_n} = \{g(12)\sigma(12)^{-1}g^{-1}\}_{g\in A_n} = \{(12)g\sigma g^{-1}(12)^{-1}\}_{g\in A_n} = (12)[\sigma]_{A_n}(12)^{-1}$$

а так как сопряжение перестановкой (12) (как и любой другой перестановкой) является биекцией, то оно сохраняет мощности, а значит:

$$\#[\sigma]_{A_n} = \#(12)[\sigma]_{A_n}(12)^{-1} = \#[(12)\sigma(12)^{-1}]_{A_n}$$

Замечание:

Отмечу, что в этой теореме учитываются циклы длины 1, т.е. если вы рассматриваете перестановку $(123) \in A_5$*, то у нее будут нечетные циклы совпадающей длины, так как ее подробный циклический тип равен* $(*)(*)(***)$*, в частном случае этой перестановки в* A_3 *или* A_4 *ее класс сопряженности в соответствующем* S_n *разбивается на два, а в* A_n *при* $n \geq 5$ *совпадает с классом в* S_n*. Из этих же соображений для любой перестановки* $\sigma \in S_n$ *будет выполнено* $[\sigma]_{S_{n+2}} = [\sigma]_{A_{n+2}}$*, так как в подробном циклическом типе этой перестановки в* S_{n+2} *будет присутствовать* $(*)(*)$*.*

Спустимся на землю к A_4.

Вычислим классы сопряженности:

$$[e]_{A_4} \qquad \# = 1$$

$$[(**)(**)]_{A_4} \qquad \# = 3$$

так как для них выполняется одно из двух условий только что доказанного очень важного утверждения, и класс сопряженности в S_4 и в A_4 совпадает. Что касается перестановок циклического типа $(***)$, то для них ни одно из двух условий не выполняется, а потому класс сопряженности в S_4 разбивается на два равных по мощности класса в A_4, таким образом копилочка сопряженных классов пополняется:

$$\text{две штуки } [(***)] \qquad \# = 4 \text{ каждая}$$

Единственной возможностью набрать нетривиальный делитель 12 из $\{1, 3, 4, 4\}$, при условии, что мы обязательно берем 1 - только один, а именно 1+3. Ясно, что в этом случае мы получаем $V_4 \lhd A_4$.

Замечания:

• *Полезно понимать, как именно делится* $[(***)]_{S_4}$ *на два класса в* A_4*, внимательный читатель вспомнит, что мы уже доказывали несопряженность* (123) *и* (132) *в* A_4*, а значит:*

$$[(123)]_{A_4} \neq [(132)]_{A_4}$$

• *Замечу, что вместо использования этой сложной теоремы - можно было бы воспользоваться лишь финальным штрихом ее доказательства о совпадении*

$$\#[\sigma]_{A_n} = \#(12)[\sigma]_{A_n}(12)^{-1} = \#[(12)\sigma(12)^{-1}]_{A_n}$$

для которого не требовался весь этот сложный анализ циклических структур, и эти равенства выполняются всегда. Таким образом используя только эти равенства, а также разложение $[\sigma]_{S_n} = [\sigma]_{A_n} \cup [(12)\sigma(12)^{-1}]_{A_n}$ *мы получим, что:*

$$\#[\sigma]_{A_n} \geq \frac{\#[\sigma]_{S_n}}{2}$$

из которой вытекает $\#[(***)]_{A_4} \geq 4$*, и этой оценки для доказательства почти хватает (равенство достигается в том случае, когда множества* $[\sigma]_{A_n}$ *и* $(12)[\sigma]_{A_n}(12)^{-1}$ *не пересекаются). "Хватает почти", потому что остается довольно неприятная возможность* $\#[(***)]_{A_4} = 5$ *(которая сразу отметается,*

если использовать теорему в полную ее мощь), так как в этом гипотетическом случае этот класс вместе с тривиальным будут давать 6 элементов, а 12 делится на 6. Возможно, самый простой способ с этим справить (т.е. доказать, что не может каждая нетривиальная перестановка в $H \lhd A_4$ быть 3-циклом) это рассмотреть эту нетривиальную перестановку (переобозначая элементы можно считать ее равной $\sigma = (123)$), а дальше заметить, что $(142) = (243)(123)(243)^{-1} \in H$, но при этом $(123)(142)^2 = (13)(24)$, иными словами сопряжения и произведения обязательно выкинут за рамки 3-циклов. А вообще, разбиение $[(* * *)]_{S_4}$ на два класса в A_4 - это фактически, единственное место, где мы существенно использовали сложную структурную теорему о классах сопряженности в A_n, и ясно, что можно было не стрелять из пушки по воробьям и найти много более простых подходов в этой простой ситуации. Но другое дело, что эта "пушка" попадает в категорию must know, а потому чем раньше мы начнем ее не бояться и пользоваться ею - тем будет лучше.

• *Отмечу, что между делом мы получили другой способ описания всех подгрупп A_4, потому что, насколько помните, главной трудностью было именно доказательство отсутствия подгрупп порядка 6, но так как у них индекс равен 2, то они автоматически нормальны. Значит, если нет нормальных подгрупп порядка 6, то и нет обычных подгрупп такого порядка.*

Одним из ключевых понятий в теории групп является понятие простой группы:

Определение

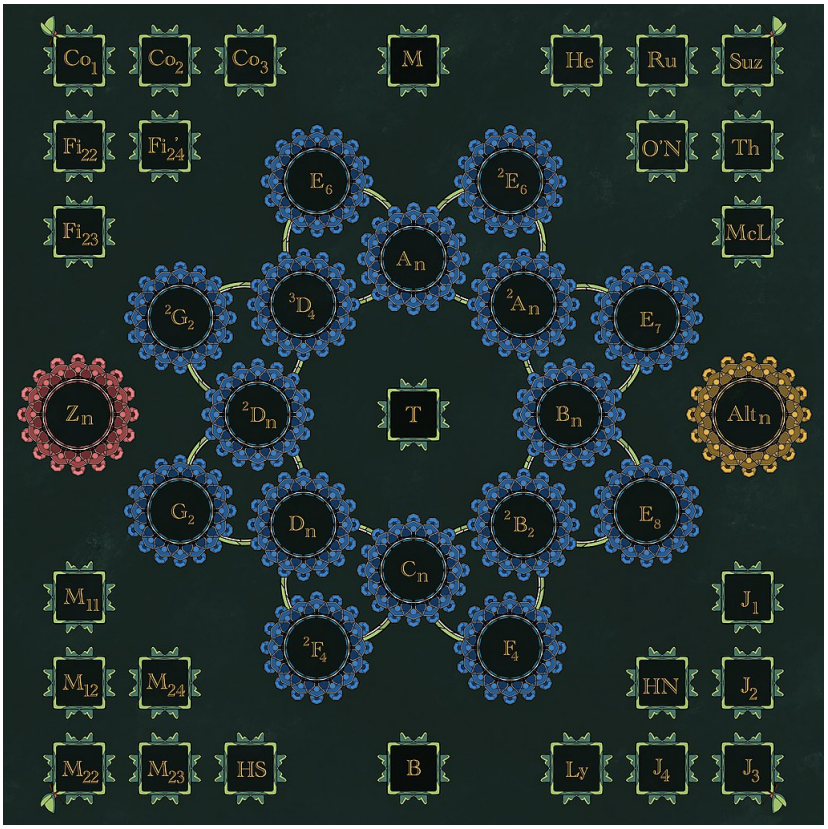
Группа G называется простой, если в ней нет нетривиальных (отличных от $\{e\}$ и G) нормальных подгрупп.

Как я уже говорил, для $H \lhd G$ в некотором очень приблизительном смысле $G \approx H \times G/H$, т.е. наличие нетривиальной нормальной подгруппы позволяет свести почти любую задачу к двум обычно менее трудным группам. Отсутствие нетривиальных нормальных подгрупп означает в некотором роде "неразложимость" группы и что она является базисным строительным кирпичиком, из которых можно сконструировать любую другую группу (потому что процесс расщепления группы G на N и G/N можно продолжать много раз до тех пор, пока нетривиальных нормальных подгрупп не останется). Поэтому естественно в первую очередь изучить "элементарные кирпичики" (т.е. простые группы), а затем уже переходить к более сложным группам.

Но задача полного описания простых конечных групп оказалась очень сложной. Есть две серии, которые лежат на поверхности: это A_n при $n \geq 5$ и $\mathbb{Z}_p$ для простого p, и еще некоторые довольно несложные; но с поиском других примеров или с доказательством, что других нет у математиков были серьезные проблемы. Однако со временем начинали находиться экзотические примеры простых групп, которые назвали *спорадическими группами*. Например в начале 1980-х годов нашли простую группу порядка

$$808017424794512875886459904961710757005754368000000000$$

которую неформально в математических кругах по понятным причинам называют "Монстром". Вот картинка, где приведены все простые группы:



В начале 2000-х годов математики поставили точку в классификации простых конечных групп, доказав, что все простые конечные группы сводятся либо к трем сериям (красные $\mathbb{Z}_p$, желтые A_n и еще одна синяя серия, связанная с группами Ли, которую очень приблизительно можно мыслить как фактор по центру некоторых матричных групп над конечными полями), либо к паре десятков зеленых спорадических групп, причем из этих несерийных спорадических самый большой порядок имеет упомянутый выше "Монстр". Обычно теорему о классификации конечных простых групп называют "Классификацией" с большой буквы, так как она занимает около 10000 страниц и пока не очень ясно, можно ли существенно упростить доказательство. Так что все познается в сравнении: пришлось бы вам разбираться с классификацией - вы бы за счастье и легкую прогулку восприняли характеризацию классов сопряженности в A_n. Несмотря на то, что "Классификацию" проверили и сомнениям она не подлежит - не все математики с большой охотой готовы в своих работах ссылаться на теорему с доказательством на тысячи страниц. Однако есть очень красивые результаты, например разрешимость группы внешних автоморфизмов простой конечной группы, которые пока не удается доказать без применения "Классификации". Также стоит уточнить, что эта "Классификация" дает описание лишь всех *простых* конечных групп, и ничего не говорит про группы, не являющиеся простыми. Конечно же, простые группы являются своеобразными кирпичиками, из которых строится любая конечная группа; а потому некоторые вопросы про конечные группы можно свести к случаю простых групп; но не все, потому что, к сожалению, лишь часть информации про группу можно восстановить по кирпичикам, из которых она состоит: потому что (в отличие от того же линала), группа G допускает лишь точную последовательность $0 \to N \to G \to G/N \to 0$ и в большинстве случаем неизоморфна $N \times G/N$, и G лишь очень отдаленно по свойствам напоминает прямое произведение. Поэтому не нужно думать, что "Классификация"

это панацея.

Все большое всегда начинается с малого - и мы ограничимся лишь доказательством крошечного кусочка классификационной теоремы, а именно:

Утверждение
Группа A_n простая при $n \geq 5$.

Мы будем придерживаться первого подхода к описанию нормальных подгрупп, так как с ростом n растет количество классов сопряженности - и теряется возможность проверять условия делимости порядка группы на мощность некоторого набора классов сопряженности.

Пусть существует некоторая нетривиальная $H \lhd A_n$. Рассмотрим нетривиальную $\theta \in H$, возводя ее в правильную степень k можно добиться, чтобы у $\sigma = \theta^k$ был простой порядок p. Тогда так как порядок перестановки - это НОК длин ее независимых циклов, то перестановка состоит из некоторого количества циклов длины p.

• Пусть $p \geq 5$, тогда с точностью до перенумерации можем считать, что разложение σ в независимые циклы выглядит так:

$$\sigma = (12 \dots p)\tau$$

где τ - блок оставшихся независимых циклов; пусть $\omega = (123)$, тогда $\sigma' = \omega\sigma\omega^{-1} = (2314 \dots p)\tau$ и

$$\sigma'\sigma^{-1} = (124) \in H$$

Все тройные циклы в A_n при $n \geq 5$ сопряжены (это вытекает из Очень Важного Утверждения, так как тройные циклы имеют при $n \geq 5$ циклический тип $(*)(*)(***)\dots$), а значит если в H есть какой-то тройной цикл, то есть все тройные циклы, а они порождают A_n. Таким образом $H = A_n$.

• Пусть $p = 3$. Если σ состоит из одного цикла, то как и выше получаем $H = A_n$. Если тройных циклов больше одного, то с точностью до перенумерации можем считать $\sigma = (123)(456)\tau$, то пусть $\omega = (14)(25)$, тогда

$$\sigma' = \omega\sigma\omega^{-1} = (453)(126)\tau$$

$$\sigma'\sigma^{-1} = (14)(26) \in H$$

Опять-таки из Очень Важного Утверждения вытекает, что все перестановки циклического типа $(**)(**)$ сопряжены, а потому они тоже лежат в H. Но группа A_n порождается перестановками вида $(**)(**)$ при $n \geq 5$ (при $n = 4$ они порождают не A_4, а всего-лишь V_4), действительно, достаточно с помощью этих циклов получить произвольный тройной цикл, а тройные циклы, как мы знаем, порождают A_n:

$$[(ij)(ab)][(ik)(ab)] = (ikj)$$

• Пусть $p = 2$, тогда с точностью до перенумерации (одного цикла длины 2 быть не может, так как σ четная перестановка):

$$\sigma = (12)(34)\tau$$

$$\sigma' = (123)\sigma(123)^{-1} = (23)(14)\tau$$

$$\sigma'\sigma^{-1} = (13)(24) \in H$$

Как и в предыдущем пункте - вместе с этой перестановкой все (**)(**) лежат в H, а так как они порождают A_n, то $H = A_n$.

Замечание:

В изложении этого результата я почти дословно следовал книжке Э.Б. Винберга. Хотя в доказательстве я уточнил, почему сложно было бы пойти вторым путем анализа делимости на сумму мощностей классов сопряженности, однако эту трудность можно обойти и пойти на хитрость, на которую пошел А.И. Кострикин в своей книжке: сначала он доказывает простоту A_5, у которой порядок не зависит от n, а потому можно разобраться с делимостями; а потом из простоты A_5 с помощью метода математической индукции он "получает" простоту A_n для $n \geq 5$. "Получает" взято в кавычки, потому что индуктивный переход он оставляет читателям в качестве упражнения, хотя и дает максимально подробные указания.

Задачи для самостоятельной работы

- *Изоморфны ли группы S_5 и D_{60}?*
- *Найти число классов сопряженности в A_9?*
- *Вычислить $[G, G], Z(G)$ и $G/[G, G]$ для $G = D_{2n+1}$.*
- *Описать все нормальные подгруппы группы S_4.*
- *Доказать, что в A_5 нет нетривиальных нормальных подгрупп вторым способом, т.е. исследуя мощности классов сопряженности.*

Гомоморфизмы групп

Гомоморфизмы групп - это отображения между группами, уважающие групповую структуру, более формально:

Определение

Отображение $\alpha : G \to H$ *называется гомоморфизмом, если*

$\alpha(g^{-1}) = (\alpha(g))^{-1}$ *для всех* $g \in G$

$\alpha(gh) = \alpha(g)\alpha(h)$ *для всех* $g, h \in G$

Гомоморфизмы удовлетворяют следующим простым свойствам:

• $\alpha(e_G) = e_H$, действительно, для всякого $g \in G$ (любая группа G не пуста, потому что как минимум в G есть e_G) будет выполнено:

$$\alpha(e_G) = \alpha(gg^{-1}) = \alpha(g)\alpha(g^{-1}) = \alpha(g)(\alpha(g))^{-1} = e_H$$

• Пусть $\alpha : G \to H$, $\beta : H \to K$ - гомоморфизмы, тогда $\beta \circ \alpha : G \to K$ тоже гомоморфизм (очевидно, так как если каждое отображение уважает операции умножения и взятия обратного, то и композиция тоже будет их уважать). Отмечу, что на множестве гомоморфизмов $\{\alpha : G \to H\}$ нет никакой естественной структуры за исключением случая, когда H - абелева: тогда множество гомоморфизмов превращается в абелеву группу с операцией поточечного сложения (в аддитивной форме H). Также огромную роль в теории групп играет *группа автоморфизмов*, которую мы будем проходить далее и которая определяется как множество биективных гомоморфизмов $\{\alpha : G \to G\}$ с операцией композиции, типично, что группа автоморфизмов будет неабелевой. На множестве гомоморфизмов $\{\alpha : G \to H\}$ вы не сможете определить композицию, так как область определения не совпадает с образом.

• $\mathrm{ord}(g)$ делится на $\mathrm{ord}(\alpha(g))$ для любого $g \in G$. Действительно, пусть $n = \mathrm{ord}(g)$, тогда $(\alpha(g))^n = \alpha(g^n) = e$, а так как любая степень, в которой элемент равен нейтральному, делится на порядок элемента, то и n делится на $\mathrm{ord}(\alpha(g))$. Это достаточно простое соображение существенно помогает при изучении гомоморфизмов.

Пример

Описать все гомоморфизмы из $\mathbb{Z}_n$ *в произвольную группу* G.

Будем работать с мультипликативной формой, $\mathbb{Z}_n = \langle x \rangle$. Пусть $x \mapsto g$ отображается в некоторый элемент $g \in G$, тогда:

$$e \mapsto e$$

$$x \mapsto g$$

$$x^2 \mapsto g^2$$

$$\dots\dots\dots$$

$$x^n \mapsto g^n$$

Ясно, что это отображение уважает произведение и взятие обратного, т.к. операция индицируется сложением в степенях. Единственное, что нужно проверить - это корректность отображения, что если элементы совпадали в $\mathbb{Z}_n$, то их образы в G

тоже совпадут. Так как элементы совпадают в $\mathbb{Z}_n$ iff их степени отличаются на число, кратное n, то критерием корректности будет:

$$x^n \mapsto e$$

Иными словами происходящие в $\mathbb{Z}_n$ зацикливание происходит и в G. Таким образом, произвольный гомоморфизм $\alpha : \mathbb{Z}_n \to G$ задается некоторым элементом $g \in G$, таким что $g^n = e$; и задается на порождающем формулой $\alpha(x) = g$ и корректно продолжается до гомоморфизма всей группы при условии $g^n = e$.

Замечание:

Нетрудно понять, что значения на порождающих элементах полностью восстанавливают гомоморфизм, так как тогда в силу определения восстанавливаются значения и на произвольных произведениях и обратных, а они дают всю группу. Однако замечу, что задание образов порождающих элементов не всегда продолжается до гомоморфизма всей группы, так как между порождающими типично, что есть соотношения, которые должны выполняться и в образе, как хорошо видно в только что разобранном примере $\mathbb{Z}_n$ и соотношения $x^n = e$. Или приведем другой пример: если продублировать какой-нибудь порождающий группы, а именно $G = \langle g, g, x, y, \ldots \rangle$ и попытаться задать α на порождающих так, что значение на "первом" g будет отличаться от значения на "втором", то никакому гомоморфизму это не будет соответствовать. Немного забегая вперед скажу, что если группа задана копредставлением $G = \langle A|R \rangle$, то заданное на A отображение продолжается до гомоморфизма всей группы iff каждый элемент из "базисных" соотношений R переходит в 1.

Пример

Описать все гомоморфизмы из $\mathbb{Z}$ в произвольную группу G.

Здесь ситуация еще проще, так как если порождающий $x \in \mathbb{Z} = \langle x \rangle$ отправить в произвольный элемент $g \in G$, то такое отображение всегда можно продолжить до гомоморфизма всей циклической группы:

$$e \mapsto e$$

$$x \mapsto g$$
$$x^2 \mapsto g^2$$
$$x^{-1} \mapsto g^{-1}$$

$$\ldots\ldots\ldots$$

Ясно, что таким образом продолженное отображение будет удовлетворять аксиомам гомоморфизма, так как произведению соответствует удовлетворяющее аксиомам группы сложение степеней, корректность в отличие от предыдущего примера проверять не нужно: так как в $\mathbb{Z}$ нет никаких тривиальных соотношений, т.е. зацикливания.

Таким образом произвольный гомоморфизм задается образом порождающего, без каких-либо на него условий. А потому - гомоморфизмов $\{\mathbb{Z} \to G\}$ столько, сколько элементов группы G.

Пример

Описать все гомоморфизмы в следующих случаях:

- $\mathbb{Z}_{10} \to \mathbb{Z}_6$
- $\mathbb{Z}_7 \to \mathbb{Z}_5$

Используем данное выше описание гомоморфизмов из конечных циклических групп:

1) Пусть $\mathbb{Z}_{10} = \langle x \rangle$ и $\mathbb{Z}_6 = \langle y \rangle$, тогда $\alpha : \mathbb{Z}_{10} \to \mathbb{Z}_6$ заданное на порождающем $\alpha(x) = y^k$ (можем считать $0 \leq k < 6$), продолжается до гомоморфизма $\Leftrightarrow y^{10k} = e$, то есть $10k$ делится на 6, что эквивалентно $2 \cdot 5 \cdot k = 6m \Leftrightarrow 5k = 3m \Leftrightarrow k$ делится на 3. Этому условию удовлетворяют в точности $k = 0, 3$. Таким образом существует лишь два гомоморфизма:

$$\alpha_1(x^m) = e$$

$$\alpha_2(x^m) = y^{3m}$$

2) Все совершенно аналогично: $\mathbb{Z}_7 = \langle x \rangle$, $\mathbb{Z}_5 = \langle y \rangle$, $\alpha(x) = y^k$, условие для продолжения до гомоморфизма: $7k$ делится на 5, но в силу взаимной простоты 5 и 7 этому условию удовлетворяет только $k = 0$ (разумеется мы рассматриваем числа по модулю 5, так как эти числа - степени порождающего элемента из $\mathbb{Z}_5$). Таким образом существует только один тривиальный гомоморфизм из $\mathbb{Z}_7$ в $\mathbb{Z}_5$, отправляющий все $\mathbb{Z}_7$ в тривиальный элемент. Эти рассуждения можно сформулировать чуть иначе: мы помним, что для любого гомоморфизма $\operatorname{ord}(x) = 7$ делится на $\operatorname{ord}(\alpha(x))$, а потому $\alpha(x)$ имеет либо порядок 7 (что невозможно в $\mathbb{Z}_5$), либо 1, иными словами $\alpha(x) = e$ для порождающего x, а значит и гомоморфизм тривиален.

Задача

Пусть $\varphi : G \to K$ - гомоморфизм. Тогда

$$\ker \varphi = \{g \in G : \varphi(g) = e\} \lhd G$$

Во первых нужно проверить, что ядро - это подгруппа, пусть $x, y \in \ker \varphi$, тогда:

$$\varphi(x^{-1}) = (\varphi(x))^{-1} = e \quad \Longrightarrow \quad x^{-1} \in \ker \varphi$$

$$\varphi(xy) = \varphi(x)\varphi(y) = e \quad \Longrightarrow \quad xy \in \ker \varphi$$

Проверим нормальность ядра, пусть $g \in G, h \in \ker \varphi$:

$$\varphi(g^{-1}hg) = (\varphi(g))^{-1}e\varphi(g) = e \quad \Longrightarrow \quad g^{-1}hg \in \ker \varphi$$

Очень важное замечание:

На самом деле верно и обратное утверждение, а именно что любая нормальная подгруппа получается как ядро некоторого гомоморфизма: достаточно для $H \lhd G$ рассмотреть канонический гомоморфизм $\pi : G \to G/H$, у которого ядро в точности совпадает с H. Это наблюдение позволяет провести глубочайшую параллель между теорией нормальных подгрупп и теорией гомоморфизмов: потому что по большому счету в некотором смысле - это одно и то же: и вы можете изучать одно методами другого. Например, вы можете без устали клепать нормальные

подгруппы, коль скоро вы наладили стабильное производство гомоморфизмов, или наоборот - многое сказать о гомоморфизмах, если вы досконально разобрались с нормальными подгруппами.

Пример

Описать все гомоморфизмы

- $\mathbb{Z} \to A_5$
- $A_5 \to \mathbb{Z}$

---

1) Вспоминаем описание всех гомоморфизмов из циклической группы в произвольную: для произвольного $g \in A_5$ отображение

$$\alpha(\text{порождающий } \mathbb{Z}) = g$$

однозначно и корректно продолжается до гомоморфизма на всей $\mathbb{Z}$ даже без дополнительных условий на g (в отличие от конечных циклических групп $\mathbb{Z}_n$). К примеру, если использовать аддитивную форму записи $\mathbb{Z}$, то гомоморфизм будет выглядеть так: $\alpha(0) = e, \alpha(1) = g, \alpha(2) = g^2, \alpha(3) = g^3, \ldots$. Таким образом всего гомоморфизмов 60 штук (в точности столько, сколько элементов A_5).

2) Согласно предыдущему утверждению для $\alpha : A_5 \to \mathbb{Z}$ имеем $\ker\alpha \lhd A_5$. Ранее мы доказывали, что A_5 является простой группой, а потому в ней отсутствуют нетривиальные нормальные подгруппы. Таким образом либо $\ker\alpha = \{e\}$, либо $\ker\alpha = A_5$. Первый случай невозможен, т.к. тогда гомоморфизм бы был инъективен, но A_5 неабелева и не может быть гомоморфно вложена в абелеву группу (или можно рассуждать так: в A_5 есть элементы разных конечных порядков (подумайте какие именно порядки могут быть у элементов группы A_5), тогда как в $\mathbb{Z}$ нет нетривиальных элементов конечного порядка). Таким образом остается лишь второй случай $\ker\alpha = A_5$, который в точности означает, что гомоморфизм тривиален, т.к. все переводится в нейтральный элемент, т.е. существует лишь один гомоморфизм из A_5 в $\mathbb{Z}$.

Замечание

По итогам доказательства второго пункта можно сделать следующий вывод: что гомоморфизмов из простых групп очень мало (они сводятся лишь к тривиальным и инъективным). Простейшие примеры конечных простых групп следующие: A_n при $n \geq 5$ и $\mathbb{Z}_p$ при простом p. Попробуйте придумать какой-нибудь пример бесконечной простой группы.

Пример

Описать все гомоморфизмы

- $\mathbb{Z}_3 \to S_3$
- $S_3 \to \mathbb{Z}_3$

---

1) В первом случае как уже неоднократно повторялось: гомоморфизмы однозначно задаются элементами, такими, что $g^3 = e$ (выступающими в роли образа порождающего $\mathbb{Z}_3$); таких элементов в S_3 три штуки: $\{e, (123), (132)\}$, значит всего существует 3 гомоморфизма.

2) Пусть $\alpha : S_3 \to \mathbb{Z}_3$. Так как для любой транспозиции выполняется $(ij)^2 = e$, то $(\alpha(ij))^2 = e$, но в $\mathbb{Z}_3$ только e в квадрате дает нейтральный (либо вместо этих

рассуждений можно было воспользоваться одним из упомянутых выше свойств, что порядок элемента делится на порядок его образа, а значит если $\mathrm{ord}(ij) = 2$, то $\mathrm{ord}(\alpha(ij))$ должен делиться на 2, а в $\mathbb{Z}_3$ этому условию удовлетворяет только нейтральный элемент). В любом случае получаем:

$$\alpha(ij) = e$$

А так как транспозиции порождают S_3, то $\alpha(\sigma) = e$ для любой перестановки $\sigma \in S_3$. Значит существует только тривиальный гомоморфизм $S_3 \to \mathbb{Z}_3$.

==========

Теорема о гомоморфизме

Пусть $\varphi : G \to F$ - гомоморфизм, тогда:

$$\boxed{G/\ker\varphi \cong \operatorname{Im}\varphi}$$

==========

Изоморфизм здесь явно строится:

$$g\ker\varphi \mapsto \pi(g)$$

И для доказательства этой теоремы нужно аккуратно проверить, что это отображение является корректно определенным биективным гомоморфизмом.

Во-первых отмечу, что природа этой теоремы - общекатегорна, т.е. в любой разумной категории, где есть факторы - фактор по ядру изоморфен образу морфизма (вспомните фактор-пространства из линала). Во-вторых, теорема эта очень важная (одна из самых важных), потому что на практике очень многие группы получаются как некоторые факторы (те же копредставления групп определяются как факторы) - и эта теорема позволяет сводить изучение немного абстрактной состоящей из каких-то непонятных смежных классов фактор-группы ко вполне понятному образу, который легко вычисляется, так как совпадает с подгруппой, порожденной образами порождающих элементов группы G - и это главная стезя применения этой теоремы.

Возвращаясь к более практическим насущным вопросам - если Вам нужно описать некоторую фактор-группу G/H, то обычно подбирается некоторый гомоморфизм $\varphi : G \to F$ в некоторую группу F, такой, что $\ker\varphi = H$. Тогда по теореме о гомоморфизме $G/H \cong \operatorname{Im}\varphi$ (в силу ранее упомянутой двойственности между гомоморфизмами и нормальными подгруппами такой φ всегда найдется, теоретически можно взять $\varphi : G \to G/H$, но практически это совершенно бесполезно, т.к. вы этот гомоморфизм ищете как раз для того чтобы G/H найти). В роли φ обычно выступает какой-нибудь крайне естественный гомоморфизм, в поиске которого помогает опыт, интуиция и минимальный здравый смысл (к примеру, если порядок фактора должен получиться очень большой - бессмысленно в качестве F пытаться искать маленькую группу). Также отмечу, что не нужно фанатично гнаться за совпадением $\operatorname{Im}\varphi = F$, так как во многих ситуациях $\operatorname{Im}\varphi < F$ оказывается намного естественнее, и лишь потом вы уже будете выяснять, какую именно подгруппу в F представляет $\operatorname{Im}\varphi$, хотя в учебных задачах чаще всего вы будете сталкиваться именно с ситуацией равенства $\operatorname{Im}\varphi = F$.

Также уточню, что иногда фактор-группу можно легко найти из других соображений: к примеру, если получается, что порядок вашей фактор-группы простое число - то безо всяких гомоморфизмов понятно, что она будет циклическая - об этом не забывайте.

Пример

Описать следующие фактор-группы:

- $\mathbb{Z}/n\mathbb{Z}$
- $GL_n(F)/SL_n(F)$, *где* F - *поле*
- $\mathbb{Z}_{125}/\mathbb{Z}_5$
- A_4/V_4
- $\mathbb{R}/\mathbb{Z}$

---

1) $\mathbb{Z}/n\mathbb{Z}$. Рассмотрим гомоморфизм: $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, заданный формулой

$$x \mapsto x \mod n$$

в аддитивной записи. Тогда ясно, что это гомоморфизм, что он сюръективный, а значит $\operatorname{Im}\varphi = \mathbb{Z}_n$, и что $\ker\varphi = n\mathbb{Z}$ - т.е. в ноль переходят в точности числа, кратные n. Таким образом по теореме о гомоморфизме получаем $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

2) $GL_n(F)/SL_n(F)$. Где-где, а в этом случая совершенно ясно, какой гомоморфизм стоит брать, чтобы его ядро в точности состояло из $SL_n(F)$ (какой нужно взять гомоморфизм, чтобы матрицы, переходящие под действием определителя в 1, переходили бы в 1?). Рассмотрим $\det : GL_n(F) \to F^*$, являющийся гомоморфизмом в группу ненулевых элементов поля по умножению. Ясно, что $\ker(\det) = SL_n(F)$ по определению $SL_n(F)$. При этом $\operatorname{Im}\det = F^*$, так как для любого ненулевого числа x существует матрица (например $\operatorname{diag}(x, 1, \ldots, 1)$), с равным x определителем. Тогда по теореме о гомоморфизме мы получаем

$$GL_n(F)/SL_n(F) \cong F^*$$

3) $\mathbb{Z}_{125}/\mathbb{Z}_5$. Мы с вами помним полное описание подгрупп конечной циклической группы, в частности для каждого делителя порядка циклической группы существует в точности одна подгруппу с таким порядком, иными словами существует лишь один способ вложения $\mathbb{Z}_5 < \mathbb{Z}_{125}$, рассмотрим сюръективный гомоморфизм:

$$\varphi : \mathbb{Z}_{125} = \langle x \rangle \to \mathbb{Z}_{25} = \langle y \rangle$$

$$x \mapsto y^5$$

Таким образом $\mathbb{Z}_{125}/\ker\varphi \cong \operatorname{Im}\varphi = \mathbb{Z}_{25}$, из соображений мощности получаем, что $|\ker\varphi| = 5$. В силу единственности подгруппы порядка 5 мы получаем равенство $\ker\varphi$ тому самому $\mathbb{Z}_5$, а значит и изоморфизм:

$$\mathbb{Z}_{125}/\mathbb{Z}_5 \cong \mathbb{Z}_{25}$$

Но идеологически эту задачу правильнее и проще решать немного иначе: заметим, что если $\pi : G \to G/H$ - канонический фактор-гомоморфизм, и если $G = \langle g_1, g_2, \ldots \rangle$, то $G/H = \langle g_1H, g_2H, \ldots \rangle = \langle \pi(g_1), \pi(g_2), \ldots \rangle$, откуда сразу можно сделать крайне полезный вывод:

Минимальное количество порождающих для фактор группы G/H всегда не превосходит минимального числа порождающих для G.

В частности для нашей задачи: если группа G порождается одним элементом, т.е. циклична, тогда и любой ее фактор тоже будет цикличен. По формуле индекса получается, что $|\mathbb{Z}_{125}/\mathbb{Z}_5| = 25$, а значит $\mathbb{Z}_{125}/\mathbb{Z}_5 \cong \mathbb{Z}_{25}$.

4) A_4/V_4. Здесь все еще проще, так как по формуле для индекса $|A_4/V_4| = 3$, то из-за того, что 3 - простое число, а мы помним, что группы простого порядка обязаны быть циклическими, то $A_4/V_4 \cong \mathbb{Z}_3$.

В частности канонический гомоморфизм будет гомоморфизмом $A_4 \to Z_3$, в существование которого довольно сложно поверить без знания теоремы о гомоморфизме. Сам гомоморфизм зависит от отождествления $A_4/V_4 \cong \mathbb{Z}_3$, которое можно подкрутить на автоморфизм $\mathbb{Z}_3$. Одним из таких гомоморфизмов будет следующий: $V_4 \mapsto 0$, $(123)V_4 \mapsto 1$, $(132)V_4 \mapsto 2$. Другой получается, если поменять местами образы двух нетривиальных смежных классов. Также замечу, что этим списком исчерпываются все нетривиальные гомоморфизмы $\varphi : A_4 \to \mathbb{Z}_3$, так как если гомоморфизм нетривиален, то в его образе есть нетривиальный элемент, а так как $\operatorname{Im}\varphi < \mathbb{Z}_3$, то в силу того, что в $\mathbb{Z}_3$ отсутствуют нетривиальные подгруппы - мы получаем, что $\operatorname{Im}\varphi = \mathbb{Z}_3$, в частности из теоремы о гомоморфизме вытекает, что раз $|A_4| = 12$, а $|\operatorname{Im}\varphi| = 3$, то $|\ker\varphi| = 4$; но мы с вами ранее описывали все подгруппы группы A_4 и хорошо помним, что кроме V_4 подгрупп порядка 4 в A_4 нет. Значит при этом гомоморфизме $V_4 \mapsto 0$, значит $(123)V_4$ отправляется либо в 1 либо в 2, соответственно $(132)V_4$ в другой оставшийся для него элемент. Ясно, что построенное отображение является гомоморфизмом, так как оно является композицией двух гомоморфизмов $A_4 \to A_4/V_4 \to \mathbb{Z}_3$, и по ходу рассуждений ясно, что других быть не может. То есть грубо говоря, из-за того, что в A_4 существует только одна нормальная подгруппа порядка 4 - любой гомоморфизм $A_4 \to \mathbb{Z}_3$ пропускается чеpед $A_4 \to A_4/V_4 \to \mathbb{Z}_3$, и с такими жесткими ограничениями их не может быть много.

5) Для описания $\mathbb{R}/\mathbb{Z}$ рассмотрим гомоморфизм

$$\varphi : \mathbb{R} \to \mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$$

заданный формулой $x \mapsto e^{2\pi i x}$. Ясно, что это - гомоморфизм, что он эпиморфен (эпиморфизмами называют сюръективные морфизмы в некоторой категории, например, сюръективные гомоморфизмы в теории групп, сюръективные линейные отображения в линале и т.д.), а значит $\operatorname{Im}\varphi = \mathbb{T}$, также легко проверяется $\ker\varphi = \mathbb{Z}$. Таким образом $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$.

Пример

Пусть

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a > 0, b \in \mathbb{R} \right\}$$

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}$$

Доказать, что $H \lhd G$ и найти G/H.

Обратная к треугольной 2×2 матрице легко угадывается (или вычисляется по формуле), тогда нормальность H получается из:

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{x} & -\frac{y}{x} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & bx \\ 0 & 1 \end{pmatrix} \in H$$

Примерно ясно, куда нужно строить гомоморфизм, так как процедура факторизации фактически является процедурой отождествления-склейки, призывающая

фактически отождествлять матрицы из H с единичной, что означает, что b при факторизации "умирает", такими образом выжившим параметром останется a - а значит нужно искать гомоморфизмы в группу, которые бы хорошо "параметризовались" возможными значениями параметра a. Но здесь ситуация существенно более простая, чем в "общем" случае: заметим, что множество всевозможных значений параметра a само образует группу $\mathbb{R}_+$ положительных чисел по умножению.

Перейдем к деталям: для описания фактор-группы рассмотрим гомоморфизм $\varphi : G \to \mathbb{R}_+$, заданный формулой $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto a$. Перемножая и беря обратные от такого типа матриц мы убеждаемся, что это - гомоморфизм, также замечаем, что он сюръективный, и что ядро в точности совпадает с H. Таким образом $G/H \cong \mathbb{R}_+$.

Также в этом разделе мне хочется рассказать вам о решении задачи об отсутствии подгрупп порядка 6 в A_4 с помощью теории нормальных групп:

Пример

Докажем другим способом, что в A_4 нет подгрупп порядка 6.

Пусть существует $H < A_4$, такая, что $|H| = 6$. Так как ее индекс равен 2, то по доказанному ранее свойству получаем $H \lhd A_4$. Рассмотрим канонический гомоморфизм $\pi : A_4 \to A_4/H \cong \mathbb{Z}_2$, для которого $\ker \pi = H$. По свойствам гомоморфизма $\operatorname{ord}(x)$ всегда делится на $\operatorname{ord}(\pi(x))$. Тогда для перестановок циклического типа $x = (***) \in A_4$ мы получаем $\operatorname{ord}(x) = 3$, $\operatorname{ord}(\pi(x))$ делит 3, но при этом $\pi(x) \in \mathbb{Z}_2$, где порядками элементов могут быть только 2 и 1, откуда получаем, что порядок должен быть равен 1, а значит $\pi(x) = e$ для всех тройных циклов x. А дальше можно либо сказать, что:

• Перестановок типа (***) 8 штук, тогда $|\ker \pi| \geq 8$, но при этом $|\ker \pi| = |H| = 6$.

• Либо сказать, что тройные циклы порождают A_n, а так как ядро - это подгруппа, то $A_4 < \ker \pi$, но при этом $|\ker \pi| = 6$

В любом случае мы приходим к противоречию.

Следующая теорема как и теорема о гомоморфизме помогает описывать факторы, правда несмотря на ее безусловную фундаментальность - она не такая важная как теорема о гомоморфизме, и область ее применения очень специфична; но знать ее крайне желательно, хотя и без нее (в отличие от теоремы о гомоморфизме) можно прожить вполне счастливую математическую жизнь.

Теорема (I об изоморфизме)
Пусть $H \lhd G$ и $K < G$. Тогда $HK < G$ и

$$\boxed{K/(H \cap K) \cong HK/H}$$

То, что $HK < G$ проверяется просто, проверим, к примеру, замкнутость относительно умножения:

$$h_1k_1h_2k_2 = h_1(k_1h_2k_1)^{-1}k_1k_2 \in HK$$

Изоморфизм тоже строится явно:

$$k(H \cap K) \mapsto kH$$

Также отмечу, что $hk = k(k^{-1}hk)$, а потому из нормальности H мы получаем, что $hkH = kH$ для любого h: а потому вас не должен смущать странный визуальный вид изоморфизма, кажется, словно он покрывает очень мало классов в HK/H. Безусловный пафос этой теоремы, разумеется, в том, что она сводит задачу описания фактор-группы к задаче описания фактор-группы с более простыми компонентами, так как $H \cap K < H$ и $H < HK$; и в большинстве случаев это существенно упрощает задачу. Таким образом, если пытаться описывать границы и способ применения этой теоремы, то можно сказать следующее:

Если вам нужно описать фактор G/H - то вы пытаетесь найти "секущую" подгруппу K, такую, что $HK = G$. Тогда задача описания фактора существенно упрощается: т.к. мы приходим к ситуации $K/(H \cap K)$ с более простыми компонентами (по крайней мере с точки зрения порядков групп).

Классический пример применения I теоремы об изоморфизме
Описать фактор-группу S_4/V_4.

Порядок $|S_4/V_4| = 6$ - мы не так много знаем групп порядка 6 (их в принципе с точностью до изоморфизма 2 штуки), так что скорее всего настраиваться нужно на то, что фактор будет изоморфен S_3, но возможность применения теоремы о гомоморфизме пока не очень прозрачная, так как никакой простой и естественный гомоморфизм $\pi : S_4 \to S_3$ не напрашивается. Довольно легко проверить, что S_4/V_4 - не абелева, и если знать, что S_3 - единственная неабелева группа порядка 6, то доказательство на этом можно закончить. Но мы пока этого факта не знаем. Есть еще один подход: я бы не сказал, что перебор 6 элементов какой-то очень заоблачный: теоретически можно выписать все 6 смежных классов и составить их таблицу умножения, либо даже пойти на небольшие хитрости (использование пройденного материала поможет существенно упростить выкладки, к примеру элемент $(12)V_4$ имеет порядок 2, элемент $(123)V_4$ имеет порядок 3.

$$[(12)V_4] \cdot [(123)V_4] \cdot [(12)V_4]^{-1} = (12)(123)(12)^{-1}V_4 = (213)V_4 = [(123)V_4]^{-1}$$

и это равенство есть в точности мясорубочное соотношение из D_3, и если чуть поднажать - то можно понять, что $S_4/V_4 \cong D_3 \cong S_3$: более-менее ясно, что у $(12)V_4$ и $(123)V_4$ такая же таблица умножения, как и у порождающих b, a группы D_3, из

этого в частности вытекает, что подгруппа, порожденная $(12)V_4$ и $(123)V_4$, имеет порядок 6, но так как $|S_4/V_4| = 6$, то они порождают весь фактор. Используя теорию копредставлений такие рассуждения можно превратить в конфетку (а именно используя копредставление $D_3 = \langle a, b | a^3 = b^2 = 1, b^{-1}ab = a^{-1} \rangle$ группы Диэдра), но в такой форме доказательство очень муторное и тяжеловесное, после него остается неприятный осадок осознания идейной опустошенности доказательства (возились с соотношениями, что-то перемножали... и под конец получили изоморфизм). Однако есть классическое простое решение с помощью I теоремы об изоморфизме:

Рассмотрим $G = S_4$, $H = V_4$ и секущую подгруппу $K = S_3 < S_4$ состоящую из перестановок, оставляющих неподвижным последний элемент. Тогда легко понять, что $H \cap K = \{e\}$. Тогда если $h_1k_1 = h_2k_2$, то $H \ni h_2^{-1}h_1 = k_2k_1^{-1} \in K$, и из тривиальности пересечения мы получаем $h_1 = h_2$ и $k_1 = k_2$, что означает, что $|HK| = |H| \cdot |K|$. Для наших подгрупп мы имеем $|H| = 4$, $|K| = 6$, а значит $HK = S_4$. Таким образом I теорема об изоморфизме примененная к нашим подгруппам дает следующий изоморфизм:

$$S_4/V_4 \cong S_3$$

Замечание:

Есть еще красивое доказательство с использованием теории действий, которую мы обсудим чуть позже, но доказательство приведу сейчас: обозначим через X трехэлементное множество неединичных перестановок из V_4. Циклический тип при сопряжении сохраняется, а значит S_4 действует сопряжениями на этом множестве: $\pi : S_4 \curvearrowright X$:

$$\pi : S_4 \to S(X) \cong S_3$$

$$\pi_\sigma(x) = \sigma^{-1}x\sigma$$

Таким образом самый сложный шаг пройден: с помощью действий мы получили явную формулу для гомоморфизма $\pi : S_4 \to S_3$ - и чтобы применить теорему о гомоморфизме - осталось доказать, что $\ker \pi = V_4$ и $\operatorname{Im} \pi = S_3$. Начнем со второго: для проведения конкретных технических выкладок перенумеруем перестановки из X:

$$(12)(34) \leftrightarrow I$$

$$(13)(24) \leftrightarrow II$$

$$(14)(23) \leftrightarrow III$$

Будем использовать римские цифры для нумерации элементов X, чтобы не путать перестановки из S_4 и из его образа S_3. Заметим, что

$$[(1234)][(12)(34)][(1234)]^{-1} = (23)(41)$$

$$[(1234)][(23)(41)][(1234)]^{-1} = (34)(12)$$

Ясно, что при сопряжении оставшийся элемент остается неподвижным. Эти соотношения на языке действий означают:

$$\pi((1234)^{-1}) = (I, III)$$

Минус первая степень возникла потому, что действие сопряжением задается формулой $x \mapsto \sigma^{-1}x\sigma$, тогда как волшебная формула, когда моментально можно написать результат сопряжения, выписывается для $\sigma x \sigma^{-1}$, причем

в действии минус первую степень нельзя поставить справа, потому что в таком случае действие уже будет не гомоморфизмом в $S(X)$, как положено, а антигомоморфизмом, т.е. меняющим порядок. Типичный пример антигомоморфизма - это $x \mapsto x^{-1}$.

Теперь, если в образе мы получили перестановку (I, III), то с помощью подходящей перенумерации мы сможем получить на самом деле любую транспозицию в образе, но образ - это подгруппа, а S_3 порождается транспозициями, таким образом $\operatorname{Im}\pi = S_3$.

Дальше замечаем, что раз V_4 - абелева группа, то сопряжение элементами V_4 оставляет все элементы V_4 неподвижными, а это в точности означает, что $V_4 < \ker\pi$. А теперь, заметим, что теорема о гомоморфизме в данном случае даже позволяет не мучиться с доказательством равенства, потому что из $S_4/\ker\pi \cong \operatorname{Im}\pi$, из $|S_4| = 24$ и $|\operatorname{Im}\pi| = 6$ автоматически вытекает, что $|\ker\pi| = 4$, таким образом в точности $\ker\pi = V_4$ и значит по лемме о гомоморфизме: $S_4/V_4 \cong S_3$.

И завершает вереницу упрощающих описание фактор-группы теорем - самая непопулярная:

Теорема (II об изоморфизме)
Пусть $K, H \lhd G$ и $K < H$. Тогда

$$\boxed{G/H \cong (G/K)/(H/K)}$$

Мнемонически формулировку теоремы легко запомнить - так как если фактор-группы воспринимать как дроби, то при "сокращении" правой части на K в точности получится левая часть. Немного поясню формулировку: ясно, что если $K < H$ и $K \lhd G$, то и $K \lhd H$, так что H/K корректно определена.

Ценность этой теоремы больше теоретическая (обычно бонусом к этой теореме прилагается теорема о взаимно-однозначном соответствии между множеством подгрупп (нормальных подгрупп) $H < G$, содержащих K, и множеством всех подгрупп (соответственно нормальных подгрупп) G/K; хотя ясно, что при работе с обычными подгруппами мы не требуем нормальности H в условии: а именно верно, что при $K < H < G$ с одной стороны $H/K < G/K$, а с другой стороны любая $F < G/K$ равна $F = H/K$ для некоторой $K < H < G$). Но реально на практике этой теоремой очень сложно воспользоваться: главным образом потому, что в жизни очень редко встречаются фактор группы по фактор-группе (четырехэтажные факторы), но чтобы не быть совсем оторванным от реальности - покажем ее применение на одном довольно неестественном примере:

Пример

Описать фактор-группу следующих фактор-групп: $(\mathbb{Z}_{125}/\mathbb{Z}_5)/(\mathbb{Z}_{25}/\mathbb{Z}_5)$.

Пусть $G = \mathbb{Z}_{125}$, $H = \mathbb{Z}_{25}$, $K = \mathbb{Z}_5$. Тогда согласно II теореме об изоморфизме:

$$(\mathbb{Z}_{125}/\mathbb{Z}_5)/(\mathbb{Z}_{25}/\mathbb{Z}_5) \cong \mathbb{Z}_{25}/\mathbb{Z}_5$$

Последний фактор мы уже обсуждали как описывать - фактор циклической группы является циклическим и имеет по формуле для индекса порядок 5, таким образом исходная группа изоморфна $\mathbb{Z}_5$.

Замечание:

Из того, что происходило ранее могло сформироваться интуитивное представление, что с G/H в некотором роде можно работать как с дробью. Частично это так, но далеко не полностью. Показательным будет следующий пример: рассмотрим $G = \mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ с операцией умножения, и пусть $H = \{-1, 1\} \cong \mathbb{Z}_2$. Из абелевости G вытекает, что $H \lhd G$, но при этом $G/H \cong G$, и изоморфизм задается формулой $z\{1, -1\} \mapsto z^2$ (геометрически это понять очень легко: если вы склеиваете диаметрально противоположные точки окружности то снова получится окружность: словно вы выкинули половину окружности (так как она приклеивается к противоположной половине), а полученные граничные точки склеили между собой). Таким образом фактически $G/H \cong G/\{e\}$, но при этом $H \ncong \{e\}$. Группы, для который из $G/H \cong G$ вытекает $H = \{e\}$ называются хопфовыми и мы о них поговорим в самом конце методички.

Действия групп

Специально изучающая действия различных групп дисциплина называется "Теорией динамических систем", чтобы понять значимость этого раздела скажу лишь, что на сайте arxiv.org, где почти все математики обычно выкладывают свои свежие результаты - "Теория групп" и "Динамические системы" являются отдельными равнозначными разделами. В динамических системах тоже есть свое разделение: например, действия непрерывных групп больше тяготеет к геометрии и дифференциальным уравнениям, где обычно возникает необходимость в анализе действия группы $\mathbb{R}$ на фазовом пространстве, которое "сдвигает" состояние системы по времени, задавая эволюцию системы. Действия группы $\mathbb{Z}$ задают дискретную эволюцию системы, когда время может идти только с шагом 1.

Стоит также сказать, что в некотором смысле понятие действия группы появилось даже исторически раньше самих групп, так как изначально математики воспринимали группы как замкнутое относительно композиции и взятие обратного подмножество биекций некоторого множества - и только потом поняли, что их можно задавать аксиоматически, оторвавшись от привязки к действиям. Также скажу, что с помощью действий типично, что получаются самые красивые доказательства, так как именно здесь смыкаются два в некотором смысле диаметрально противоположных раздела математики: олицетворяющая алгебру теория групп и геометрия в виде действия группа на пространствах. Более того, с помощью действий очень часто удается решить задачи, в изначальной постановке далекие от действий в принципе. Поэтому *если по жизни не получается какая-то математическая задача - то ищите действие некоторой группы.* Действия очень важны и в физике, потому что одно из ключевых понятий физических симметрии связано с действиями самым непосредственным образом.

Определение

Действием группы называется гомоморфизм $\pi : G \to S(X)$ группы G в группу симметрий $S(X)$ некоторого множества X. Довольно часто в таком случае пишут $\pi : G \curvearrowright X$.

Иными словами каждому элементу группы сопоставляется некоторая биекция множества X, таким образом, что это сопоставление является гомоморфизмом. Существует несколько общепринятых обозначений для действия элемента $g \in G$ на конкретном элементе $x \in X$:

$$\pi(g)(x) = \pi(g)x = \pi_g(x) = g \cdot x = gx$$

Как видите иногда опускают π, когда не может возникнуть недоразумений по поводу того, какое действие рассматривается. Группа симметрий $S(X)$ определяется как множество биекций множества X в себя, ясно, что $S(\{1, 2, \ldots, n\}) = S_n$. Если на X есть хорошая структура, то осмысленно рассматривать только уважающую эту структуру биекции, к примеру, в случае топологического пространства X вместо $S(X)$ идейно правильнее рассматривать множество $Homeo(X)$ гомеоморфизмов X в себя, если X - гладкое многообразие - то рассматривают множество диффеоморфизмов, если X - линейное пространство, то биективные линейные преобразования $GL(X)$. Но мы с вами не будем изучать никакие дополнительные структуры - и в нашем изложении мы будем рассматривать X исключительно как "голое" множество, даже если на нем и будет существовать хорошая структура (хотя

если вы обратите внимание, то рассматриваемые нами естественные действия будут сохранять структуру, и внутри должно что-то колоть, если вы попытаетесь задать, скажем, нелинейные действия на линейных пространствах - хотя чисто теоретически никаких препятствий к этому нет). Определим *орбиту* и *стабилизатор*, являющиеся важнейшими характеристиками действия:

$$\boxed{\begin{array}{c}\mathrm{Orb}(x) = Gx = \{gx\}_{g\in G} \subset X \\ \mathrm{St}(x) = \{g \in G : gx = x\} < G\end{array}}$$

Отмечу, что на орбите нет никакой дополнительной структуры - это "голое" подмножество множества X, тогда как стабилизатор является подгруппой и это легко и непосредственно проверяется:

1) $ghx = g(hx) = gx = x \implies gh \in \mathrm{St}(x)$

2) $g^{-1}x = g^{-1}gx = x \implies g^{-1} \in \mathrm{St}(x)$

Также, думаю, понятно откуда взялись такие названия: стабилизатор - это элементы группы "стабилизирующие", т.е. оставляющие на месте. Орбита - это как в космосе орбиты планет: траектория, оставляемая точкой при ее групповой эволюции.

Определение

Действие $\pi : G \curvearrowright X$ называется транзитивным, если существует x, такой что $X = \mathrm{Orb}(x)$.

Определение

Действие $\pi : G \curvearrowright X$ называется точным, если $\pi : G \to S(X)$ является инъективным гомоморфизмом.

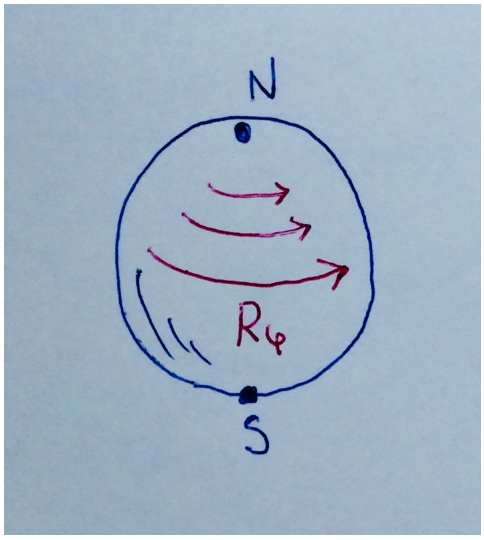
А теперь несколько ключевых примеров, чтобы для вас понятие действий стало более естественным, и свойства более интуитивно осязаемые:

Действие	Формула	Орбиты	Стабилизаторы
$\lambda : G \curvearrowright G$	$\lambda_g(h) = gh$	$\mathrm{Orb}\, h = G$	$\mathrm{St}(h) = \{e\}$
$\lambda : G \curvearrowright G/H$	$\lambda_g(\tilde{g}H) = g\tilde{g}H$	$\mathrm{Orb}(gH) = G/H$	$\mathrm{St}(gH) = gHg^{-1}$
$\mathrm{Ad} : G \curvearrowright G$	$\mathrm{Ad}_g(h) = g^{-1}Hg$	$\mathrm{Orb}(h) = [h]$	$\mathrm{St}(h) = \{h \in G : gh = hg\}$
$\pi : GL_n(F) \curvearrowright F^n$	$\pi_g(x) = gx$	$\mathrm{Orb}(x) = \begin{cases} 0, x = 0 \\ F^n, x \neq 0 \end{cases}$	$\mathrm{St}(x) = \begin{cases} GL_n(F), x = 0 \\ \{g : gx = x\}, x \neq 0 \end{cases}$
$\pi : S_n \curvearrowright \{1, \ldots, n\}$	$\pi_\sigma(m) = \sigma(m)$	$\mathrm{Orb}(m) = \{1, \ldots, n\}$	$\mathrm{St}(m) \cong S_{n-1}$
$\pi : G \curvearrowright X$	$\pi_g(x) = x$	$\mathrm{Orb}(x) = \{x\}$	$\mathrm{St}(x) = G$
$\pi : \mathbb{Z} \curvearrowright \mathbb{R}$	$\pi_n(x) = x + n$	$\mathrm{Orb}(x) = \{x\} + \mathbb{Z}$	$\mathrm{St}(x) = \{0\}$
$\pi : \mathbb{T} \curvearrowright \mathbb{C}$	$\pi_\varphi(z) = e^{i\varphi}z$	$\mathrm{Orb}(z) = \begin{cases} 0, z = 0 \\ \text{окружность}, z \neq 0 \end{cases}$	$\mathrm{St}(z) = \begin{cases} \mathbb{T}, z = 0 \\ 1, z \neq 0 \end{cases}$
$\pi : \mathbb{T} \curvearrowright S^2$	$\pi_\varphi(x) = R_\varphi(x)$	$\mathrm{Orb}(x) = \begin{cases} x, x = N, S \\ \text{окружность}, x \neq S, N \end{cases}$	$\mathrm{St}(x) = \begin{cases} \mathbb{T}, x = S, N \\ 1, x \neq S, N \end{cases}$

Немного прокомментирую табличку: для второго действия $H < G$ - это некоторая подгруппа; стабилизатор находится с помощью простой и прямой проверки:

$$xgH = gH \iff g^{-1}xgH = H \iff g^{-1}xg \in H \iff x \in gHg^{-1}$$

В третьем действии стабилизатор обычно обозначается $\mathrm{St}(h) = C_G(h) < G$ и называется централизатором элемента h. То, что централизатор является подгруппой тоже проверяется простым расписыванием условия коммутации. Четвертое действие вы все должны знать с занятий по линалу - матрица естественным образом действует как оператор на линейном пространстве F^n, правда нам нужно оставить только обратимые матрицы, чтобы был обратный. Стабилизатором ненулевого вектора фактически являются матрицы, для которых этот вектор является собственным с собственным значением 1. В пятом случае действия S_n на n-элементном множестве стабилизатором являются множество перестановок, оставляющих фиксированный элемент неподвижным - это множество естественным образом можно отождествить с помощью с S_{n-1} перестановок оставшихся элементов. Шестой пример обычно называют *тривиальным действием* - любой элемент группы оставляет все точки неподвижными. В последнем примере $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\} = \{e^{i\varphi}\}$ - окружность с естественной групповой структурой сложения углов, S^2 - это двумерная сфера. Через N, S обычно обозначают Северный и Южный полюс соответственно, а R_φ - это поворот на угол φ по широте. Последний пример, на мой взгляд, очень показательный и наглядный. Чтобы лучше привыкнуть к этим очень важным примерам советую вам сделать следующее простое упражнение:



Выяснить какие из перечисленных действия являются точными, какие являются транзитивными.

Сразу же уточню, что точность и транзитивность мало с связаны друг с другом: реализуются все 4 возможности выполнения/невыполнения обоих свойств - и все 4 примера можно отыскать в описанной выше таблице. Скажу больше - их даже можно найти среди тривиальных действий:

- Точное+Транзитивное: тривиальное действие группы $\{e\}$ на одноэлементном множестве.
- Точное+Транзитивное: тривиальное действие группы $\{e\}$ на множестве, состоящем более чем из 1 элемента.
- Точное+Транзитивное: тривиальное действие неединичной группы на одноэлементном множестве
- Точное+Транзитивное: тривиальное действие неединичной группы на множестве, состоящем более чем из 1 элемента.

Попробуйте найти все 4 примера среди нетривиальных действий. Замечу, что хотя по определению транзитивность - это совпадение некоторой орбиты со всем X, но на самом деле *любая орбита* транзитивного действия совпадает с X - это легко проверяется: пусть даны две точки $x, y \in X$ и пусть $Gx = X$, тогда $gx = y$ для некоторого $g \in G$, а значит $Gy = Ggx = Gx = X$.

Есть еще одно крайне важное понятие *свободного действия*, акцент на которое я не делаю исключительно из-за того, чтобы не перегружать изложение. По определению, действие называется свободным, если $gx \neq x$ для любой $x \in X$ и любого $g \neq e$, человеческими словами это означает, что все неединичные элементы группы двигают абсолютно все точки без исключения (в этих терминах точные действия - это те, в которых неединичные элементы сдвигают хотя бы одну точку). Ясно, что если действие свободное - то оно заведомо точное, но не наоборот: так как в свободных действиях сдвигаются абсолютно все точки, тогда как в точных лишь некоторые. На первых порах часто происходит путаница с понятиями свободы и точности.

Также замечу, что существуют топологические версии описанных выше понятий, например топологически транзитивное действие - это когда существует всюду плотная в X орбита. Теория топологических модификаций не переносится прямо-таки дословно с обычных действий: например, у топологически транзитивных действий не каждая орбита должна быть плотной, даже при условии непрерывности действия. Можно рассмотреть такой пример: зададим некоторое транзитивное действие группы на плотном множестве, а на дополнении к этому множеству пусть группа действует тривиально. Тогда у вас будет одна плотная орбита и много одноэлементных орбит. Часто такие действия не будут непрерывными, но построить непрерывный пример можно: рассмотрим действие группы $\mathbb{Z}$ на множестве $X = \mathbb{Z} \cup \{+\infty\}$ левыми сдвигами (доопределим действие на бесконечности по правилу $+\infty + n = +\infty$, иными словами сделаем бесконечность неподвижной относительно сдвигов, а топология на X строится так, что $+\infty$ является добавленной точкой одноточечной компактификации $\mathbb{N} \subset \mathbb{Z}$, иными словами база окрестностей $+\infty$ будет состоять из множеств $\{n, n+1, n+2, \ldots, +\infty\}$. Ясно, что в такой топологии $\lim\limits_{n\to\infty} = +\infty$, причем здесь $+\infty$ не абстракция, а вполне конкретная точка). В таком случае $\mathrm{Orb}(0) = \mathbb{Z} \subset X$ будет всюду плотным множеством, тогда как $\mathrm{Orb}(+\infty) = \{+\infty\}$. Также можно проверить, что в так заданной топологии на X это действие будет непрерывным, иными словами действие каждого элемента группы является гомеоморфизмом X. Обычно самая красота возникает в действиях не на голом множестве, а со структурой, так как в таком случае соединяются разные математические области, что зачастую приводит к фантастическим результатам. Вообще, большая часть идеологии математики заключается в том, чтобы по максимуму использовать структуры на исследуемых вами объектах, а если их пока нет - то находить (к примеру, помните, что у нас ничего не получалось сказать про группы, когда мы только дали определение и работали с таблицами умножения. Но если рассмотреть некоторую подгруппу - то появляется структуры смежных классов и действия группы на этом множестве - и это сразу переводит нашу дисциплину на новый уровень: появляется теорема Лагранжа и множество теорем из нее вытекающих).

Вернемся к насущным обыденным вопросам: из таблички нетрудно заметить, что обычно чем у элемента больше орбита - тем меньше оказывается стабилизатор. И

оказывается, что это не специфика частных примеров, а общая закономерность:

Орбитальная теорема
Пусть $|G| < \infty$. *Тогда верна следующая формула:*

$$\boxed{|\operatorname{Orb}(x)| = \frac{|G|}{|\operatorname{St}(x)|}}$$

Для доказательства можно явно построить биекцию:

$$gx \leftrightarrow g\operatorname{St}(x)$$

Идейно эта конструкция и сама орбитальная теорема очень похожа на теорему Лагранжа. Замечу, что на самом деле теорема верна в более общей формулировке совпадения мощностей $|\operatorname{Orb}(x)|$ и $[G : \operatorname{St}(x)]$ даже в случае бесконечных групп, но эту теорему мы будем применять только для конечных G, для которых выполнено $[G : \operatorname{St}(x)] = \frac{|G|}{|\operatorname{St}(x)|}$.

Пример
Вычислить централизатор $C((12)(34)) < S_4$, *т.е. элементы из* S_4, *коммутирующие с данной перестановкой, он же стабилизатор этого элемента для действия* $\operatorname{Ad} : S_4 \curvearrowright S_4$.

В принципе есть общий алгоритм вычисления централизатора безо всяких действий - мы просто расписываем коммутационное соотношение как $g(12)(34)g^{-1} = (12)(34)$, а дальше вспоминая формулу для сопряжения получаем: $(g(1)g(2))(g(3)g(4)) = (12)(34)$ - после чего остается сделать грамотный комбинаторный перебор всех вариантов. Обычно этот метод тем сложнее работает, чем больше в исследуемой перестановке независимых циклов одинаковой длины - потому что мало того, что g может перетасовывать элементы внутри независимых циклов - так еще может перетасовывать и сами циклы.

Замечание, что централизатор - это на самом деле стабилизатор действия сопряжения, существенно помогает в решении задач, так как орбитальная теорема моментально дает порядок централизатора. Таким образом мы будем знать сколько именно нам нужно найти элементов - а когда понятна цель, то и движение к цели идет быстрее: как правило требуемое количество коммутирующих элементов легко находится. Перейдем к деталям:

Из орбитальной теоремы мы получаем, что

$$|C((12)(34))| = \frac{|S_4|}{|\operatorname{Orb}((12)(34))|} = \frac{24}{3} = 8$$

так как орбита $(12)(34)$ - это все элементы с ним сопряженные, т.е. имеющие с ним один и тот же циклический тип, а их три штуки. Найдем 8 элементов коммутирующих с $(12)(34)$: 6 элементов находятся сразу: V_4 (так как она абелева, то там все друг с другом коммутируют), (12), (34). Также нужно отметить, что централизатор - это подгруппа, а значит вместе с любой парой элементов в централизаторе лежит их произведение, значит получаем, что $[(13)(24)](12) = (1423)$. Если есть он, то есть и обратный: $(1423)^{-1} = (3241)$. Так как на данном этапе набралось уже 8 элементов, то больше быть не может.

Замечание:

Отмечу, что раз описанное выше 8-элементное множество является централизатором, то автоматически оно является подгруппой: проверка чего без этого замечания была бы очень проблематичной. Замечу также, что раз мощности классов сопряженности в S_4 равны:

$$(**) \longleftrightarrow 6$$

$$(***) \longleftrightarrow 8$$

$$(**)(**) \longleftrightarrow 3$$

$$(****) \longleftrightarrow 6$$

то мы задаром получаем в S_4 подгруппы порядков $4, 3, 8, 4$ как централизаторы соответствующих элементов - конечно же в случае S_4 впечатлиться здесь можно только построенной в этой задачей подгруппой порядка 8, так как остальные порядки покрываются циклическими подгруппами. Но, повторюсь - воспринимайте это как общий полезный прием на поиск подгрупп: скажем, если у вас есть группа порядка 100, и в ней вы нашли класс сопряженности мощности 5 - то в вашей копилке сразу появляется подгруппа порядка 20.

Отмечу, что из орбитальной теоремы также получается, что мощность любого класса сопряженности делит порядок группы - так как класс сопряженности - это орбита действия сопряжениями. Факт, истинная суть которого проявляется только если на него через призму действий смотреть.

По аналогии с разбиением на смежные классы в теореме Лагранжа, наше множество

$$X = \coprod_{\text{орбиты}} \mathrm{Orb}(X)$$

разбивается в дизъюнктное объединение орбит: потому что любые две орбиты или не пересекаются, или совпадают. Это легко доказать, пусть $z \in Gx \cap Gy$. Тогда $z = gx$, а значит $Gz = Ggx = Gx$. Аналогично $Gz = Gy$. На уровне мощностей эта формула превращается в *формулу орбит:*

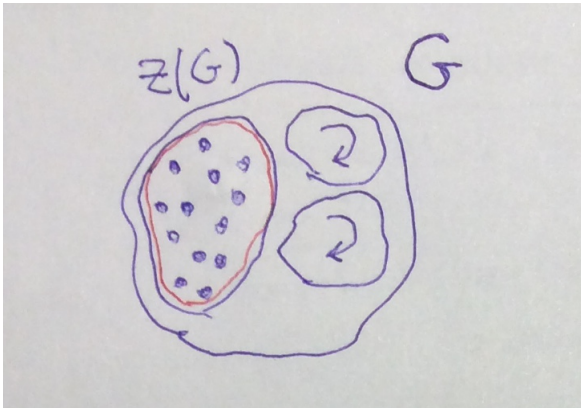
$$\boxed{|X| = \sum_{\text{орбиты}} |\,\mathrm{Orb}(x)| = \sum_{\text{орбиты}} \frac{|G|}{|\,\mathrm{St}(x)|}}$$

В суммировании каждой орбите соответствует свое слагаемое, более формально: мы выбираем в каждой орбите произвольного представителя x, и суммирование фактически происходит по этим представителям. Замечу, что слагаемые в самой правой сумме не зависят от выбора элемента x в каждой орбите (фактически, это следствие орбитальной теоремы). Также отмечу деталь, которая мне кажется совершенно фантастической в этой формуле: это связь мощности голого множества X с некоторыми чисто "групповыми" мощностями смежных классов.

В частном случае действия сопряжением $\mathrm{Ad} : G \curvearrowright G$ эта формула превращается в *адовую формулу орбит*:

$$\boxed{|G| = |Z(G)| + \sum_{|[g]|\neq 1} \frac{|G|}{|C_G(g)|}}$$

суммирование здесь проходит по классам сопряженности (это в точности орбиты сопряжения) - каждому классу сопряженности соответствует одно слагаемое, причем от выбора элемента из $[g]$ соответствующее слагаемое не зависит. Также обычно от суммы отщепляют слагаемые, соответствующие которым классы сопряженности состоят из одного элемента. Нетрудно понять, что все такие элементы образуют в точности центр $Z(G)$ группы G, и они соответствуют $|Z(G)|$ в формуле.



И за счет такой исключительной роли центра в этой формуле - обычно эту формулу используют как раз тогда, когда нужно что-то про центр группы сказать, типично, в вопросах делимости его порядка (например, если для конечной группы нужно проверить ее абелевость - можно просто доказать, что порядок центра совпадает с порядком всей группы).

Утверждение (теорема Кэли)
Доказать, что если $|G| = n$, то $G \hookrightarrow S_n$.

Классическая конструкция, которую обычно рассказывают на первом курсе, и которую мы повторим, описывая ее только на языке действий: рассмотрим действие левым умножением группы на себе $\lambda : G \curvearrowright G$, забвение групповой структуры на множестве фактически позволяет отождествить группу (на которой действуем) с n-элементным множеством: $G = \{1, 2, \ldots, n\}$, таким образом получаем гомоморфизм:

$$G \to S(\{1, 2, \ldots, n\}) = S_n$$

который очевидно, что инъективен (так как любой неединичный элемент левым умножением "смещает" все элементы группы. Таким образом можно сказать даже большее: что неединичные перестановки образа этого гомоморфизма не имеют неподвижных элементов, иными словами это действие свободное).

Замечание

Также хочется отметить важность и содержательность этой теоремы даже в случае бесконечных групп - потому что фактически для произвольной группы G мы получили вложение $G \hookrightarrow S(G)$. К примеру в частном случае счетной группы G мы получаем, что $G \hookrightarrow S(\mathbb{N})$, и это довольно полезный структурный результат, фактически позволяющий в некоторых ситуациях при работе со счетными группами ограничиваться биекциями фиксированного счетного множества, которые, как и в конечном случае, тоже допускают теорему о разложении на независимые циклы, имеют такую же простую формулу для сопряжения и т.д.

Задача

Пусть $|G| = p^n$ для простого p. Доказать, что $Z(G) \neq \{e\}$.

На языке действий принадлежность элемента центру группы может быть перефразирована как тривиальность его орбиты для действия сопряжением:

$$g \in Z(G) \iff \mathrm{Orb}(g) = \{g\}$$

так как если $hgh^{-1} = g$ для любого h, то $g \in Z(G)$ и наоборот. Это также эквивалентно $[g] = \{g\}$. Воспользуемся теперь адовой формулой орбит:

$$|G| = |Z(G)| + \sum_{|[g]|\neq 1} \frac{|G|}{|C_G(g)|}$$

Так как централизатор - это подгруппа, то по теореме Лагранжа $|C_G(g)| = p^k$ для некоторого k. Поэтому $\frac{|G|}{|C_G(g)|} = \frac{p^n}{p^k} = p^m$ и раз суммирование ведется по нетривиальным смежным классам, то $m \neq 0$ (в противном случае элемент лежит в центре группы). Таким образом адовая формула орбит на уровне мощностей превращается в:

$$p^n = |Z(G)| + p^{m_1} + p^{m_2} + \ldots + p^{m_r}$$

причем все степени отличны от нуля. Отсюда вытекает, что $|Z(G)|$ делится на p, в частности $|Z(G)| \neq 1$.

Задача

Пусть $|G| = p^2$ для простого p. Докажите, что G - абелева.

Посмотрим, какой порядок может быть у центра:

$$|Z(G)| = \begin{cases} p^2 \implies G - \text{ абелева.} \\ p \implies |G/Z(G)| = p \implies G/Z(G) \cong \mathbb{Z}_p \implies G - \text{ абелева (раньше доказывали)} \\ 1 \implies \text{противоречие с предыдущей задачей} \end{cases}$$

Поясню немного второй случай, который на самом деле не может быть реализован: пусть $|Z(G)| = p$, раньше мы доказывали, что если фактор по центру цикличен - то группа абелева, но в таком случае $|Z(G)| = p^2$, и мы приходим к противоречию. Таким образом остается лишь первый случай.

Замечание:

Сразу возникает закономерный вопрос, а не любая ли группа G с $|G| = p^n$ является абелевой (такие группы называются p-группами). Разумеется, ответ отрицательный - и достаточно вспомнить неабелеву группу кватернионов, для которой $|Q_8| = 8 = 2^3$. Однако несмотря на неабелевость, действия позволяют кое-что сказать про количество классов сопряженности в p-группах, и этому будет посвящена следующая задача:

Задача

Пусть $|G| = p^3$, p - простое и G - неабелева. Найти количество классов сопряженности.

В абелевом случае каждый элемент представляет собой класс сопряженности, т.е. всего их будет p^3, посмотрим насколько меньше их станет в неабелевом случае:

Из теоремы Лагранжа $|Z(G)|$ может быть равен $1, p, p^2, p^3$.

• Случай $|Z(G)| = 1$ невозможен, т.к. центра p-группы всегда нетривиален (советую запомнить этот факт, т.к. его очень часто используют).

• Случай $|Z(G)| = p^2$ также невозможен, т.к. тогда $|G/Z(G)| = p$, но в неабелевом случае фактор-группа по центру не может быть циклической.

• И случай $|Z(G)| = p^3$ тоже невозможен: т.к. по условия дана неабелева группа.

Таким образом $|Z(G)| = p$. Применим теперь адовую формулу орбит:

$$|G| = |Z(G)| + \sum_{|[g]|\neq 1} \frac{|G|}{|C(g)|}$$

т.е. формулу орбит, где группа действует на себе сопряжениями, здесь в обозначении централизатора $C(g)$ мы не писали индекса, так как понятно о какой группе идет речь. Рассмотрим произвольный нетривиальный класс сопряженности $[g]$, где $g \notin Z(G)$ (для $g \in Z(G)$ как раз $|[g]| = 1$), тогда по орбитальной теореме:

$$|[g]| = \frac{|G|}{|C(g)|}$$

И опять рассмотрим возможные порядки, но уже $C(G)$:

• Два случая $|C(g)| = 1, p$ невозможны, т.к. в централизаторе заведомо лежит сам g и все элементы из $Z(G)$, а это уже как минимум $p + 1$ элемент.

• Случай $|C(g)| = p^3$ тоже невозможен, т.к. в таком случае все элементы группы коммутируют с g, а это означало бы, что $g \in Z(G)$, тогда как мы рассматриваем нецентральный элемент. Таким образом $|C(g)| = p^2$, а значит $|[g]| = p$ по формуле орбит.

Резюмируем общую картину: в неабелевой группе $|G| = p^3$ существует p классов сопряженности, состоящих за 1 элемента (это в точности элементы центра), остальные классы сопряженности состоят из p элементов: ясно, что раз классы сопряженности не пересекаются, то чтобы ими исчерпать всю группу таких классов должно быть $p^2 - 1$. Таким образом, всего классов сопряженности $p^2 + p - 1$. К примеру, если Вы рассмотрите Q_8, то даже не разбираясь со структурой группы - из ее неабелевости следует, что у нее 5 классов сопряженности.

Задача

Задача, близкая к предыдущей: описать все конечные группы, у которых в точности 3 класса сопряженности.

Пусть $|G| = n$ и

$$G = \{e\} \cup [x] \cup [y]$$

Пусть $a = |[x]|$ и $b = |[y]|$ (без ограничения общности $b \leq a$). Из орбитальной теоремы получаем, что a и b делит n. Нетривиальные делители n есть в точности целочисленные элементы множества (элементы которого расположены в порядке убывания):

$$\left\{\frac{n}{2}, \frac{n}{3}, \frac{n}{4}, \dots\right\}$$

Замечу, что невозможна ситуация $a = b = \frac{n}{2}$, т.к. в таком случае не хватит места для $\{e\}$. Таким образом получаем: $a \leq \frac{n}{2}$ и $b \leq \frac{n}{3}$. Но при этом $1 + a + b = n$, учитывая полученные неравенства получаем:

$$n \leq 1 + \frac{n}{2} + \frac{n}{3}$$

Таким образом $n \leq 6$. Если $n = 1, 2, 4, 5$, то группа абелева и количество классов сопряженности совпадает с количеством элементов - значит эти случаи нам не подходят. При $n = 3$ мы имеем $G \cong \mathbb{Z}_3$, группа тоже абелева, но имеет в точности 3 класса сопряженности, а значит нам подходит. Осталось рассмотреть случай $n = 6$. Ясно, что в этом случае $b = 2, a = 3$.

Когда в изучении групп мы продвинемся чуть дальше - то сможем доказать, что групп порядка 6 кроме $\mathbb{Z}_6$ и S_3 в природе не бывает. Но сейчас воспользуемся кустарными методами, например, можно рассуждать так: рассмотрим класс сопряженности $[x]$ мощности 3. Тогда группа G действует сопряжениями на $[x]$ (ведь сопряжение элемента не выводит его за границы класса сопряженности), таким образом мы получаем гомоморфизм

$$\pi : G \to S([x]) = S_3$$

Так как действие сопряжением на классе сопряженности является транзитивным, то в $\operatorname{Im}\pi$ есть как минимум 3 элемента. Таким образом из теоремы Лагранжа получаем, что $|\operatorname{Im}\pi| = 3$ или $|\operatorname{Im}\pi| = 6$. Если $|\operatorname{Im}\pi| = 3$, из теоремы о гомоморфизме $|\ker\pi| = 2$, но при этом $\ker\pi \lhd G$, а значит она "набирается" из классов сопряженности G, мощности которых равны $1, 2, 3$. И набрать 2, при условии, что мы обязаны включить $\{e\}$ не получается. Приходим к противоречию. Значит $|\operatorname{Im}\pi| = 6$ и так как группы конечны, то получаем $G \cong S_3$ (сюръекция двух конечных множеств одинаковой мощности является биекцией). Советую попробовать и помучиться решить эту задачу с помощью анализа таблицы умножения и порядков элементов, или с помощью вычленения каких-нибудь соотношений на групповые элементы - чтобы понять, насколько упростилась жизнь, когда найдя действие на некотором множестве мы задаром получили гомоморфизм $G \to S_3$, а дальше делом техники было проверить, что это изоморфизм.

Замечание:

Условие конечности группы очень существенно, т.к. в бесконечном случае могут вылезать разные артефакты. К примеру, если решать аналогичную задачу

описания конечных групп с 2 классами сопряженности, то получим: $G = \{e\} \cup [x]$, *пусть* $|G| = n$. *Но так как по орбитальной теореме* $|[x]| = n - 1$ *делит порядок группы, то* $n = 2$. *Значит* $G = \mathbb{Z}_2$ - *что согласуется с интуицией, что группа с всего лишь двумя классами сопряженности должна быть простенькой.*

Однако в бесконечном случае существует множество примеров групп с двумя классами сопряженности, самый простой строится следующим образом: рассматриваем произвольную группу без кручений, например $G_0 = \mathbb{Z}$, *а затем строим ее расширение* G_1 *(термин "расширение" означает, что* $G_0 \triangleleft G_1$*), в котором все неединичные элементы* G_0 *являются сопряженными: сделать это довольно просто с помощью копредставлений: достаточно принудительно добавить новые образующие и соотношениями заставить их сопрягать нужные нам элементы, к примеру для группы* $G_0 = \mathbb{Z} = \langle x \rangle$ *мы получим:*

$$G_1 = \langle x, y_i | y_i^{-1} x y_i = x^i, i \neq 0 \rangle$$

Дальше строим аналогичным образом расширение G_2 *группы* G_1, *где все неединичные элементы группы* G_1 *будут сопряженными и т.д. Главное, чтобы порядки сопрягаемых элементов совпадали, но если в исходной группе не было кручения, то оно никогда не появится в таким образом построенных расширениях. Продолжая этот процесс много-много раз построим цепочку:*

$$G_0 < G_1 < G_2 < \dots$$

Ясно, что в

$$G = \bigcup_n G_n$$

любые два неединичные элемента будут сопряженными, т.к. если $x, y \in G$, *то* $x, y \in G_n$ *для некоторого* n, *и по построению они будут сопряжены не просто в* G, *а даже в* G_{n+1} *некоторыми порождающими* G_{n+1}.

Разумеется, такое построение дает бесконечно-порожденную группу (я бы сказал очень бесконечно-порожденную). Однако построение конечно-порожденной группы лишь с двумя классами сопряженности оказалось намного более сложной задачей, с которой справился Денис Осин 10 лет назад с помощью теории малых сокращений (Small cancellation theory) для гиперболических групп. Советую подумать над тем, существуют ли бесконечные группы с 3 классами сопряженности.

Утверждение (теорема Коши)
Пусть $|G|$ *делится на простое число* p. *Тогда существует* $x \in G$ *порядка* $\mathrm{ord}(x) = p$.

В решении нам понадобится классификация конечных абелевых групп, которую мы обсудим чуть позже. Решим задачу с помощью индукции, база индукции $|G| = p$ очевидна. Для доказательства шага предположим, что мы доказали утверждение для групп, у которых порядок строго меньше порядка G. Применим адовую формулу орбит:

$$|G| = |Z(G)| + \sum_{|[g]|\neq 1} \frac{|G|}{|C(g)|}$$

Рассмотрим два случая:

• Пусть $\frac{|G|}{|C(g)|}$ не делится на p для некоторого $g \notin Z(G)$. Тогда $|C(g)|$ наоборот делится на p по основной теореме арифметики, но так как $C(g) \neq G$ (иначе $g \in Z(G)$), то по предположению индукции найдется $x \in C(g) \subset G$ порядка $\mathrm{ord}(x) = p$.

• Пусть $\frac{|G|}{|C(g)|}$ делится на p для всех $g \notin Z(G)$, а раз $|G|$ делится на p по условию, то в таком случае $|Z(G)|$ тоже делится на p, но применять предположение индукции здесь нельзя, потому что никто не запрещает $G = Z(G)$, и мощность в данном случае не будет строго меньше. Но используя классификацию конечных абелевых групп мы получим, что

$$Z(G) = \mathbb{Z}_{p^n} \oplus H$$

для некоторой группы H, иными словами всегда отщепляется циклическое слагаемое порядка p^n для некоторого n. Ясно, что можно положить

$$x = (p^{n-1}, 0)$$

в аддитивной записи - этот элемент будет как раз иметь порядок p.

Замечание:

Неискушенный в алгебраических задачах глаз может с первого раза и не обнаружить место, где мы использовали простоту числа p, но использовали мы ее, когда применяли основную теорему арифметики. Ясно, что теорема Коши будет неверна, если не требовать простоты p, к примеру, возьмите S_4: хотя 8 является делителем порядка группы, в ней нет элементов с таким порядком. Однако несмотря на эти ограничения - это очень мощная теорема, которая позволяет задаром находить элементы фиксированных порядков, а значит и циклические подгруппы заданных порядков. К примеру, если у вас есть группа порядка 450 - то вы заведомо знаете, что в ней есть циклические подгруппы порядка 3 и 5 - разве это не здорово? Замечу, что раньше мы уже сталкивались с baby-версией теоремы Коши, когда доказывали, что группа четного порядка имеет элемент порядка 2 - даже в таком частном случае эта теорема кажется внушительной.

Пример

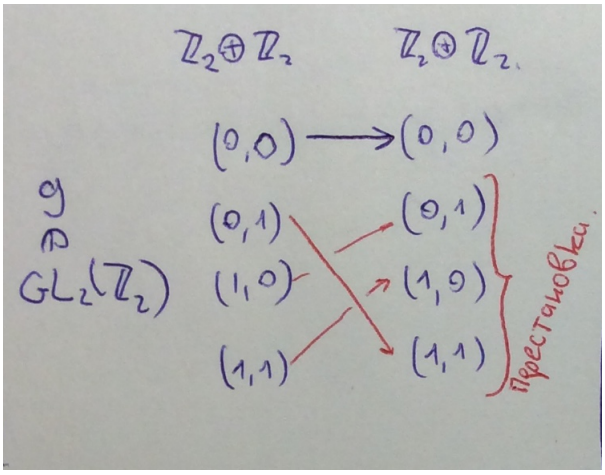
Докажите, что $GL_2(\mathbb{Z}_2) \cong S_3$.

Чтобы построить дом - сначала нужно построить фундамент. Чтобы построить изоморфизм - сначала нужно построить гомоморфизм. Гомоморфизм в S_n получается задаром, коль скоро мы нашли действие группы на n-элементном множестве. Попробуем найти действие $GL_2(\mathbb{Z}_2)$ на чем-то трех-элементном.

У обратимых матриц есть очевидное действие на соответствующем векторном пространстве:

$$\pi : GL_2(\mathbb{Z}_2) \curvearrowright \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Всего векторов в этом векторном пространстве 4, и так как матрицы обратимы - то соответствующие операторы являются биекциями, то есть перестановками векторов в пространстве. А так как 0 всегда переходит при линейном отображении в 0, то фактически мы имеем дело с перестановкой оставшихся трех ненулевых векторов:



Таким образом мы приходим к гомоморфизму:

$$\pi : GL_2(\mathbb{Z}_2) \to S_3$$

Ясно, что это отображение инъективное: ведь если $\pi(x) = \pi(y)$, то у матриц x, y совпадает действие на всех ненулевых векторах, а это в точности означает, что они являются совпадающими (так как два отображения совпадают в точности тогда, когда совпадают их действия на всех элементах).

Инъективность можно доказать разными способами: так как по теореме о гомоморфизме $GL_2(\mathbb{Z}_2) \cong \operatorname{Im}\pi$, и из теоремы Лагранжа $|\operatorname{Im}\pi|$ делит 6 - то достаточно предъявить 4 различные обратимые матрицы (если в подгруппе группы порядка 6 есть 4 элемента, то она совпадает со всей группой), и это делается очень легко. Либо можно вспомнить описание всех подгрупп S_3 и заметить, что все нетривиальные подгруппы абелевы, но при этом:

$$\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & ?\\ ? & ?\end{pmatrix} \neq \begin{pmatrix}0 & ?\\ ? & ?\end{pmatrix} = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$$

Значит образ неабелев, а единственная неабелева подгруппа S_3 это сама S_3 - значит

$$GL_2(\mathbb{Z}_2) \cong S_3$$

Отмечу, что здесь при подборе некоммутирующих матриц я не пользовался никакими сверхъестественными приемами - а просто взял две первые попавшиеся матрицы - и они оказались некоммутирующими (разумеется, я даже не пытался брать две совпадающие матрицы, или пару матриц, где одна из них единичная: просто случайные, но с долей здравого смысла. Бывают такие ситуации в математике, где для поиска контрпримера нужно копать и копать, но бывают и обратные ситуации, когда контрпримеры типичны, как например в этой ситуации). Также для экономии времени я не вычислял оставшиеся элементы произведения - так как если матрицы не совпадают в угловом элементе - то как они могут совпадать? Не забывайте про эту небольшую хитрость - подчас, нам не нужно знать про некоторое выражение абсолютно все, а достаточно небольшого фрагмента информации. Также уточню, что матричные коэффициенты лежат в $\mathbb{Z}_2$, а потому 2=0.

Замечание:

Отмечу, что то, что матричная группа оказалась изоморфна группе перестановок - это лишь исключение, и нисколько не закономерность: и хотя матрицы и перестановки в чем-то похожи, но все же это разные классы групп со структурно различными свойствами. Однако стоит заметить, что всегда существует вложение:

$$S_n \hookrightarrow G_n(F)$$

$$\sigma \mapsto T_\sigma$$

где соответствующая матрицы перестановки переставляет базисные векторы по правилу $T_\sigma(e_i) = e_{\sigma(i)}$. *У такой матрицы в каждой строке и в каждом столбце стоит лишь одна 1, а все остальные элементы равны 0, к примеру при таком гомоморфизме:*

$$(13)(245) \mapsto \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Разбиение перестановки σ *в произведение независимых циклов разбивает также базис на блоки (в этом примере* $[e_1, e_3][e_2, e_4, e_5]$*). В таком базисе матрица* T_σ *будет иметь блочный вид, и матрица в каждом блоке будет равна матрице стандартного сдвига (1 над диагональю, 1 в противоположном углу, а остальные* 0*):*

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ & & \ddots & \ddots & \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Напомню, что в m*-ом столбце матрицы линейного оператора стоят координаты разложения образа* e_m.

Пример

Построить вложение $S_4 \hookrightarrow A_6$.

Рассмотрим 4-элементное множество $X = \{1, 2, 3, 4\}$, а также множество его двухэлементных подмножеств $Y = \{\{a, b\} : a \neq b, a, b, \in X\}$, ясно, что $|Y| = 6$. Любая перестановка элементов X также некоторым образом переставляет элементы множества Y, таким образом мы получаем действие S_4 на 6-элементном множестве, или что то же самое - гомоморфизм:

$$\pi : S_4 \to S_6$$

Докажем, что π инъективно: действительно если $\pi(x) = \pi(y)$, то x, y совпадают на всех двухэлементных множествах, т.е. если рассмотреть три различных аргумента i, j, k - то

$$\{x(i), x(j)\} = \{y(i), y(j)\}$$

$$\{x(i), x(k)\} = \{y(i), y(k)\}$$

Таким образом пересечения для этих множеств тоже одинаковые, т.е. $x(i) = y(i)$. В силу произвольности i получаем $x = y$.

Покажем, что $\operatorname{Im}\pi < A_6$. Так как S_4 порождается транспозициями, то $\operatorname{Im}\pi$ порождается образом этих транспозиций, если организовать нумерацию $I = \{1,2\}, II = \{1,3\}, III = \{1,4\}, IV = \{2,3\}, V = \{2,4\}, VI = \{3,4\}$, то

$$\pi(12) = (II, IV)(III, V)$$

Ясно, что циклический тип образов других транспозиций будет тем же самым - потому что общий случай сводится к рассмотренному частному лишь перенумерацией аргументов. Таким образом, мы доказали, что $S_4 \hookrightarrow A_6$.

Замечания:

Полезно ориентироваться в похожих ситуациях, к примеру:

• *Существует ли вложение $S_4 \hookrightarrow A_5$? Такого вложения не существует и препятствием к нему служит теорема Лагранжа: 60 не делится на 24.*

• *Существует ли вложение $S_5 \hookrightarrow A_6$? Препятствием в данном случае служит порядки элементов: в S_5 существует элемент порядка 5, тогда как элемента с таким порядком не существует в A_6.*

• *На самом деле, верно куда более общее утверждение, чем заявленное в задаче: а именно, что существует вложение $\pi : S_n \hookrightarrow A_{n+2}$. Построить это вложение можно явно:*

$$\sigma \mapsto \sigma, \quad \sigma \in A_n$$

$$\sigma \mapsto \sigma(n+1, n+2), \quad \sigma \notin A_n$$

Нетрудно проверить, что это отображение будет гомоморфизмом: потому что этот гомоморфизм можно записать в других терминах (здесь τ - это гомоморфизм четности, и мы отождествляем $\mathbb{Z}_2 = S_2$):

$$\pi = \mathrm{id} \times \tau : S_n \to S_n \times S_2 < S_{n+2}$$

Ясно, что за счет второго прямого сомножителя $\operatorname{Im}\pi < A_{n+2}$. И хотя более общее утверждение доказывается намного проще - мне кажется, что рассмотрение вместе с действием $G \curvearrowright X$ индуцированного действия на двухэлементных подмножествах - очень глубокая и красивая идея, которую я не мог обойти стороной. Ясно, что для других задач вместо двухэлементных подмножеств могут подойти какие-то другие: трехэлементные, счетные и т.д.

• *Советую подумать, при каких n существует вложение $S_n \hookrightarrow A_{n+1}$.*

Задача

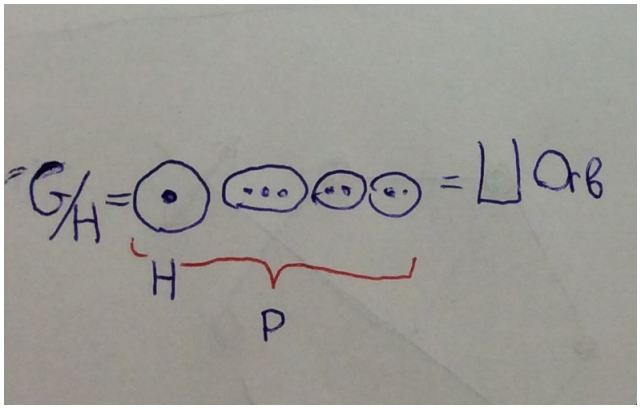
Пусть G - конечная группа, $H < G$ и $[G : H] = p$, где p - минимальный простой делитель $|G|$. Докажите, что $H \lhd G$.

Эта теорема является далеко идущим обобщением теоремы о нормальности подгруппы индекса 2. Классическое доказательство опирается на теорию действий:

Рассмотрим действие подгруппы H левыми умножениями на множестве левых смежных классов:

$$\lambda : H \curvearrowright G/H$$

Пространство G/H разбивается на орбиты, причем одной из орбит будет $\{H\}$.



Рассмотрим произвольную отличную от $\{H\}$ орбиту $\mathrm{Orb}(x)$. Тогда по орбитальной теореме получаем, что $|\mathrm{Orb}(x)|$ делит порядок группы, с другой стороны $|\mathrm{Orb}(x)| < p$, т.к. $|G/H| = p$, орбита $\{H\}$ - это один элемент в G/H, так что свободных элементов для остальных орбит остается только $p-1$. Но так как p - минимальный простой делитель, то $|\mathrm{Orb}(x)| = 1$, иными словами все орбиты одно-элементные для этого действия. Распишем этот факт алгебраически: для любого $h \in H$ и для любого $g \in G$ получаем:

$$hgH = gH$$

$$g^{-1}hgH = H$$

Отсюда вытекает, что $g^{-1}hg \in H$, что в точности означает $H \lhd G$.

Замечания:

Немного странным может показаться выбор действия, т.к. обычно более естественно рассматривать $\lambda : G \curvearrowright G/H$. Целью ограничения действия на подгруппу H было получение одно-элементной орбиты. Если бы мы рассматривали действие всей группы на множестве смежных классов - то действие получилось бы транзитивным и информативность для нашего похода была бы нулевой: так что иногда осмысленно ограничивать действия на важные для задачи подгруппы.

Также отмечу, что теорема становится неверной, если убрать условие минимальности для простого делителя p: к примеру $\langle(12)\rangle < S_3$ является подгруппой индекса 3, причем 3 - это простое число; но подгруппа нормальной не является.

Подчеркну, что теорема очень сильная и очень информативная: только подумайте! К примеру, если у вас есть группа порядка 45, то любая подгруппа порядка 15 автоматически будет нормальной! А нормальностью подгруппы обычно не разбрасываются.

Задача

Пусть $|G| = 4n+2$. Доказать, что найдется подгруппа $H < G$ индекса 2.

Если такая подгруппа найдется, то она автоматически будет нормальной. Мы помним, что все нормальные подгруппы получаются как ядра некоторых гомоморфизмов. Таким образом для решения задачи достаточно построить эпиморфизм (сюръективный гомоморфизм) $\pi : G \to \mathbb{Z}_2$ - тогда $\ker \pi$ будет необходимой подгруппой (скажу большее: не просто достаточно, а необходимо и

достаточно - если такой гомоморфизм нельзя построить, то и такой подгруппы не существует).

Гомоморфизм из произвольной группы в $\mathbb{Z}_2$ легко построить в качестве сквозного для гомоморфизма вложения в симметрическую группу из теоремы Кэли (обозначим это вложение как $g \mapsto \sigma_g$, напомню, что σ - это просто действие G на себе левыми сдвигами) и гомоморфизма четности:

$$G \to S(G) = S_{4n+2} \to \mathbb{Z}_2$$

Осталось доказать эпиморфность этого гомоморфизма. Вспомним, что в любой группе четного порядка есть элемент $g \in G$ порядка 2. Разберемся с циклическим типом перестановки $\sigma_g \in S(G)$ (так как $g^2 = e$, то и $\sigma_g^2 = e$ - и значит циклы будут только длины 2 и 1, но этого недостаточно для определения циклической структуры, так как нужно понять сколько именно циклов длины 2 в σ_g). Рассмотрим произвольный $a \in G$, тогда процесс умножения на g будет выглядеть следующим образом: $a \to ga \to a$, то есть циклов длины 1 не будет, так как они соответствуют неподвижным элементам левого умножения; таким образом циклическая структура получается следующей:

$$\sigma_g = (**)(**)(**)\dots$$

Всего будет $2n + 1$ циклов длины 2 (так как порядок изначальной группы $4n + 2$), значит σ_g - нечетная перестановка, и таким образом построенный гомоморфизм $G \to \mathbb{Z}_2$ будет сюръективным.

Замечание:

Условие в задаче на порядок $|G| = 2(2n + 1)$ существенно и не может быть отброшено: иными словами недостаточно просто четности порядка и нужно, чтобы при разложении на простые делители 2 входила в 1 степени. Если степень будет другая, то такой подгруппы может и не найтись: например, если рассмотреть A_4, то там единственной нетривиальной нормальной подгруппой является V_4, индекс которой равен 3. Также отмечу, что у этого утверждения есть обобщение, формулирующееся следующим образом:

Теорема

Пусть $|G| = 2^k(2m + 1)$ и существует элемент $g \in G$ порядка 2^k. Тогда в G есть нормальная подгруппа индекса 2^k.

Попробуйте доказать эту теорему.

Надеюсь, вам удалось прочувствовать красоту и глубину этой теории, а также подчерпнуть для себя мощные и полезные приемы: в этой теории все очень неалгоритмизировано, и изначально даже сложно сказать, может ли в той или иной теоретико-групповой задаче как-то помочь теория действий, но если ее применение все же находится - доказательство, как правило, получается очень эффектным и красивым, что его хочется поставить в рамочку. Повторюсь: если в какой-то задаче вы пришли в тупик - подумайте, нельзя ли прикрутить какое-нибудь действие: ведь посмотрите на все задачи из этого раздела - почти во всех в их изначальной формулировке действиями и не пахло.

Прямое произведение

Пусть A, B - произвольные группы, тогда декартово произведение

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

естественным образом наделяется групповой структурой по-элементных операций: $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$ и $(a, b)^{-1} = (a^{-1}, b^{-1})$, относительно которых оно превращается в группу, которую называют *прямым произведением* (иногда, а в абелевом случае почти всегда, используют обозначением как в линейной алгебре для прямой суммы $A \times B = A \oplus B$, чтобы подчеркнуть, что элементы из различных компонент произведения коммутируют между собой, да и в целом прямое произведение по свойствам очень похоже на прямую сумму линейных пространств). Обычно A отождествляется с $A \times \{e\} = \{(a, e) : a \in A\}$, аналогично и со вторым прямым сомножителем B. К очевидным свойствам отнесем следующие:

- $A, B \lhd A \times B$.
- $A \cap B = \{e\}$.

Оказывается, эти два свойства в некотором роде характеризуют прямые произведения, а именно верна следующая теорема:

Теорема

Пусть даны $A, B \lhd G$, такие, что $A \cap B = \{e\}$ и $A \cdot B = G$ (здесь имеется в виду теоретико-множественное умножение). Тогда:

$$G \cong A \times B$$

Обычно в таком случае говорят о *внутреннем прямом произведении*, так как несмотря на то, что группа внешне может не быть похожей на некоторое прямое произведение, но внутренняя структура группы все же допускает разложение в прямое произведение.

Замечу также, что из условий теоремы в частности вытекает, что подгруппы $A, B \lhd G$ обязаны коммутировать друг с другом: доказывается это непосредственными выкладками:

$$[a, b] = aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1}$$

Из красной формулы с учетом нормальности подгрупп получаем, что $[a, b] \in A$, из синей - что $[a, b] \in B$. Так как $A \cap B = \{e\}$, то и $[a, b] = e$.

К важным свойствам прямых произведений я бы отнес следующие:

- $[A \times B, A \times B] = [A, A] \times [B, B]$
- $Z(A \times B) = Z(A) \times Z(B)$
- $\mathbb{Z}_n \cong \mathbb{Z}_k \times \mathbb{Z}_m \iff \begin{cases} km = n \\ (k, m) = 1 \end{cases}$

Пример

Выяснить, какие из следующих групп допускают разложение в нетривиальное прямое произведение: $Q_8, S_4, A_4, \mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{C}^*, S_3, \mathbb{Z}_{35}$.

Сразу же отмечу, что для любой группы есть тривиальное разложение в прямое произведение: $G \cong G \times \{e\}$, хотя это разложение совершенно неинформативное. Поиск возможности разложения в нетривиальное прямое произведение я бы всегда начинал с вопроса, а какие вообще существуют нормальные подгруппы у заданной группы, можно ли найти две подгруппы, пересекающиеся по $\{e\}$, а если да - то много ли элементов найдется в их теоретико-множественном произведении. Если ответы на все вопросы окажутся положительными - то скорее всего нужно искать такое разложение.

Q_8 - мы все помним, что произвольная нетривиальная подгруппа группы кватернионов является циклической, порожденной $(-1), i, j$ или k. Замечу, что какую бы пару циклических подгрупп мы не взяли - он все пересекаются по $\{1, -1\}$ - таким образом группа кватернионов не разлагается в нетривиальное прямое произведение.

S_4 - посмотрим на мощности классов сопряженности, чтобы понять, какие могут быть порядки у нормальных подгрупп:

$$\#\{e\} = 1$$

$$\#\{(**)\} = \frac{4 \cdot 3}{2} = 6$$

$$\#\{(***)\} = \frac{4 \cdot 3 \cdot 2}{3} = 8$$

$$\#\{(****)\} = \frac{4!}{4} = 6$$

$$\#\{(**)(**)\} = 3$$

Так как 24 - четное число, то чтобы получить делитель порядка группы и с учетом того, что мы обязаны включить e в нормальную подгруппу - мы обязаны также включить и класс $\{(**)(**)\}$, так как он единственный из оставшихся имеет нечетный порядок. Таким образом, любые две нетривиальные нормальные подгруппы пересекаются как минимум по V_4 - приходим к противоречию даже без явного описания всех подгрупп, таким образом S_4 не разлагается в нетривиальное прямое произведение.

A_4 - эта еще проще: мы с вами раньше доказывали, что единственной нетривиальной нормальной подгруппой A_4 является V_4. Из этой одной выбрать две с тривиальным пересечением никак не получится, т.е. A_4 тоже не разлагается в нетривиальное прямое произведение.

$\mathbb{Z}$ - рассмотрим две нетривиальные нормальные подгруппы $A, B < \mathbb{Z}$, они автоматически будут нормальными в силу абелевости группы. Если использовать аддитивную запись и рассмотреть ненулевые элементы $n \in A, m \in B$, то ясно, что $nm \in A \cap B$, таким образом пересечение не может быть тривиальным, а значит $\mathbb{Z}$ не разлагается в нетривиальное прямое произведение. На всякий случай напомню, что произвольная подгруппа $\mathbb{Z}$ имеет вид $n\mathbb{Z}$, правда в доказательстве удалось избежать

необходимости полного описания подгрупп, так как в первом приближении нам интересно только тривиально ли пересечение.

$\mathbb{Q}$ - здесь уже все подгруппы описать сложнее, но сработает почти дословно такой же прием, как и с $\mathbb{Z}$: пусть $\frac{n}{m} \in A$ и $\frac{p}{q} \in B$, тогда $np \in A \cap B$, а значит $\mathbb{Q}$ также не разлагается в нетривиальное прямое произведение.

$\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$ причем изоморфизм задается очевидной формулой $z \mapsto (Re(z), Im(z))$.

$\mathbb{C}^* \cong \mathbb{T} \times \mathbb{R}^*$, причем изоморфизм задается в тригонометрической форме формулой $re^{i\varphi} \mapsto (e^{i\varphi}, r)$, где, напомню, $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. То, что это гомоморфизм и биекция непосредственно проверяется.

S_3 тоже не разлагается в нетривиальное прямое произведение, так как в S_3 только одна нетривиальная нормальная подгруппа A_3.

$\mathbb{Z}_{35} \cong \mathbb{Z}_5 \times \mathbb{Z}_7$ - этот изоморфизм на порождающем элементе задается формулой $a \mapsto (b, c)$, где a, b, c - порождающие соответственно $\mathbb{Z}_{35}, \mathbb{Z}_5$ и $\mathbb{Z}_7$. Ясно, что в силу взаимной простоты порядков элемент (b, c) имеет порядок в точности 35 - поэтому это отображение корректный инъективный гомоморфизм. Сюръективность вытекает из соображения мощности. Этот пример - частный случай упомянутого выше критерия разложимости $\mathbb{Z}_n$ в нетривиальное прямое произведение.

Центр, коммутант и абеленизация являются очень мощным инструментом в вопросах изоморфности групп, и при этом они в большинстве случаев довольно легко вычисляются: и если они не изоморфны, то и исходные группы тоже неизоморфны. К очень эффективно работающим инвариантам я бы также отнес: порядок (для конечных групп), количество элементов фиксированного порядка, количество и существование элементов, удовлетворяющих определенным соотношениям: от элементарных в духе $\#\{x : x^3 = e\}$ вплоть до очень неэлементарных олимпиадных

$$\#\{x : \text{существует } y \quad \text{что} \quad y^{-1}x^2y = x^3\}$$

Часто (особенно для абелевых групп) в качестве инварианта берут факт разрешимости некоторого уравнения (чаще всего линейного), к примеру, разрешимость уравнения $nx = y$ для любого y означает, что группа (в аддитивной записи) допускает деление на n (а в мультипликативной - допускает извлечение корня n-ой степени, хотя, повторюсь, инвариант этот чаще используют для абелевых групп, которые обычно в аддитивной форме записываются). Отмечу также, что здесь $nx = x + x + \ldots + x$, где x складывается с собой n раз (если $n \in \mathbb{Z}$), так что эта операция сводится к групповым. Потренируемся на следующих примерах проверять группы на изоморфность с помощью этих инвариантов:

Пример

Выяснить, изоморфны ли следующие группы:

$$S_n \cong A_n \times \mathbb{Z}_2$$

$$A_5 \times S_4 \cong A_4 \times S_5$$

$$\mathbb{Z}_{30} \times S_4 \cong \mathbb{Z}_5 \times S_5$$

$$Q_8 \times S_4 \cong D_{46} \times S_3$$

$$\mathbb{Z}_2 \times S_3 \times S_4 \times S_5 \cong D_{144} \times S_5$$

$$S_3 \times \mathbb{Q} \cong S_5 \times \mathbb{Q}$$

$$S_5 \times \mathbb{Q} \cong A_5 \times \mathbb{Q}$$

• $S_n \ncong A_n \times \mathbb{Z}_2$ Порядки в данном случае совпадают, но самым простым напрашивающимся различающим инвариантом в данном случае будет центр группы: ясно, что $Z(S_n) = \{e\}$, но $Z(A_n \times \mathbb{Z}_2) = \{e\} \times \mathbb{Z}_2 \cong \mathbb{Z}_2$ при $n \geq 4$. Прим $n = 3$ группы также будут неизоморфны, т.к. слева стоит неабелева, а справа абелева группа. В совсем вырожденном случае $n = 2$ группы будут изоморфны.

• $A_5 \times S_4 \ncong A_4 \times S_5$ Порядки в данном случае совпадают, центры - тоже. Вычислим коммутанты: $[A_5 \times S_4, A_5 \times S_4] = A_5 \times A_4$, тогда как $[S_5 \times A_4, S_5 \times A_4] = A_5 \times V_4$ - у коммутантов разные порядки, значит исходные группы были неизоморфными (напомню, что $[G \times H, G \times H] = [G, G] \times [H, H]$).

• $\mathbb{Z}_{30} \times S_4 \ncong \mathbb{Z}_5 \times S_5$ Здесь опять группы имеют одинаковые порядки, но у них неизоморфные центры: $Z(\mathbb{Z}_{30} \times S_4) \cong \mathbb{Z}_{30}$ но $Z(\mathbb{Z}_5 \times S_5) = \mathbb{Z}_5$.

• $Q_8 \times S_4 \ncong D_{16} \times S_3$ Порядки в данном случае совпадают, центры будут изоморфны. Коммутанты же у них будут различными: $[Q_8 \times S_4, Q_8 \times S_4] \cong \mathbb{Z}_2 \times A_4$, тогда как $[D_{16} \times S_3, D_{16} \times S_3] = \mathbb{Z}_8 \times A_3 \cong \mathbb{Z}_8 \times \mathbb{Z}_3 \cong \mathbb{Z}_{24}$ - и левый коммутант неабелев, тогда как правый абелев. В качестве различающего инварианта можно было использовать порядки элементов: к примеру, в правой группе есть элементы порядков 16 и 48, тогда как в левой группе таких элементов попросту нет.

• $\mathbb{Z}_2 \times S_3 \times S_4 \times S_5 \ncong D_{144} \times S_5$ Порядки и центр здесь опять-таки совпадают, но опять различаются коммутанты: $[\mathbb{Z}_2 \times S_3 \times S_4 \times S_5, \mathbb{Z}_2 \times S_3 \times S_4 \times S_5] \cong A_3 \times A_4 \times A_5$, но при этом $[D_{144} \times S_5, D_{144} \times S_5] \cong \mathbb{Z}_{72} \times A_5$, и коммутанты неизоморфны, потому что у них различные центры - у левого коммутанта центр тривиален, а у правого - нетривиален.

• $S_3 \times \mathbb{Q} \ncong S_5 \times \mathbb{Q}$ Здесь опять же различные коммутанты: $[G \times \mathbb{Q}, G \times \mathbb{Q}] \cong [G, G]$. Отмечу, что хотя в конечных группах количество элементов фиксированного порядка является более эффективным и сильным инвариантом, но для бесконечных групп все же эффективнее использовать центры и коммутанты, т.к. типично, что у групп нет элементов конечного порядка, а если они и есть - то обычно их бесконечное число и никакой информативности в множестве или количестве таких элементов нет. К тому же, как я раньше говорил - чем больше в математическом объекте структур - тем лучше, и если множество элементов фиксированного порядка - это лишь голое множество, то коммутант и центр наделены групповой структурой.

• $S_5 \times \mathbb{Q} \ncong A_5 \times \mathbb{Q}$ Здесь группы бесконечны, как и множества элементов фиксированного порядка. Коммутанты и центры тоже оказываются изоморфными, однако у этих групп разная абеленизация (т.е. фактор по коммутанту):

$$S_5 \times \mathbb{Q}/[S_5 \times \mathbb{Q}, S_5 \times \mathbb{Q}] \cong \mathbb{Z}_2 \times \mathbb{Q}$$

$$A_5 \times \mathbb{Q}/[A_5 \times \mathbb{Q}, A_5 \times \mathbb{Q}] \cong \mathbb{Q}$$

Эти абеленизации различны хотя бы потому, что в первой абеленизации есть элемент порядка 2, а во второй такой элемент отсутствует.

==========

Группа автоморфизмов

Автоморфизмом группы называется биективный гомоморфизм группы в себя. Ясно, что множество автоморфизмов само является группой (относительно композиции), при этом использование его в качестве инварианта не эффективно из-за сложности вычисления этой группы, но при этом группа автоморфизмов несет много ценной информации про исходную группу. Как минимум потому что это согласуется с одной из основных идеологий математики: "хочешь изучать объекты - изучай функции на нем". Именно поэтому на линале столько времени вы тратили на линейные функционалы, именно поэтому мы разбирали с вами гомоморфизмы, а сейчас переходим к идейному продолжению - автоморфизмам: то, как объект может отображаться на себе уже говорит очень о многом. Теперь немножко терминологии:

$$\mathrm{Aut}(G) = \{\varphi : G \to G : \varphi - \text{биективный гомоморфизм}\}$$

$$\mathrm{Inn}(G) = \{\mathrm{Ad}_g\}_{g\in G} \lhd \mathrm{Aut}(G)$$
$$\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$$

Групп $\mathrm{Inn}(G)$ называется *группой внутренних автоморфизмов*, ее нормальность в группе всех автоморфизмов легко непосредственно проверяется:

$$(\varphi\,\mathrm{Ad}_g\,\varphi^{-1})(h) = \varphi(g^{-1}\varphi^{-1}(h)g) = \varphi(g)^{-1}h\varphi(g)$$

Таким образом $\varphi\,\mathrm{Ad}_g\,\varphi^{-1} = \mathrm{Ad}_{\varphi(g)}$. Также, хочу отметить арифметико-терминологическую тонкость: что $\varphi(g)^{-1} = \varphi(g^{-1})$ и $\varphi^{-1}(g)$ - это две совершенно разные вещи: в одном случае мы применяем автоморфизм к обратному элементу, а в другом случае - применяем к элементу обратный автоморфизм. Наиболее ярко различия проявляются, если рассматривать не автоморфизмы, а просто биективные преобразования $\varphi : G \to H$: тогда эти элементы лежат даже в разных множества: первый в H, а второй в G.

Обманчиво может показаться, что $\mathrm{Inn}(G)$ должна быть изоморфна G - ведь сопряжений всего столько, сколько и элементов, на которые мы сопрягаем. Но не стоит забывать, что сопряжение на центральные элементы тождественно. На самом деле группа внутренних автоморфизмов произвольной группы имеет довольно явное описание:

Задача
Докажите, что $\mathrm{Inn}(G) \cong G/Z(G)$.

Легко доказывается с помощью леммы о гомоморфизме: рассмотрим гомоморфизм

$$\pi : G \to \mathrm{Inn}(G)$$
$$\pi(g) = \mathrm{Ad}_g$$

Ясно, что это эпиморфизм и что $\ker\pi = Z(G)$. Таким образом $\mathrm{Inn}(G) \cong G/Z(G)$.

В некоторых особенно хороших случаях $\mathrm{Aut}(G) = \mathrm{Inn}(G)$ все автоморфизмы совпадают с внутренними; причем отмечу, что случаи эти не исключительные и встречаются довольно часто, а потому этот изоморфизм позволяет описать всю группу автоморфизмов, или по крайней мере большую его часть, если вдруг есть

не являющиеся внутренними автоморфизмы. Группа $\mathrm{Out}(G)$ называется *группой внешних автоморфизмов* и что самое парадоксальное в этой терминологии - его элементы не являются автоморфизмами (это лишь смежные классы по подгруппе внутренних автоморфизмов). Ясно, что чем группа внешних автоморфизмов больше - тем больше у группы автоморфизмов, не являющихся внутренними.

По виду группы очень сложно понять, насколько велика окажется группа автоморфизмов: ясно, что $|\mathrm{Aut}(G)| \leq |G|^{|G|}$ (напомню, что $2^{|X|} = |X|^{|X|}$ для бесконечных множеств X), так как ясно, что автоморфизмов меньше чем всех отображений из множества в себя. Но часто бывают ситуации, когда у огромной группы очень мало автоморфизмов (например $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$ - у бесконечной группы будет конечная группа автоморфизмов). Чтобы подступиться к описанию группы автоморфизмов я вам советую ваши рассуждения всегда начинать с вопроса *куда при произвольном автоморфизме переходят порождающие элементы группы* - потому что порождающих как правило очень мало, тогда как автоморфизм полностью определяется значениями на порождающих. Также можно посмотреть, что происходит со структурным каркасом группы, например, с коммутантом или центром, или же с множеством элементов порядка 2, или же с множеством элементов какого-то другого фиксированного вида - т.е. с таким множеством, которое, переходит в себя под действием произвольного автоморфизма - очень часто это сильно помогает в описании группы автоморфизмов (например, если нужно описать группу автоморфизмов, скажем, A_4 - вы заведомо знаете, что любой автоморфизм переводит V_4 в себя, так как это коммутант, а также, что при автоморфизме сохраняется порядок перестановки, а значит сохраняется и ее циклический тип: потому что каждому порядку элементов в A_4 соответствует единственный циклический тип; в A_n при больших n это уже неверно). Часто при вычислении группы автоморфизмов помогает следующее наблюдение: если $H \lhd G$, то существует естественный гомоморфизм $\alpha : G \to \mathrm{Aut}(H)$, такой что $g \mapsto \mathrm{Ad}_g$; иными словами кроме внутренних автоморфизмов группы H всегда есть внутренние автоморфизмы некоторой большей группы G, содержащей H как нормальную, и при этом часто не являющиеся на H внутренними. К примеру мы знаем, что $V_4 \lhd A_4$, а значит задаром получаем гомоморфизм $A_4 \to \mathrm{Aut}(V_4)$. Ясно, что чем больше группа G - тем больше автоморфизмов мы можем получить, хоте тем меньшее шансов гомоморфизму α быть инъективным, хотя это не проблема, так как всегда можно рассматривать не саму группу G, а ее образ $\alpha(G) < \mathrm{Aut}(H)$. Также замечу, что всегда существует такая G, что α - сюръективно, потому что в качестве такой G можно взять $G = H \rtimes \mathrm{Aut}(H)$.

В общем, картина во многом напоминает задачу описания гомоморфизмов за той лишь разницей, что нужно следить не только за тем, чтобы соотношения в прообразе выполнялись в образе, но и за тем, чтобы получаемые гомоморфизмы являлись биекциями.

Пример
Доказать, что $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

Если работать с $\mathbb{Z}$ в аддитивной записи, то произвольный автоморфизм $\pi \in \mathrm{Aut}(\mathbb{Z})$ переводит порождающий 1 в порождающий, но $\mathbb{Z}$ порождают всего два элемента - это 1 и -1. Ясно, что оба эти выбора соответствуют автоморфизмам (id и $-\mathrm{id}$ соответственно). Таким образом $|\mathrm{Aut}(\mathbb{Z})| = 2$, а группа простого порядка обязана быть циклической.

Пример
Доказать, что $\mathrm{Aut}(\mathbb{Q}) \cong \mathbb{Q}^*$.

Опять будем работать с аддитивной записью и для произвольного автоморфизма $\pi \in \mathrm{Aut}(\mathbb{Q})$ рассмотрим $\pi(1) = q \in \mathbb{Q}^*$. По этим входным данным автоморфизм восстанавливается *единственным* образом (даже несмотря на то, что 1 не является порождающим в группе), для доказательства заметим, что для любого m выполнено:

$$q = \pi(1) = \pi\left(\frac{1}{m} + \ldots + \frac{1}{m}\right) = \pi\left(\frac{1}{m}\right) + \ldots + \pi\left(\frac{1}{m}\right) = m\pi\left(\frac{1}{m}\right)$$

И так как в $\mathbb{Q}$ уравнение $ax = b$ имеет единственное решение, то $\pi\left(\frac{1}{m}\right) = \frac{q}{m}$. Окончательно имеем:

$$\pi\left(\frac{n}{m}\right) = \pi\left(\frac{1}{m} + \ldots + \frac{1}{m}\right) = \frac{q}{m} + \ldots + \frac{q}{m} = q \cdot \frac{n}{m}$$

Назовем построенное отображение π_q. Ясно, что это гомоморфизм и что он является биективным с обратным $\pi_q^{-1}(p) = q^{-1}p$. Также понятно, что композиции таких автоморфизмов соответствует произведению образов 1, а именно $\pi_{q_1} \circ \pi_{q_2}(p) = \pi_{q_1}(q_2 p) = q_1 q_2 p = \pi_{q_1 q_2}(p)$. Таким образом отображение $\mathbb{Q}^* \to \mathrm{Aut}(\mathbb{Q})$ заданное $q \mapsto \pi_q$ является изоморфизмом.

Практически полностью можно описать группу автоморфизмов в случае произвольной циклической группы, правда групповая структура не так, чтобы совсем легко восстанавливалась:

Пример
Доказать, что $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^* = \{k : (k, n) = 1\}$, *где групповая операция - умножение соответствующих обратимых элементов.*

Напомню, что $\mathbb{Z}_n^*$ - это группа обратимых по умножению элементов $\mathbb{Z}_n$. Действуем аналогично предыдущим примерам: пусть $\pi(1) = k$ для некоторого автоморфизма π. Тогда $\pi(m) = \pi(1 + \ldots + 1) = k + \ldots + k = km$, иными словами соответствующий автоморфизм - это просто умножение на k. Далее, к биективности можно подступиться либо говоря, что раз композиции соответствует произведение, то для биективности нужна обратимость соответствующего k. Либо можно сказать, что порождающий должен переходить при автоморфизме в порождающий, а k в аддитивной записи порождает $\mathbb{Z}_n$ в точности тогда, когда $(k, n) = 1$. И если порождающий перейдет в порождающий - то построенный гомоморфизм будет сюръекцией, а из соображений мощности и биекций тоже (сюръективное

отображение n-элементного множества на себя является биекцией, однако в случае бесконечных групп это уже верно не всегда - и только в хопфовых группах, которые мы обсудим в самом конце, любой сюръективный гомоморфизм на себя является биекцией).

Подытожу: любой автоморфизм задается умножением на некоторое $k \in \mathbb{Z}_n^*$, при этом верно и обратное - умножение на любое такое число задает автоморфизм (и обратным к нему будет умножение на k^{-1}). Ясно, что как и в предыдущих примерах композиции автоморфизмов соответствует умножение чисел из $\mathbb{Z}_n^*$.

Из теории числе вы знаете, что $|\mathbb{Z}_n^*| = \varphi(n)$, где $\varphi(n)$ - функция Эйлера, равная количеству натуральных чисел, меньших n и взаимно простых с ним. Для $\varphi(n)$ есть довольно явная формула: если $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$, где p_i - простые числа, то:

$$\varphi(n) = p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1)\dots p_m^{k_m-1}(p_m-1) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

Важно знать, что $\varphi(nm) = \varphi(n)\varphi(m)$, если $(n,m) = 1$; этот факт легко доказывается с помощью упомянутой выше формулы для $\varphi(n)$. Давайте посмотрим, что получится в некоторых конкретных частных случаях:

• $\mathrm{Aut}(\mathbb{Z}_6) = \mathbb{Z}_6^* = \{1,5\} \cong \mathbb{Z}_2$ так как существует всего одна группа порядка 2.

• $\mathrm{Aut}(\mathbb{Z}_8) = \mathbb{Z}_8^* = \{1,3,5,7\}$. Группа порядка p^2 всегда абелева, хотя здесь это и так ясно, потому что групповая операция - обычное умножение чисел. Изучая абеленизацию Q_8 кустарными методами анализа таблицы умножения мы доказали, что существуют только две абелевы группы порядка 4: это $\mathbb{Z}_4$ и $\mathbb{Z}_2 \times \mathbb{Z}_2$, хотя чуть позже мы обсудим теорему о классификации конечных абелевых групп, дающую простое и полное описание всех конечных абелевых групп. И для того, чтобы понять, какой именно из этих двух групп изоморфна $\mathbb{Z}_8^*$ - начнем перемножать элементы, чтобы получше понять таблицу умножения этой группы (а чтобы этот процесс был более структурированным - предлагаю посмотреть на циклические подгруппы, порожденные каждым из элементов): $3^2 = 3 \cdot 3 = 1$, $5^2 = 5 \cdot 5 = 1$ - и здесь уже можно остановиться, так как в $\mathbb{Z}_4$ есть только 1 элемент порядка 2. Таким образом $\mathrm{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

• $\mathrm{Aut}(\mathbb{Z}_9) = \mathbb{Z}_9^* = \{1,2,4,5,7,8\}$. Начнем смотреть на циклические подгруппы: $2^2 = 2 \cdot 2 = 4$, $2^3 = 2 \cdot 4 = 8$ - и на этом можно закончить вычисления, так как получается, что у 2 порядок строго больше 3, и значит по теореме Лагранжа он должен быть равен 6 (порядку группы автоморфизмов). Таким образом, циклическая подгруппа $\langle 2 \rangle$ совпадает со всей группой, а значит $\mathrm{Aut}(\mathbb{Z}_9) \cong \mathbb{Z}_6$.

В общем случае цикличность $\mathbb{Z}_n^*$ эквивалентна в теоретико-числовой терминологии существованию первообразного корня; и есть теорема, что первообразный корень в $\mathbb{Z}_n^*$ существует тогда и только тогда, когда или $n = 2$, или $n = 4$, или $n = p^k$, или $n = 2p^k$, где p - нечетное простое число. В частности получаем, что $\mathrm{Aut}(\mathbb{Z}_{242}) \cong \mathbb{Z}_{110}$ так как $242 = 2 \cdot 11^2$ - значит группа автоморфизмов по этой теореме циклична, и $\varphi(2 \cdot 11^2) = \varphi(11^2) = 11^2 - 11 = 110$. Замечу, что два из трех рассмотренных примеров как раз подпадали под действие этой общей теоремы. Советую поразмышлять над тем, каким абелевым группам может быть изоморфна $\mathrm{Aut}(\mathbb{Z}_n)$ кроме циклических и $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Подгруппа $H < G$ называется *характеристической подгруппой* (иногда в таком случае пишут H *char* G) если $\pi(H) \subset H$ для любого $\pi \in Aut(G)$ (нетрудно понять, что это эквивалентно $\pi(H) = H$ - так как применяя определение характеристичности для π и π^{-1} мы получим $\pi(H) \subset H$ и $\pi^{-1}(H) \subset H$, второе вложение влечет в свою очередь $H \subset \pi(H)$, откуда и получаем равенство), т.е. она неподвижна под действием любого автоморфизма. В частности, ее неподвижность относительно всех внутренних автоморфизмов влечет ее автоматическую нормальность; и во многом теория характеристических подгрупп похожа на теорию нормальных подгрупп, но, к сожалению, характеристических подгрупп бывает намного меньше чем нормальных, и очень часто в группе нет никаких характеристических подгрупп кроме тривиальной $\{e\}$ и всей группы G.

Есть два типичных примера характеристических подгрупп: первый - это подгруппа, задаваемая некоторыми условиями или соотношениями, сохраняющимися под действием любого автоморфизма, например: $Z(G)$, $[G, G]$, $[[G, G], G]$ и т.д., хотя и часто эти подгруппы оказываются тривиальными. Второй яркий пример характеристических подгрупп - это подгруппа, такая, что она единственная из подгрупп имеет заданный порядок: так как автоморфизм сохраняет мощности будучи биекцией - а значит под действием любого автоморфизма эта подгруппа перейдет в себя. К примеру в Q_8 есть только одна подгруппа порядка два - это $\{1, -1\}$. Таким образом она будет переходить в себя под действием любого автоморфизма, или что то же самое - она будет характеристической (кстати, это еще один забавный способ доказательства нормальности этой подгруппы).

Пример

Описать $\mathrm{Aut}(\mathbb{Z}^2)$.

Уверен, что у многих от одной только формулировки сердце наполнилось счастьем и радостью от ностальгических воспоминаний о линале. Рассмотрим произвольный $\pi \in \mathrm{Aut}(\mathbb{Z}^2)$ и пусть $\pi \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$ и $\pi \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix}$. Тогда:

$$\pi \begin{pmatrix} n \\ m \end{pmatrix} = n \begin{pmatrix} a \\ b \end{pmatrix} + m \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} n \\ m \end{pmatrix}$$

Таким образом каждому гомоморфизму соответствует матрица $A_\pi = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, и эту матрицу нужно воспринимать как целочисленный аналог матрицы линейного отображения из линала, причем существует и обращение этой конструкции: а именно по целочисленной 2×2 матрице A можно построить гомоморфизм $\pi : \mathbb{Z}^2 \to \mathbb{Z}^2$, заданный формулой $\pi(v) = Av$, где $v = \begin{pmatrix} x \\ y \end{pmatrix}$. Как и в линале эти два соответствия взаимно обратные, а потому задают биекцию $\pi \leftrightarrow A_\pi$ между множеством гомоморфизмов $\mathbb{Z}^2$ в себя и множеством целочисленных матриц, также ясно, что произведению матриц соответствует композиция гомоморфизмов, а потому получаем, что π является автоморфизмом тогда и только тогда, когда матрица A_π является целочисленно обратимой, т.е. матрицей, у которой есть обратная и все матричные коэффициенты обратной матрицы целочисленные. Причем с учетом того, что произведению и обратной матрице соответствует композиция и обратный

автоморфизм, мы получаем, что $\mathrm{Aut}(\mathbb{Z}^2)$ изоморфна группе целочисленно обратимых матриц, что на самом деле является почти тавтологическим утверждением.

Нетрудно понять, что матрицы A целочисленно обратима iff $\det(A) = \pm 1$.

$\Rightarrow$ Если B - целочисленная обратная, то $\det(A)\det(B) = 1$, откуда $\det(A) = \pm 1$, так как у целочисленных матриц целочисленный определитель и произведение двух целых чисел может быть равно 1 только если оба из них равны ± 1.

$\Leftarrow$ Вытекает из формул для обратной матрицы через миноры:

$$A^{-1} = \frac{1}{\det(A)} \cdot \text{ минорная матрица}$$

Поэтому если $\det(A) = \pm 1$, то обратная матрица обязательно будет целочисленной.

Таким образом мы получаем изоморфизм

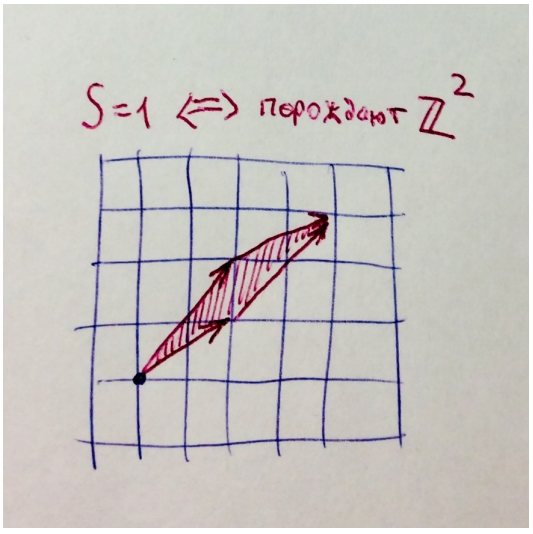
$$\mathrm{Aut}(\mathbb{Z}^2) \to \{g \in GL_2(\mathbb{Z}) : \det(g) = \pm 1\}$$

$$\pi \mapsto A_\pi$$

Отмечу, что в доказательстве мы нигде не использовали принципиально, что размерность нашего целочисленного линейного пространства равна 2, а потому заменяя в доказательстве 2 на n мы получаем:

$$\mathrm{Aut}(\mathbb{Z}^n) = \{g \in GL_n(\mathbb{Z}) : \det(g) = \pm 1\}$$

Из рассуждений про целочисленную обратимость матрицы следует такой занятный геометрический факт: векторы $a_1, \ldots, a_n$ будем называть "базисом" в $\mathbb{Z}^n$ если любой вектор выражается как целочисленная линейная комбинация "базисных" векторов, и что никакой вектор из "базисного" набора выкинуть нельзя. Так вот, векторы являются "базисом" iff матрица, i-ый столбец которой равен a_i, имеет определитель ± 1. В случае с плоскостью получаем такую картинку - что линейными комбинациями двух векторов на клетчатой бумаге вы сможете замостить весь лист iff площадь натянутого на эти векторы параллелограмма равна 1 (потому что определитель - это площадь параллелограмма).



Группу $\{g \in GL_n(\mathbb{Z}) : \det(g) = \pm 1\}$ иногда обозначают просто как $GL_n(\mathbb{Z})$ - все зависит от того как вы воспринимаете обратимость: если понимать как обычную

$\mathbb{R}$-обратимость - то лучше уточнить, что нам нужно $\det(g) = \pm 1$, чтобы обратная матрица была целочисленной; если в обратимость уже вкладывать то, что обратная матрица имеет целочисленные коэффициенты - тогда условие на определитель излишне. Это терминологический комментарий и все зависит от того, является ли для вас и ваших читателей/слушателей матрица $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ обратимой.

Последняя задача, все же, решалась скорее методами линала, но следующие примеры будут насыщены теоретико-групповыми методами работы с группами автоморфизмов намного больше:

Пример
Вычислить $\mathrm{Aut}(S_4)$.

Докажем в данном случае, что любой автоморфизм будет внутренним (это большая удача, и в таком случае процесс вычисления группы автоморфизмов практически тривиализуется).

С порождающими тут будет рассуждать сложно, потому что произвольный набор порождающих может быть очень специфичен и неоднороден, а потому предлагаю посмотреть на порядки: ясно, что элементы циклического типа (**) имеют порядок 2, а потому при автоморфизме переходят в элементы порядка 2, но a-priori мы ничего не можем сказать про циклический тип образа, так как в группе S_4, в отличие от S_3, порядок элемента не всегда восстанавливает циклической структуры, и порядок 2 имеют элементы вида (**) и (**)(**). Однако не стоит унывать и можно заметить, что при автоморфизме сопряженные элементы переходят в сопряженные. А потому, скажем, если (12) при автоморфизме перешел в (**)(**), то и все транспозиции должны перейти в элементы циклического типа (**)(**). Но это невозможно из соображений мощности, т.к. автоморфизм - это биекция, и при этом элементов циклического типа (**) $\frac{4\cdot 3}{2} = 6$ штук, тогда как элементов типа (**)(**) всего три штуки, таким образом косвенно, но мы все равно доказали, что транспозиции S_4 переходят в транспозиции при автоморфизме.

Пусть $\pi \in \mathrm{Aut}(S_4)$ - произвольный автоморфизм, и пусть $\pi(12) = (ab)$. Тогда $\pi(13) = (cd)$, причем $\{c, d\}$ как множество не может совпадать с $\{a, b\}$ - потому что это противоречило бы биективности π, и не может не пересекаться с $\{a, b\}$, т.к. если бы $\{a, b, \} \cap \{c, d\} = \emptyset$, то $[\pi(12), \pi(13)] = e$, тогда как $[(12), (13)] \neq e$, что опять противоречит биективности π. Таким образом у этих двух-элементных множеств есть один общий элемент, без ограничения общности можем считать, что $\pi(13) = (ad)$. Далее, аналогичные рассуждения показывают, что $\pi(14) = (af)$ (так как у транспозиции $\pi(14)$ должен быть лишь один общий элемент как с (ab), так и с (ad) - ясно, что этим общим элементом может быть только a). Таким образом для любого i мы получаем $\pi(1i) = (a*)$, то есть если в транспозиции есть 1 - то в ее образе обязательно будет a. Аналогичные рассуждения можно провести и для остальных элементов 2,3 и 4. Иными словами, раз изначально определенное на двухэлементных множествах отображение уважает пересечение - то его можно согласованно доопределить и на одноэлементных множествах, и фактически по автоморфизму мы строим некоторую биекцию $\{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$, отображая $1 \mapsto a$, $2 \mapsto b$ и т.д. А дальше можно пойти двумя дорогами:

• Для тех, кто любит короткие дороги: можно сказать, что на основании этого автоморфизм полностью определяется параметрами $\{a, b, d, f\}$, потому что, как мы

помним, $S_n = \langle (1i) \rangle$. Таким образом задав его на порождающих как $\pi(1i) = (a*)$ мы полностью восстановим автоморфизм. Таким образом $|\operatorname{Aut}(S_4)| \leq 4! = 24$ - то есть не превосходит количества возможных параметров - а это четверки различных чисел от 1 до 4. Но при этом мы знаем, что $\operatorname{Inn}(S_4) \cong S_4/Z(S_4) \cong S_4$ - то есть внутренних автоморфизмов уже 24. Таким образом из соображений мощности места для не внутренних автоморфизмов никак не хватит, а значит

$$\operatorname{Aut}(S_4) \cong S_4$$

• Для тех, кто любит долгую дорогу и понимание происходящего: эту конструкцию можно довести до победного конца и понять, что раз $\{a, b, d, f\}$ - различные числа, то можно рассмотреть перестановку

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & d & f \end{pmatrix}$$

и заметить, что по построению чисел $\{a, b, d, f\}$ мы получаем:

$$\pi(1i) = (\tau(1)\tau(i)) = \tau(1i)\tau^{-1}$$

Но раз транспозиции вида $(1i)$ порождают S_n, а на них автоморфизм действует как сопряжение, то и для любой перестановки из мультипликативности сопряжения будет вытекать:

$$\pi(\sigma) = \tau\sigma\tau^{-1}$$

То есть пойдя и по этой дороге мы тоже пришли к внутренности любого автоморфизма и изоморфизму $\operatorname{Aut}(S_4) \cong S_4$, причем на данной дороге мы даже поняли как строить соответствующую сопрягающую перестановку.

Очень важное замечание:

Сразу отмечу довольно интересную групповую аномалию: что $\operatorname{Aut}(S_n) \cong S_n$ *для всех n кроме 2 и... 6. Вы скажете, что 2 - это нормально, это типичный вырожденный случай для группы перестановок, когда группа перестановок оказывается как минимум абелевой. Но 6? Как это, как это? На самом деле 6 очень часто в математике играет роль как число колоссальных симметрий: те же пчелы строят свои соты в форме правильных шестиугольников. И та же решетка из правильных шестиугольников имеет симметрий намного больше, чем правильная квадратная. И неслучайно в последнее время особую популярность стала приобретать дискетизация физических уравнений не на квадратной, а шестиугольной решетке.*

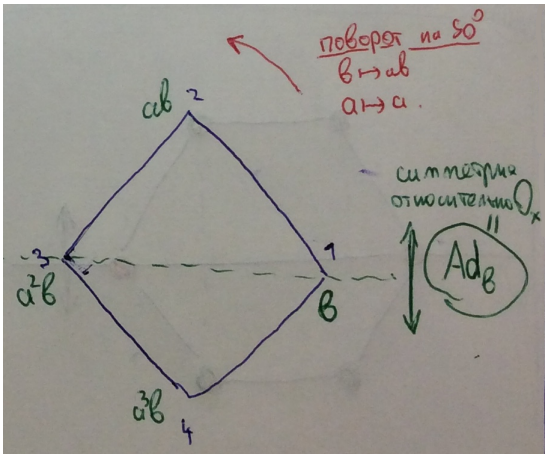
Для $n = 6$ *доказательство сломается там, где мы доказывали, что транспозиции переходят в транспозиции при автоморфизме из соображений мощности - и вот в случае* $n = 6$ *эти соображения уже не работают, так как перестановок* $(**)$ *будет* $\frac{6 \cdot 5}{2} = 15$*, тогда как перестановок* $(**)(**)(**)$ *будет тоже* $\frac{1}{3} \cdot \frac{6 \cdot 5}{2} \cdot \frac{4 \cdot 3}{2} \cdot \frac{2 \cdot 1}{2} = 15$*, и есть как минимум один внешний автоморфизм, переводящий* $(**)$ *в* $(**)(**)(**)$*. Самая теоретически прозрачная конструкция этого автоморфизма требует теорем Силова, а потому мы ее позже рассмотрим. Самое главное: важно понимать, что циклическая структура не восстанавливается из чисто групповых характеристик, а потому не обязана сохраняться при автоморфизме. Подумайте над тем, чему на самом деле равна* $\operatorname{Aut}(S_6)$*.*

Пример
Вычислите $\mathrm{Aut}(D_4)$.

В данном случае группа автоморфизмов уже не будет совпадать с группой внутренних автоморфизмов. Прежде всего заметим, что есть лишь одна подгруппа порядка 4 - это подгруппа $\langle a \rangle$ поворотов - ясно, что при автоморфизме она обязана перейти в подгруппу порядка 4, но так как такая подгруппа единственна - то она перейдет в себя (напомним, что в таком случае обычно используют термин "характеристическая подгруппа"). Таким образом для произвольного $\pi \in \mathrm{Aut}(D_4)$ мы имеем $\pi(a) = a^k$, где $k = 1, 3$, так как порождающий группы поворотов должен перейти в порождающий. Ясно, что осевые симметрии переходят в осевые симметрии, а значит $\pi(b) = a^m b$, где на m a-priori нет никаких ограничений (отмечу, что осевые симметрии переходят в осевые симметрии потому, что они являются дополнением до переходящего в себя множества поворотов. Это не вытекает из факта, что элементы порядка 2 переходят в элементы порядка 2, так как поворот на 180 градусов тоже имеет порядок 2 - здесь нужен более тонкий анализ, как в предыдущем примере с циклическим типом). Таким образом, для произвольного автоморфизма у нас имеется не более чем 8 вариантов, таким образом

$$|\mathrm{Aut}(D_4)| \leq 8$$

Сразу уточню, что на данном этапе довольно сложно будет сказать, что $|\mathrm{Aut}(D_4)| = 8$, т.к. не факт, что каждому из 8 различных наборов параметров соответствует некоторый автоморфизм (теоретически, это может оказаться простым гомоморфизмом, или еще хуже - отображение может даже до гомоморфизма не продолжаться). К сожалению $|\mathrm{Inn}(D_4)| = |D_4/Z(D_4)| = 4$, то есть внутренних автоморфизмов явно недостаточно для применения соображений мощности. Однако можно сделать следующее нетривиальное наблюдение: если перенумеровать осевые симметрии $\{b, ab, a^2b, a^3b\} = \{1, 2, 3, 4\}$ и расположить их в вершинах квадрата, то произвольный $\pi \in \mathrm{Aut}(D_4)$ будет переставлять эти осевые симметрии, и с учетом того, что композиции автоморфизмов соответствует композиция соответствующих перестановок - мы получаем действие на четырехэлементном множестве, а значит и гомоморфизм $\mathrm{Aut}(D_4) \to S_4$. Но оказывается, что если формально эти осевые симметрии симметрии расположить в вершине квадрата, то тогда это действие $\mathrm{Aut}(D_4)$ будет изометричным (в том смысле, что будет сохраняться взаимный порядок осевых симметрий вдоль этого формального квадрата):



Для проверки того, что порядок осевых симметрий на квадрате сохраняется, предположим, что две соседние осевые симметрии $a^k b$ и $a^{k+1}b$ перешли не в соседние, то:

$$\pi(a^{-1}) = \pi((a^k b)(a^{k+1}b)^{-1}) = \pi(a^k b)\pi(a^{k+1}b)^{-1}$$

и раз образы не являются соседними, то правая часть имеет вид a^2 (потому что именно таким групповым соотношением задается то, что симметрии не являются соседними), тогда как в левой части стоит либо a либо a^3, потому что порождающий $\langle a \rangle$ под действием автоморфизма обязан переходить в порождающий, что приводит к противоречию. Таким образом этот гомоморфизм в симметричную группу на самом деле снайперски попадает в группу Диэдра и мы получаем гомоморфизм:

$$\omega : \mathrm{Aut}(D_4) \to D_4$$

Сюръективность ω легко проверяется, так как если A, B - порождающие поворот и осевая симметрия группы Диэдра справа, то

$$\omega(\mathrm{Ad}_b) = B$$

$$\omega(T) = A$$

где $T \in \mathrm{Aut}(D_4)$ - это такой автоморфизм, что $T(a) = a$ и $T(b) = ab$. Проще всего убедиться в том, что T продолжается до автоморфизма всей группы, используя теорию копредставлений (то есть теорию задания группы с помощью порождающих и определяющих соотношений, которую мы обсудим позже). Группа Диэдра допускает следующее копредставление:

$$D_4 = \langle a, b | a^4 = b^2 = 1, b^{-1}ab = a^{-1} \rangle$$

Но так как:

$$T(a)^4 = a^4 = 1$$

$$T(b)^2 = (ab)^2 = 1$$

$$T(b)^{-1}T(a)T(b) = (ab)^{-1}a(ab) = a^{-1} = T(a)^{-1}$$

то из свойства универсальности определенное на порождающих отображение T продолжается до гомоморфизма $T : D_4 \to D_4$. Так как $a = T(a)$ и $b = a^{-1}ab = T(a)^{-1}T(b)$, то $\{a, b\} \in \mathrm{Im}\, T$, а раз они порождают группу Диэдра, то $\mathrm{Im}\, T = D_4$, то есть T является эпиморфизмом (эпиморфность можно доказать и таким немного примитивным способом: из-за того, что $T(a) = a$, $T(b) = ab$, мы получаем $\{ab, e, a, a^2, a^3\} \subset \mathrm{Im}\, T$, а значит $|T(D_4)| \geq 5$, что из теоремы Лагранжа влечет $|T(D_4)| = 8$, так как 8 - это единственный больший или равный 5 делитель 8). Так как сюръекция конечного множества в себя есть биекция, то T биективен, то есть является автоморфизмом.

Таким образом нами доказано, что ω эпиморфизм. В начале доказательства мы убедились, что $|\mathrm{Aut}(D_4)| \leq 8$, а значит из соображений мощности получаем, что ω - изоморфизм, иными словами $\mathrm{Aut}(D_4) \cong D_4$.

Замечание:

В общем случае верно $\mathrm{Aut}(D_n) \cong Hol(\mathbb{Z}_n)$, *где* $Hol(G) = G \rtimes \mathrm{Aut}(G)$ *голоморф группы* G, *в котором элемент* $\mathrm{Aut}(G)$ *действует на* G *как обычный автоморфизм, иными словами* $\mathrm{Aut}(D_n) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$, *где* $\mathbb{Z}_n^*$ *действует на* $\mathbb{Z}_n$ *умножением, иными словами является расширением циклической группы группой ее обратимых по умножению элементов. Здесь элементу* $m \in \mathbb{Z}_n$ *соответствуют поворот на* m *формального многоугольника* $\{b, ab, a^2b, \ldots, a^{n-1}b\}$, *у которого в вершинах находятся осевые симметрии, т.е. более формально элементу* $m \in \mathbb{Z}_n$ *соответствует автоморфизм* A_m, *определенный на порождающих* $A_m(a) = a, A_m(b) = a^m b$. *Элементу же* $k \in \mathbb{Z}_n^*$ *соответствует автоморфизм, заданный на порождающих* $B_k(a) = a^k, B_k(b) = b$, *то есть фактически* B_k *является поднятием автоморфизма* $m \mapsto km$ *подгруппы* $\mathbb{Z}_n = \langle a \rangle$ *до автоморфизма всей группы* D_n. *В важном частном случае* $n = 2, 4, p^k, 2p^k$ *для некоторого нечетного простого* p, *мы помним, что группа* $\mathbb{Z}_n^*$ *является циклической, а потому группа* $\mathrm{Aut}(D_n)$ *допускает простое копредставление:*

$$\mathrm{Aut}(D_n) = \langle A, B : A^n = 1, B^{\varphi(n)} = 1, BAB^{-1} = A^k \rangle$$

здесь A *- соответствует повотору на 1 формального многоугольника с осевыми симметриями в качестве вершин, то есть элементу* $1 \in \mathbb{Z}_n$, *а* $B = k \in \mathbb{Z}_n^*$ *- некоторый зафиксированный первообразный корень. В частности имеем* $|\mathrm{Aut}(D_n)| = \varphi(n)n$, *где* $\varphi(n)$ *- функция Эйлера. Подумайте над тем, при каких* n *верно* $\mathrm{Aut}(D_n) \cong D_n$*?*

Любая ли группа может быть группой автоморфизмов для некоторой другой группы? Отрицательный ответ дает следующий очень поучительный пример:

Задача

Доказать, что не существует группы G, *что* $\mathrm{Aut}(G) \cong \mathbb{Z}_{2n+1}$ *для некоторого* $n \geq 1$.

Я могу решить эту задачу только принимая аксиому выбора, не знаю, насколько она здесь существенна.

Первый шаг доказательства имеет самостоятельную ценность: рассмотрим цепочку:

$$G/Z(G) \cong \mathrm{Inn}(G) \lhd \mathrm{Aut}(G) \cong \mathbb{Z}_{2n+1}$$

Подгруппа циклической группы обязана быть циклической, причем мы помним, что фактор по центру может быть циклическим только в случае абелевой группы. Таким образом, G - абелева (иными словами у неабелевой группы группа автоморфизмов не может быть циклической: это наблюдение позволяет быстро отсеивать варианты или находить ошибки, к примеру, с ходу даже не вникая в детали вы можете сказать, что $\mathrm{Aut}(Q_8) \ncong \mathbb{Z}_4$).

Если G - абелева, то рассмотрим автоморфизм $T : G \to G$, заданный в мультипликативной форме формулой $T(x) = x^{-1}$. Возможностей для его порядка всего две:

Если $\mathrm{ord}(T) = 2$, то это противоречит теореме Лагранжа, т.к. $|\mathrm{Aut}(G)| = 2n + 1$.

Если $\mathrm{ord}(T) = 1$, то $x = x^{-1}$ для любого x, иными словами $x^2 = e$ для каждого элемента группы. В таком случае G можно рассматривать как линейное пространство над полем $\mathbb{Z}_2$, по аксиоме выбора можем построить базис в этом

пространстве: ясно, что в этом вырожденном случае автоморфизм линейного пространства это то же самое что и автоморфизм группы. Рассмотрим автоморфизм $M \in \mathrm{Aut}(G)$, переставляющий местами два выбранных базисных вектора, например, если бы базис был счетен, и мы бы выбрали первые два базисных вектора, то в координатах автоморфизм выглядел бы так:

$$M : (a, b, c, d \ldots) \mapsto (b, a, c, d \ldots)$$

Ясно, что $\mathrm{ord}(M) = 2$ - и опять приходим к противоречию с теоремой Лагранжа.

Замечания:

• *И хотя далеко не каждая группа может выступать группой автоморфизмов некоторой другой группы, как хорошо видно на этом примере - с другой стороны всякая (счетная) группа является* $\mathrm{Out}(G)$ *для некоторой группы* G.

• *Также же хочется отметить следующее: что в отношении группы автоморфизмов ситуация у групп самая сложная во всем зоопарке алгебраических структур. К примеру, в топологии есть такое понятие как жесткие пространства (rigid spaces), то есть пространства (нетривиальные), группа гомеоморфизмов которых тривиальна (вообще в математики говорят про жесткость (rigid) в тех ситуациях, когда при априорной большой степени свободы для некоторого отображения по факту оно жестко сводится к некоторому очевидному или в некотором смысле вырожденному случаю). Причем это странное пространство без гомеоморфизмов можно реализовать даже как пространство обычного* $\mathbb{R}$. *Также известен факт, что любая группа* G *является группой автоморфизма некоторого графа (не обязательно конечного). Математик де Грот (de Groot) гениально объединил эти две идеи и доказал, что для любой группы* G *существует метрическое пространство* X, *что его группа гомеоморфизмов* $Homeo(X) \cong G$, *причем в качестве такого пространства он взял граф из аналогичной теоремы для графов и заменил каждое ребро на жесткое пространство (сам граф было брать нельзя, так как помимо автоморфизмов графа, если мы переходим от графов к пространствам, могут быть еще гомеоморфизмы внутри самих ребер. Но если такое ребро заменить жестким пространством - то тогда таких внутриреберных гомеоморфизмов быть не может). И если от графов и пространств переходить к чему-то более алгебраическому - то сразу вспоминается теория* C^**-алгебр, одна из фундаментальных теорем в которой утверждает, что любая коммутативная* C^**-алгебра изоморфна алгебре стремящихся к нулю на бесконечности функций* $C_0(X)$ *на некотором локально компактном хаусдорфовом пространстве* X, *причем функтор контринвариантен. А значит любой автоморфизм такой алгебры приходит из гомеоморфизма подстилающего пространства, иными словами любой* $F : C_0(X) \to C_0(X)$ *имеет вид* $F(f)(x) = f(a^{-1}(x))$, *где* $a : X \to X$ *некоторый гомеоморфизм. Таким образом* $\mathrm{Aut}(C_0(X)) = Homeo(X)$. *Поэтому мы также сразу получаем насыщенное алгебраическими нотками утверждение, что для любой группы* G *существует алгебра* A *(даже* C^**-алгебра, даже коммутативная), что* $Aut(A) = G$ *(естественнее в категории* C^**-алгебр рассматривать не просто автоморфизмы, а непрерывные автоморфизмы, но оказывается, что любой автоморфизм (и даже гомоморфизм) между* C^**-алгебрами автоматически будет непрерывным). И как сильно это контрастирует с группами, где для групп автоморфизмов есть запретные группы (вроде* $\mathbb{Z}_{2n+1}$*). Да и вообще, очень мало понятно, какая группа может являться группой автоморфизмов некоторой другой группы: в этом*

вопросе с группами работать на порядок сложнее, чем с другими алгебраическими структурами).

Домашнее задание

Вычислите:

- *Явно вычислить* $\mathrm{Aut}(V_4)$ *(более явно, нежели* $GL_2(\mathbb{Z}_2)$*).*
- $\mathrm{Aut}(Q_8)$
- $\mathrm{Aut}(D_5)$
- *Существует ли* G*, такая, что* $\mathrm{Aut}(G) = \mathbb{Z}$*?*
- *Существует ли бесконечная группа* G*, такая что* $\mathrm{Aut}(G) = \{e\}$*?*

Группы движений фигур

Пусть $M \subset \mathbb{R}^n$. Определим соответственно *группу вращений* и *группу движений* фигуры M как:

$$\mathrm{Rot}(M) = \{g \in SO(n) : g(M) = M\}$$

$$\mathrm{Sym}(M) = \{g \in O(n) : g(M) = M\}$$

В качестве иллюстрации найдем эти группы для правильных многогранников в $\mathbb{R}^3$, которых, как мы знаем, 5 штук. Сразу же отмечу, что существенную помощь в доказательстве нам окажет применение орбитальной теоремы, которая практически задаром даст нам порядок этих групп, а когда порядок известен - доказательство упрощается, т.к. если группа угадана и гомоморфизм построен, то из соображений мощности достаточно доказывать эпиморфность вместо биективности.

Пример

Вычислить $\mathrm{Rot}(T)$ *и* $\mathrm{Sym}(T)$ *для правильного тетраэдра.*

Первым делом найдем порядок $\mathrm{Sym}(T)$ - рассмотрим произвольную точку тетраэдра x и применим к ней орбитальную теорему:

$$|\operatorname{Orb}(x)| = \frac{|\operatorname{Sym}(T)|}{|\operatorname{St}(x)|}$$

Ясно, что всего существует 6 движений, оставляющих зафиксированную точку неподвижной - это как раз всевозможные движения противоположного правильного треугольника. При этом орбита исходной точки состоит из всех 4 точек, потому что движениями тетраэдра, понятное дело, любую вершину можно перевести в любую другую. Таким образом:

$$4 = \frac{|\operatorname{Sym}(T)|}{6}$$

Т.е. $|\operatorname{Sym}(T)| = 24$. Мы с вами знаем одну хорошую группу порядка 24 - это S_4. Давайте попытаемся построить в нее гомоморфизм. С этой целью заметим, что группа движений тетраэдра естественным образом действует на множестве из четырех его вершин. Таким образом получаем гомоморфизм:

$$\pi : \operatorname{Sym}(T) \to S_4$$

Ясно, что это - эпиморфизм, т.к. любая транспозиция лежит в образе π: рассмотрим для определенности (12), тогда $\pi(S) = (12)$, где S - симметрия относительно плоскости, проходящей через 3,4 и середину отрезка [12]. Из соображений мощности получаем, что это изоморфизм.

Для описания $\mathrm{Rot}(T)$ заметим, что $|\operatorname{Sym}(T)| = 2|\operatorname{Rot}(T)|$ для всякого T: потому что если рассмотреть какую-нибудь меняющую ориентацию $\sigma \in \operatorname{Sym}(T)$, тогда

$$\operatorname{Sym}(T) = \operatorname{Rot}(M) \sqcup \sigma \operatorname{Rot}(M)$$

Действительно, если A - сохраняет ориентацию, то $A \in \mathrm{Rot}(T)$, а если нет, то $A = \sigma\sigma^{-1}A \in \sigma \operatorname{Rot}(T)$ потому что $\sigma^{-1}A \in \mathrm{Rot}(T)$. Таким образом в группе движений подгруппа вращений всегда имеет индекс 2.

Остается только заметить, что тройные циклы лежат в $\mathrm{Rot}(T) < \mathrm{Sym}(T) \cong S_4$, т.к. им соответствует повороты на 120 градусов вокруг высот тетраэдра. Таким образом $A_4 < \mathrm{Rot}(T)$. Но так как обе группы имеют порядок 12, то $\mathrm{Rot}(T) = A_4$.

Перед тем, как переходить к кубу - докажем пару теоретических утверждений:

Задача

Докажите, что $\mathrm{Rot}(M) \lhd \mathrm{Sym}(M)$.

Доказать это можно двумя способами: либо непосредственной проверкой: $A \in \mathrm{Rot}(M)$, $B \in \mathrm{Sym}(M)$, тогда

$$\det(B^{-1}AB) = \det(A) > 0$$

то есть $B^{-1}AB \in \mathrm{Rot}(M)$. Либо вспомнив, что подгруппа вращений имеет индекс 2, а такая подгруппа всегда нормальна.

Задача
Пусть $M \subset \mathbb{R}^{2n+1}$ *и* $T = -\mathrm{id} \in \mathrm{Sym}(M)$, *тогда* $\mathrm{Sym}(M) = \mathrm{Rot}(M) \times \mathbb{Z}_2$.

Для доказательства просто проверим критерий разложимости группы в прямое произведение двух его нормальных подгрупп ($A \cap B = \{e\}$ и $A \cdot B = G$): имеем две нормальны подгруппы: $\mathrm{Rot}(M), \langle -\mathrm{id}\rangle \lhd \mathrm{Sym}(M)$, причем $\mathrm{Rot}(M) \cap \langle -\mathrm{id}\rangle = \{\mathrm{id}\}$, так как $-\mathrm{id}$ в нечетномерных пространствах не сохраняет ориентацию (нормальность подгруппы $\langle -\mathrm{id}\rangle$ вытекает из ее центральности). Для доказательства равенства $\mathrm{Rot}(M) \cdot \langle -\mathrm{id}\rangle = \mathrm{Sym}(M)$ можно либо воспользоваться теоремой Лагранжа: так как индекс группы вращений равен 2, то не существует промежуточных подгрупп

$$\mathrm{Rot}(M) < H < \mathrm{Sym}(M)$$

но при этом $H = \mathrm{Rot}(M) \cdot \langle -\mathrm{id}\rangle$ строго содержит группу вращений, а значит обязательно $H = \mathrm{Sym}(M)$. Либо воспользоваться стандартным трюком: для любой $A \in \mathrm{Sym}(M)$ либо $A \in \mathrm{Rot}(M)$, либо $A \in \sigma\,\mathrm{Rot}(A)$ для некоторой несохраняющей ориентацию $\sigma \in \mathrm{Sym}(M)$ (если $A \notin \mathrm{Rot}(M)$, то $A = \sigma(\sigma^{-1}A) \in \sigma\,\mathrm{Rot}(M)$), которую в данном случае можно взять $\sigma = -\mathrm{id}$. Таким образом, с учетом того, что $\langle -\mathrm{id}\rangle \cong \mathbb{Z}_2$, мы получаем:

$$\mathrm{Rot}(M) \times \mathbb{Z}_2 \cong \mathrm{Sym}(M)$$

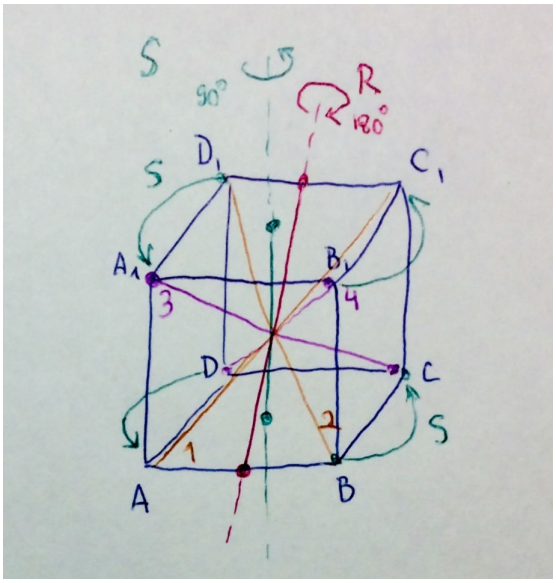
Пример
Вычислить $\mathrm{Sym}(Q)$ *и* $\mathrm{Rot}(Q)$ *для* Q *- куба.*

Так как $-\mathrm{id}$ является движением куба, то из предыдущего утверждения получаем, что $\mathrm{Sym}(Q) \cong \mathrm{Rot}(Q) \times \mathbb{Z}_2$, а потому найдем только группу вращений. Зафиксируем некоторую вершину x и применим к ней орбитальную теорему - орбита точки состоит из всех 8 вершин, при этом движения, оставляющие некоторую точку неподвижной - оставляют неподвижной диаметрально противоположную, ибо она единственная удалена на максимальное расстояние от точки x. Т.е. у нас зафиксированная диагональ (пальцами зажали две противоположные вершины) - и единственная оставшаяся степень свободы - это вращать вокруг этой диагонали. Всего таких поворотов 3 - на 0, 120 и 240 градусов. Таким образом $|\mathrm{Rot}(Q)| = 8 \cdot 3 = 24$. Хочется предположить, что это S_4, но для этого нужно сначала хотя бы построить туда гомоморфизм, придумав действие $\mathrm{Rot}(Q)$ на некотором 4-элементном множестве.

Итак, зададимся вопросом: а чего у куба 4 штуки? И ответ не заставляет себя долго ждать: диагонали, которые мы перенумеруем числами $\{1, 2, 3, 4\}$. Любое движение куба переставляет диагонали, а потому получаем гомоморфизм:

$$\pi : \mathrm{Rot}(Q) \to S_4$$

Ясно, что $\pi(R) = (12)$ и $\pi(S) = (1234)$, где R - поворот на 180 градусов вокруг отрезка, соединяющего середины AB и C_1D_1, а S - поворот на 90 градусов вокруг отрезка, соединяющего центры граней $ABCD$ и $A_1B_1C_1D_1$, где AC_1 - первая, BD_1 - вторая, CA_1 - третья, а DB_1 - четвертая диагональ соответственно. Так как (12) и (1234) порождают S_4, то π - эпиморфизм. Из соображений мощности получаем, что π на самом деле изоморфизм.



Таким образом

$$\mathrm{Rot}(Q) = S_4$$
$$\mathrm{Sym}(Q) = S_4 \times \mathbb{Z}_2$$

Докажу биективность вторым способом: вместо эпиморфности (которая мне представляется более поучительной, так как мы имеем дело с конкретными движениями), можно было доказать инъективность, что тоже влекло бы биективность из соображений мощности. Доказать можно следующими рассуждениями: пусть есть нетривиальный $T \in \mathrm{Rot}(Q)$, такой что $\pi(T) = \mathrm{id}$, т.е. он оставляет неподвижными все диагонали. Так как $T \neq \mathrm{id}$, то существует диагональ, на вершинах которой он не тождественен, а значит на этой диагонали он действует как $-\mathrm{id}$ (пусть это будет диагональ 1). Рассмотрим любую другую диагональ (например 2, в кубе они все равноправны) - так как T сохраняет расстояния, то точки, находящиеся на расстоянии 1 и $\sqrt{2}$ перейдут в точки, находящиеся на таком же расстоянии. Поэтому раз $\rho(A, B) = 1$ и $T(A) = C_1$, то тогда B должна перейти в точку, на расстоянии 1 от C_1, а так как T переводит BD_1 в себя, то $T(B) = D_1$ - это единственная возможность, ну и соответственно $T(D_1) = B$, то есть T действует на второй диагонали тоже как $-\mathrm{id}$. Эту процедуру можно повторить для всех диагоналей и получить, что на всех вершинах куба T действует как $-\mathrm{id}$, но так как движение $\mathbb{R}^3$ задается образами четырех точек, не лежащих в одной плоскости, то $T = -\mathrm{id}$ вообще на всех точках, что противоречит тому, что T сохраняет ориентацию.

Замечания:

• *Поясню, почему движение задается образом четырех точек: из линейной алгебры мы помним, что любое движение n-мерного пространства имеет в координатной записи вид $T(x) = Ux + b$, где b - произвольный вектор, а U - ортогональная матрица. Если у нас есть $n + 1$ точек $\{a_0, a_1, \ldots, a_n\}$, не лежащих в одной гиперплоскости, а значит $T(a_i)$ тоже не будут лежать в одной гиперплоскости, а значит векторы $y_i = T(a_i) - T(a_0)$ будут базисом $\mathbb{R}^n$, рассмотрим также базис $x_i = a_i - a_0$, и введем матрицы Y и X, где по столбцам последовательно записаны координаты всех векторов y_i и x_i соответственно в самом изначальном базисе. Легко заметить, что*

$$y_i = T(a_i) - T(a_0) = Ua_i + b - Ua_0 - b = U(a_i - a_0) = Ux_i$$

что на матричным уровне можно записать матричным уравнением:

$$Y = UX$$

Таким образом, раз мы имеем дело с базисами, то можно восстановить матрицу $U = YX^{-1}$, вектор b легко восстанавливается, например из равенства $b = T(a_0) - Ua_0$.

• *Есть еще более групповой и менее геометрический подход к вычислению группы движений куб: нетрудно заметить, что октаэдр - фигура двойственная к кубу, а потому у них одинаковые группы движений (двойственной к A называют фигуру B, вершинами которой являются в точности центры граней фигуры A, из условия сохранения расстояний легко понять, что центры граней (по крайней мере у правильных многогранников) переходят друг в друга). Далее, с помощью орбитальной теоремы легко понять, что порядок группы движений равен 48, таким образом достаточно предъявить 48 движений. Осталось заметить, что у октаэдра есть три диагонали, и в группе его движений есть подгруппа $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ симметрий диагоналей (т.е. относительно плоскостей, проходящих через начало координат и перпендикулярных одной из диагоналей, ясно, что все эти симметрии коммутируют, т.к. в стандартном базисе любая такая симметрия имеет диагональную матрицу) и подгруппа S_3, переставляющая эти три диагонали. Прямое произведение они не образуют, но образуют так называемое полупрямое произведение. По определению, если $\alpha : G \to \mathrm{Aut}(H)$, то полупрямым произведением групп называют группу*

$$H \rtimes G = \{(h, g) : h \in H, g \in G\}$$

со следующим правилом умножения:

$$(h_1, g_1) \circ (h_2, g_2) = (h_1 \alpha_{g_1^{-1}}(h_2), g_1 g_2)$$

иными словами пару (h, g) нужно трактовать себе как формальное произведение hg, для которого стандартное соотношение коммутации элементов из разных сомножителей заменено соотношением $\alpha_g(h) = g^{-1}hg$. Полупрямые произведения лишь отдаленно напоминают прямые произведения, несомненное их преимущество, что некоторые группы (особенно связанные с движениями или автоморфизмами) допускают разложение в полупрямое произведение - и это разложение оказывается чуть ли не единственной конструктивной формой, с которой реально можно работать (достаточно вспомнить $\mathrm{Aut}(D_n) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$ - разве получится у вас как-то еще эту группу конструктивно описать? Или группа движений n-мерного куба $\mathrm{Sym}(I^n)$, которую мы сейчас опишем). Еще одно важное свойство полупрямых произведений, что все автоморфизмы из $\mathrm{Im}\,\alpha < \mathrm{Aut}(H)$ на H имеют вид Ad_g для некоторого $g \in G$ как видно из формулы $\alpha_g(h) = g^{-1}hg$, то есть самый дикий автоморфизм, которому до внутреннего автоморфизма как до Луны, будет обычным сопряжением, правда сопрягающий элемент будет жить в объемлющей группе $H \rtimes G$.

Полупрямое произведение можно задать с помощью копредставления: пусть $R(H), R(G)$ - все соотношения групп H, G соответственно, тогда

$$H \rtimes G = \langle H, G : R(H), R(G), \alpha_g(h) = g^{-1}hg \text{ для всех } g \in G, h \in H \rangle$$

Также $H \lhd H \rtimes G$, при этом $G < H \rtimes G$ уже не обязана быть нормальной. В частном случае, когда $\alpha_g(h) = h$ действие автоморфизмами G на H тривиально, то мы получаем обычное прямое произведение $H \times G$. Придумайте себе какое-нибудь мнемоническое правило для запоминания, с какой стороны палку в полупрямом произведении нужно ставить: лично мне $\rtimes$ напоминает клещи, с помощью которых G хватает H (раз она на ней действует) - поэтому палку ставим ближе к группе, которая действует. Либо можно считать, что раз $H \lhd H \rtimes G$, то слева полупрямое произведение больше похоже на прямое произведение - а потому палка там не нужна.

Возвращаемся: таким образом можно непосредственно проверить, что подгруппы $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ и S_3 связаны определяющими полупрямое произведение соотношениями (то есть что у них пересечение состоит только из $\{e\}$ и что $\alpha_g(h) = g^{-1}hg$ вместо коммутации в прямом произведении), а потому $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes S_3 < \mathrm{Sym}(Q)$, но так как обе группы имеют порядок 48, то получаем:

$$\mathbb{Z}_2^3 \rtimes S_3 = \mathrm{Sym}(Q)$$

Самое интересное, что ситуация нисколько не меняется в многомерном случае - опять можно рассмотреть двойственный к гиперкубу гипероктаэдр, в группе симметрий которого есть "диагональная" подгруппа симметрий диагоналей $\mathbb{Z}_2^n$ и подгруппа перестановок диагоналей S_n, образующих полупрямое произведение. Из соображений мощности можно доказать, что это все движения, таким образом:

$$\mathrm{Sym}(I^n) = \mathbb{Z}_2^n \rtimes S_n$$

где I^n - n-мерный куб. В частности $|\mathrm{Sym}(I^n)| = 2^n n!$, причем подставив $n = 3$ мы как раз получим 48 движений, которые в примере мы получили геометрическими методами. Также отмечу, что вычислив группу движений куба двумя способами, мы получили довольно интересный изоморфизм $S_4 \times \mathbb{Z}_2 \cong \mathbb{Z}_2^3 \rtimes S_3$.

Ну и вторая пара - это двойственные друг к другу додекаэдр и икосаэдр. Признаться, для них очень сложно на словах и двумерных картинках объяснять свойства группы движений - а потому советую для наглядности в этой задаче склеить самостоятельно бумажный додекаэдр и повертеть его: такой интерактив может раскрыть совершенно шокирующие геометрические свойства платоновых тел, которые вы никогда не увидите ни на двумерных картинках, ни в 3D-программах.

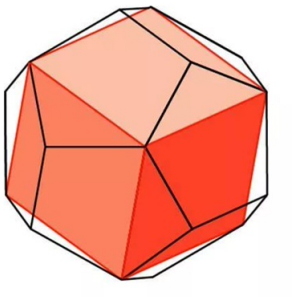
Пример

Вычислить $\mathrm{Sym}(D)$ и $\mathrm{Rot}(D)$ для D - додекаэдра.

Во-первых, $-\mathrm{id}$ является движением додекаэдра, а потому $\mathrm{Sym}(D) \cong \mathrm{Rot}(D) \times \mathbb{Z}_2$ и достаточно только группу вращений вычислить. Во-вторых, с помощью орбитальной теоремы можно вычислить порядок группы вращений: фиксируем произвольную вершину - ее орбита состоит из всех 12 вершин додекаэдра, потому что совершая повороты вдоль осей, перпендикулярных граням - точку можно "сдвинуть" вдоль любого ребра, и последовательными сдвигами вдоль ребер по ломанной добраться до любой другой точки. Что касается стабилизатора - то если точка зафиксирована - то зафиксирована и диаметрально противоположная, т.к. она единственная удалена на максимальное расстояние - следовательно зафиксирована ось и вращать можем только относительно нее. Ясно, что додекаэдр оставляют

на месте повороты на углы, кратные 120 градусам, а потому стабилизатор имеет порядок 3, а значит из орбитальной теоремы получаем $|\operatorname{Rot}(D)| = 60$.

Есть надежда, что это группа A_5, т.к. это единственная более/менее интуитивно подходящая группа порядка 60, а потому нужно придумать гомоморфизм $\operatorname{Rot}(D) \to S_5$, иными словами найти действие на пятиэлементном множестве. Давайте ответим себе на вопрос: чего у додекаэдра 5 штук? И тут уже ответ не такой очевидный, но оказывается, что у додекаэдра 5 вписанных кубов.



Перестановки этих кубов дают гомоморфизм

$$\pi : \operatorname{Rot}(D) \to S_5$$

Далее заметим, что $\pi(T) = (* * *)$, где T описанный выше поворот на 120 градусов вокруг оси, соединяющей диаметрально противоположные точки. В силу равноправия всех кубов на самом деле мы можем таким образом получить любой тройной цикл в образе. Но так как тройные циклы порождают A_5, то получаем:

$$A_5 < \operatorname{Im}\pi$$

Из этого вложения, а также с учетом факта, что образ гомоморфизма π не может иметь больше элементов, чем исходная группа $\operatorname{Rot}(D)$, мы приходим к неравенствам $|A_5| \leq |\operatorname{Im}\pi| \leq |\operatorname{Rot}(D)|$, и из соображений мощности и теоремы о гомоморфизме, примененной к $\pi : \operatorname{Rot}(D) \to \operatorname{Im}\pi$, получаем, что

$$\operatorname{Rot}(D) \cong \operatorname{Im}\pi \cong A_5$$

У икосаэдра, как у двойственного, такие же группы поворотов и движений.

Домашнее задание

Вычислить группы поворотов и движений для правильного ромбоусеченного икосододекаэдра, и вообще, советую разобраться с группами движений полуправильных многогранников: ясно, что у них не будет так много симметрий, как у правильных, а потому их группы движений будут "меньше" групп движений Платоновых тел. Советую также попытаться вычислить группы симметрий правильных многогранников более высокой размерности, например 4. Одно из направлений развития групп движений - это кристаллографические группы, определяемые как группы, переводящие в себя некоторый периодичный узор.

Раскраски

Одним из приложений действий групп в элементарной математике является подсчет количества различных раскрасок заданного множество в фиксированное количество цветов. Конечно же, это количество можно вычислить и чисто комбинаторно, но как правило комбинаторное решение на порядок сложнее группового.

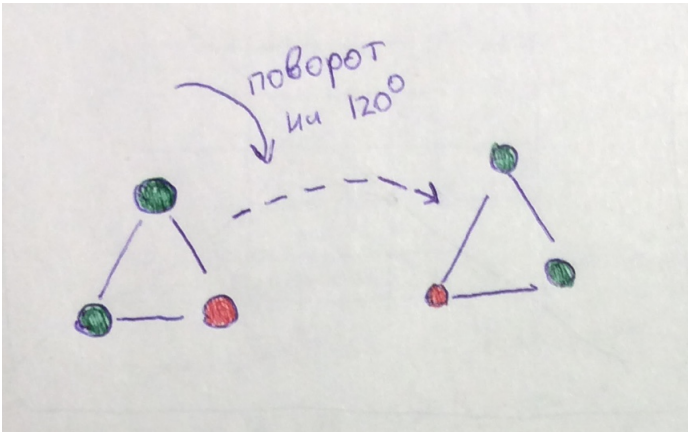
Формальная постановка задачи следующая: пусть X - некоторое конечное множество с заданным на нем действием некоторой группы $G \curvearrowright X$. Пусть $Ц = \{red, blue, \ldots\}$ - множество цветов, $|Ц| = q$. Тогда раскраской называют функцию $f : X \to Ц$. Ясно, что тотальное количество раскрасок равно $q^{|X|}$ - каждый элемент множества можно раскрасить в q цветов. Однако это число не очень интересное, потому что типично, что фигура X симметрична и из контекста задачи естественно отождествлять раскраски, переходящие одна в другую при симметриях. Чтобы более формально определить настоящее число раскрасок, рассмотрим множество:

$$\Omega = \{f : X \to Ц\}$$

Действие $G \curvearrowright X$ индуцирует естественное действие $G \curvearrowright \Omega$, заданное формулой $g \circ f(x) = f(g^{-1}x)$, иными словами групповой элемент действует на функцию, "подкручивая" ее аргумент - это стандартная математическая конструкция (отмечу, что умножать нужно на g^{-1}, чтобы получилось действие, а не анти-действие, потому что в противном случае:

$$g(hf(x)) = gf(hx) = f(hgx) = (hg)f(x)$$

Таким образом получается анти-гомоморфизм вместо гомоморфизма). Проиллюстрирую, как поворот на 120 градусов действует на следующей определенной на треугольнике цветовой функции:



И правильно считать эти две раскраски одинаковыми, если они переводятся одна в другую под действием некоторого элемента группы. Формально, мы можем дать следующее:

Определение

Раскраской мы будем называть орбиту этого действия $G \curvearrowright \Omega$, т.е. элемент Ω/G.

Количество раскрасок в данном случае по определению равно количеству орбит $|\Omega/G|$.

Для количества раскрасок есть относительно явная формула: рассмотрим вспомогательное множество $\Omega^g = \{w : gw = w\} \subset \Omega$ - некий аналог стабилизатора, живет он только в множестве Ω, а не группе G. Тогда с одной стороны:

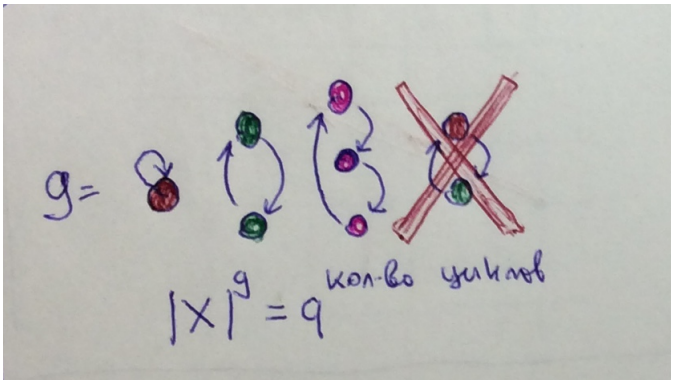
$$\sum_{g\in G} |\Omega^g| = |\{(g,w) : gw = w\}| = \sum_w |\operatorname{St}(w)| = \sum_w \frac{|G|}{|\operatorname{Orb}(w)|} = |G| \cdot \{\text{ количество орбит}\}$$

Последнее равенство выполняется, потому что в отличие от формулы орбит суммирование проводится не по всем орбитам, а по всем элементам пространства. Ясно, что соответствующие элементам одной и той же орбиты слагаемые одинаковы, а потому каждая орбита даст одинаковый вклад:

$$\frac{|G|}{|\operatorname{Orb}(w)|} + \ldots + \frac{|G|}{|\operatorname{Orb}(w)|} = |G|$$

слагаемых в данном блоке $|\operatorname{Orb}(w)|$ штук. И если каждая орбита вносит вклад $|G|$, то все орбиты дадут вклад $|G| \cdot \{$ количество орбит$\}$.

С другой стороны $|\Omega^g|$ можно вычислить в терминах циклической структуры $g \in S(X)$, для наглядности рассмотрим следующий пример:



Здесь множество X состоит из 6 элементов и стрелочками показано как на нем действует элемент g. Тогда ясно, что $gw = w \Leftrightarrow$ цвета вдоль каждого независимого цикла одинаковые, и что в общем случае ситуация будет точно такая же. Таким образом $|\Omega^g| = q^{\text{количество циклов } g}$, причем отмечу, что не нужно забывать про циклы длины 1, которые обычно в перестановке не отображаются, но они есть. Объединяя эти два наблюдения получаем окончательную формулу:

$$\boxed{|\Omega/G| = \frac{\sum\limits_{g\in G} q^{\text{количество циклов } g}}{|G|}}$$

В принципе, эту формулу можно использовать не только для вычисления количества раскрасок, но и для более общей задачи вычисления количества орбит пространства функций с индуцированным действием, если вдруг такое количество зачем-то понадобится. И сразу примеры, потому что без них эту формулу довольно непросто переварить:

Задача

Найти число раскрасок вершин правильного треугольника в 5 цвета, где раскраски отождествляются посредством

- *Тривиальной группы $G = \{e\}$*
- *Полной группы симметрий $G = S_3$*

В первом случае число раскрасок совпадает с тотальным числом раскрасок, т.к. из-за того, что группа тривиальная, то никакие тотальные раскраски мы не отождествляем. Таким образом число раскрасок:

$$N = 5^3 = 125$$

В принципе этот ответ можно было получить и из общей формулы: $|G| = 1$, при этом количество циклов $= 3$, т.к.каждый цикл имеет длину 1.

Во втором случае ситуация уже нетривиальная, хотя в силу специфики задачи получается, что циклическая структура действия $g \in G$ на X совпадает с его изначальной циклической структурой как перестановки из S_3. Таким образом описанная выше формула из рамочки дает:

$$N = \frac{5^3 + 5^1 + 5^1 + 5^2 + 5^2 + 5^2}{6} = 35$$

Замечания:

В сумме число слагаемых совпадает с порядком группы, однако в большинстве случаев бывает полезно объединять их в группы действующих "качественно одинаково", то есть имеющих одну и ту же циклическую структуру. Также отмечу, что в группе всегда есть нейтральный элемент, который при любом действии имеет циклическую структуру, состоящую исключительно из циклов длины 1, а потому в сумме всегда будет присутствовать соответствующее id *слагаемое $q^{|X|}$. Также отмечу, что количество раскрасок зависит не только от множества, но и от группы симметрий тоже; хотя с практической точки зрения для данного множества как правило понятно, какую группу симметрий естественно рассматривать.*

Задача

Найти число раскрасок правильного шестиугольника в q цветов, где раскраски отождествляются посредством группы D_6.

Посмотрим на циклические структуры элементов группы Диэдра:

• Повороты:

$e \leftrightarrow (*)(*)(*)(*)(*)(*)$

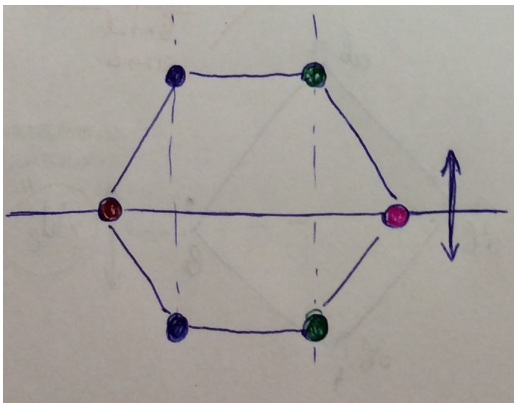
$a, a^{-1} \leftrightarrow (******)$

$a^2, a^{-2} \leftrightarrow (***)(***)$

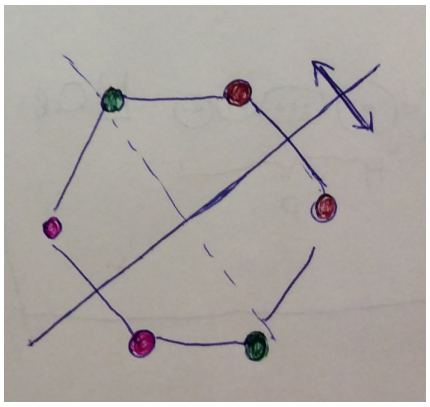
$a^3 \leftrightarrow (**)(**)(**)$

• Симметрии:

Симметрии относительно диагоналей $b, a^2b, a^4b \leftrightarrow (*)(*)(**)(**)$



Симметрии относительно "медиан" $ab, a^3b, a^5b \leftrightarrow (**)(**)(**)$



Подставляя полученную информацию в формулу из рамочки (и объединяя для удобства слагаемые с одинаковой циклической структурой), получаем количество раскрасок:

$$N = \frac{q^6 + 2q + 2q^2 + q^3 + 3q^4 + 3q^3}{12}$$

Я думаю, что вы согласитесь, что подобные формулы получается практически задаром, учитывая, насколько нетривиальной является поставленная задача с комбинаторной точки зрения.

Домашнее задание:

Потренируйтесь и найдите:

1) Число всевозможных молекул из 3 атомов, где атомы располагаются в вершинах правильного тетраэдра, а молекулы отождествляются посредством действия S_4 на тетраэдре. В задаче считать, что химические ограничения на взаимное расположение атомов отсутствуют: то есть в каждой вершине тетраэдра мы можем разместить любой атом.

2) Сколько существует раскрасок правильного семиугольника (его иногда называют гептагоном) в q цветов, где раскраски отождествляются посредством D_7. Фактически, нужно найти количество способов сплести 7-звенное ожерелье из q типов бусинок.

3) Сколько существует раскрасок куба в 2 цвета, $G =$группа вращений куба.

Разрешимые группы

Группа называется *разрешимой*, если $G^{(n)} = \{e\}$ для некоторого n, и *нильпотентной*, если $G_{(n)} = \{e\}$ для некоторого n (здесь $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$, $G_{(n)} = [G_{(n-1)}, G]$ определяются с помощью рекуррентной формулы ($G^{(0)} = G_{(0)} = G$), минимальное такое n называется *ступенью разрешимости/нильпотентности*). Разрешимость изначально появилась для разрешимости уравнений, нильпотентность тесно связана с нильпотентностью из алгебры. И разрешимость и нильпотентность нужно понимать как условие на то, что группа достаточно хорошая. Так как $G^{(n)} < G_{(n)}$, то *из нильпотентности вытекает разрешимость*. Уточню, что по аналогии с коммутантами по определению $[H_1, H_2] = \langle [h_1, h_2] : h_i \in H_i \rangle$, так как все-таки ранее определенный коммутант формально всегда имел вид $[G, G]$. Так называемый *взаимный коммутант* $[H_1, H_2]$ по свойствам очень похож на обычный коммутант, к примеру, если подгруппы нормальны $H_i \lhd G$, то и $[H_1, H_2] \lhd G$. Нильпотентные группы - это класс групп, в некотором смысле наиболее приближенных к абелевым.

Тривиальный пример: абелева группа является и разрешимой, и нильпотентной: потому что $G^{(1)} = G_{(1)} = \{e\}$, ступени разрешимости и нильпотентности равны 1. Более того, верно и обратное: что если ступень разрешимости/нильпотентности равна 1 - то группа абелева, что ясно из определения.

Исторически впервые разрешимые группы появились в работах Галуа 1830 года (ему тогда было 18 лет), где для произвольного n он доказал эквивалентность разрешимости уравнений n-ой степени в радикалах и разрешимости соответствующей группы Галуа, являющейся просто группой автоморфизмов некоторого связанного с уравнением расширения поля, тождественных на исходном поле (в частности если уравнение не имеет кратных корней и поле расширяется этими корнями, то любой автоморфизм просто переставляет эти корни, и в этом случае группа Галуа будет равна группе перестановок на множестве корней). В частности из его работ вытекает, что раз группы S_n неразрешимы при $n \geq 5$, то нет общей формулы через радикалы для решений уравнений степени 5 (и выше). Разрешимые группы получили свое название как раз из-за их связи с разрешимостью уравнений в радикалах. Что касается нильпотентных групп, то они так называются, потому что если для $g \in G$ рассмотреть присоединенное отображение $ad_g : G \to G$, $ad_g(x) = [g, x]$ (тесно связанное с теорией групп Ли), то $(ad_g)^n(x) = e$, где n это ступень нильпотентности. Более кратко: в нильпотентных группах присоединенное отображение нильпотентно. У меня ассоциативно такое название этих групп еще связывается с тем, что типичный пример нильпотентных групп - это подгруппа верхнетреугольных матриц, у которых на диагонали стоят 1, то есть фактически матриц, имеющих вид 1 + нильпотентная матрица.

Как проверять?

Для разрешимости - либо считаем коммутанты, либо применяем теорему:

Теорема

Пусть $H \lhd G$, тогда G - разрешима $\Leftrightarrow$ группы H и G/H - разрешимы.

Как правило применение это теоремы сводит задачу к изучению двух более простых групп. Для нильпотентности аналога этой теоремы нет - а потому нужно вычислять коммутанты.

Полезные свойства:

• Если $H < G$ и G разрешима/нильпотентна, то и H - разрешима/нильпотентна соответственно.

• Если π - гомоморфизм, то $\pi([H,K]) = [\pi(H), \pi(K)]$. В частности $\pi(H)^{(k)} = \pi(H^{(k)})$ и $\pi(H)_{(k)} = \pi(H_{(k)})$.

Задача

Доказать разрешимость группы Q_8.

Рассмотрим $H = \langle i \rangle \lhd Q_8$ (нормальность можно либо непосредственно проверить, либо заметить, что $\langle i \rangle$ подгруппа индекса 2). Тогда H разрешима (потому что абелева) и $Q_8/H \cong \mathbb{Z}_2$ разрешима. Значит по теореме Q_8 разрешима.

Задача

Исследовать на разрешимость и нильпотентность S_4.

$G = S_4$, $G^{(1)} = [S_4, S_4] = A_4$, $G^{(2)} = [A_4, A_4] = V_4$, $G^{(3)} = [V_4, V_4] = \{e\}$ - мы это вычисляли ранее. Значит S_4 - разрешима ступени 3.

Можно рассуждать так: группы V_4 и $A_4/V_4 \cong \mathbb{Z}_3$ абелевы - а потому разрешимы. Значит по теореме A_4 - разрешима. Так как $S_4/A_4 \cong \mathbb{Z}_2$ - разрешима, то и S_4 - разрешима. Такой подход более предпочтителен, когда достаточно лишь факта разрешимости без точного значения для ступени разрешимости. Также отмечу, что ступень разрешимости - это минимальная длина нормального ряда:

$$\{e\} \lhd G_1 \lhd \ldots \lhd G_n = G$$

каждый фактор которого абелев, а потому раз S_4/A_4, A_4/V_4 и V_4 абелевы - то мы можем сразу сказать, что для группы S_4 ступень разрешимости ≤ 3.

$G = S_4$, $G_{(1)} = [G, G] = A_4$. Вычислим $G_{(2)} = [A_4, S_4]$. Ясно, что $[A_4, S_4] < A_4$. С другой стороны:

$$[(ijk), (ij)] = (ijk)(ij)(ijk)^{-1}(ij)^{-1} = (jk)(ij) = (ijk)$$

Синее произведение легко вычисляется с использованием формулы для сопряжения перестановок. Так как A_4 порождается тройными циклами, то имеем $A_4 < [A_4, S_4]$. Таким образом $[A_4, S_4] = A_4$, т.е. $G_{(n)} = A_4$ для любого $n \geq 2$, а значит S_4 не является нильпотентной.

Задача

Разрешима ли группа S_n при $n \geq 5$?.

Имеем $[S_n, S_n] = A_n$, но $[A_n, A_n] = A_n$ (так как группа A_n является простой), значит $G^{(k)} = A_n$ при $k \geq 1$ и группа S_n не является разрешимой. Замечу, что любая простая группа является разрешимой только если она абелева, то есть изоморфна $\mathbb{Z}_p$ для некоторого простого p.

Утверждение
Пусть $|G| = p^n$. Доказать нильпотентность G.

Докажем утверждение задачи по индукции: при $n = 1$ очевидно, пусть для меньших степеней уже доказано - докажем для n. Ранее было доказано, что $Z(G) \neq \{e\}$. Значит $(G/Z(G))_{(k)} = \{e\}$ для некоторого k, так как фактор-группа имеет порядок строго меньше чем у G. Рассмотрим канонический эпиморфизм $\pi : G \to G/Z(G)$. Согласно второму полезному свойству имеем:

$$\pi : G_{(k)} \to (G/Z(G))_{(k)} = \{e\}$$

Значит $G_{(k)} < \ker \pi = Z(G)$. Таким образом:

$$G_{(k+1)} = [G_{(k)}, G] < [Z(G), G] = \{e\}$$

Более того, раз на каждом шаге индукции порядок группы уменьшался в кратное p число раз, а ступень увеличивалась каждый раз на единицу - то ступень нильпотентности исходной группы G будет $\leq n$.

Пример
Доказать нильпотентность группы Гейзенберга.

Напомню, что группа Гейзенберга - это

$$H = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{Z} \right\}$$

Непосредственной проверкой убеждаемся в формулах:

$$\left[\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 & xc - az \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\left[\begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Ясно, что $[H, H] = \left\{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{Z} \right\}$ - потому что такие матрицы реализуются как коммутаторы ($x = x, c = 1, a = z = 0$) и замкнуты относительно умножения. Таким образом $[[H, H], H] = \{e\}$, т.е. H - нильпотентная ступени 2.

Пример

Доказать разрешимость группы

$$G = \left\{ \begin{pmatrix} \alpha & x & y \\ 0 & \beta & z \\ 0 & 0 & \gamma \end{pmatrix} : x, y, z \in \mathbb{R}, \alpha, \beta, \gamma \in \mathbb{R}^* \right\}$$

Рассмотрим вещественный аналог группы Гейзенберга:

$$H = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{R} \right\}$$

В решении предыдущей задачи мы принципиально нигде не использовали целочисленность коэффициентов, а потому H тоже является нильпотентной. Из правила умножения матриц вытекает, что умножение любых верхнетреугольных матриц $g, h \in G$ на уровне диагональных элементов сводится к обычному поэлементному умножению диагональных элементов:

$$\begin{pmatrix} a & ? & ? \\ 0 & b & ? \\ 0 & 0 & c \end{pmatrix} \cdot \begin{pmatrix} x & ? & ? \\ 0 & y & ? \\ 0 & 0 & z \end{pmatrix} = \begin{pmatrix} ax & ? & ? \\ 0 & by & ? \\ 0 & 0 & cz \end{pmatrix}$$

Аналогичный факт верен и про взятие обратного. А потому:

$$[G, G] < H$$

Таким образом, раз $[G, G]$ является разрешимой (потому что она является даже нильпотентной как подгруппа нильпотентной H), то и G является разрешимой. Однако нильпотентной она уже не будет: для доказательства отсутствия нильпотентности докажем сначала, что $[H, G] = H$. Нетрудно убедиться в равенстве:

$$\left[\begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$$

И если рассматривать блочные матрицы в H и G, у которых в 2×2 блоке, соответствующем i, j строке, стоят матрицы, для которых мы вычисляли коммутатор, а в оставшемся блоке - единичная матрица (отмечу, что блоки могут быть "разорванными"), тогда коммутатор таких блочных матриц будет равен матрице $E_{ij}(\alpha) = E + \alpha e_{ij} \in [H, G]$, но такие матрицы - это в точности матрицы элементарных преобразований метода Гаусса, и ясно, что любая матрицы $h \in H$ может быть получена такими элементарными преобразованиями из единичной матрицы E (так как h треугольная - то можно обойтись и без матриц, меняющих строки/столбцы), на алгебраическом языке это означает, что $h = x_1 x_2 \dots x_k$, где x_i - матрицы элементарных преобразований, иными словами $h \in [H, G]$, то есть $H < [H, G]$, но с учетом очевидного вложения $[H, G] < H$ (потому что $h(gh^{-1}g^{-1}) \in H$ из-за $H \lhd G$) мы получаем $[H, G] = H$.

Также по доказанному ранее $[G, G] < H$, но с учетом только что доказанного равенства мы получаем $H = [H, G] < [G, G]$. Таким образом $[G, G] = H$, что вместе с $[H, G] = H$ дает $G_{(n)} = H$ для любого n, и группа G не будет нильпотентной.

Замечания:

• *Замечу также, что верхнетреугольные матрицы с 1 на диагонали - типичный пример нильпотентных групп, а просто верхнетреугольные обратимые матрицы - типичный пример разрешимых. Есть даже теоремы, что при некоторых разумных условиях разрешимая группа вкладываются в группу верхнетреугольных обратимых матриц.*

• *Отмечу, что* $[a,b]^{-1} = [b,a]$, *а потому* $[H_1, H_2] = [H_2, H_1]$, *а потому не так важно определяется ли нижний центральный ряд рекуррентной формулой* $G_{(n+1)} = [G_{(n)}, G]$ *или же* $G_{(n+1)} = [G, G_{(n)}]$. *Сразу возникает вопрос, почему этот ряд называется "нижним"? Значит есть и "верхний"? Да, и картина здесь следующая:*

Есть более теоретизированный подход к определению нильпотентных групп: а именно группа называется нильпотентной $\Leftrightarrow$ *она допускает центральный ряд:*

$$\{e\} = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$$

то есть такой ряд, что $[G, H_{i+1}] < H_i$ *(из этого вложения в частности вытекает, что* $[G, H_{i+1}] < H_i < H_{i+1}$, *а значит для любого* $g \in G$ *и* $h \in H_{i+1}$ *выполнено* $ghg^{-1}h \in H_{i+1}$, *в частности все* H_i *будут нормальными). Центральность последовательности понимается в том смысле, что все последовательные факторы* $H_{i+1}/H_i = Z(G/H_i)$ *являются соответствующими центрами. Таких центральных рядов у группы может быть много, и интересно, что к построения оптимальных и в то же время конструктивных примеров можно подойти с двух сторон и получить различные центральные ряды: первый подход - это стартуя с* G *двигаться сверху вниз и последовательно строить* $H_n, H_{n-1}, H_{n-2}, \ldots$ *- и проще всего в роли* H_i *брать те самые определенные рекуррентно через коммутанты* $G_{(n)}$, *через которые мы и определяли нильпотентные группы, правда нужно их перечислять в обратном порядке, потому что мы их нумеровали от* G *к* $\{e\}$*). Кстати, для них равенство* $[G, H_{i+1}] = H_i$ *реализуется в точности.*

Но ряд H_i *можно строить и снизу вверх, стартуя с* $\{e\}$ *и двигаясь к* G*: а именно построить ряд* $\{e\} = Z_0(G) \lhd Z_1(G) \lhd Z_2(G) \ldots$, *который определяется следующим образом:* $Z_1(G) = Z(G)$, *и:*

$$Z_{i+1}(G) = \{x \in G : [x, y] \in Z_i(G) \text{ для любого } y \in G\}$$

то есть $Z_{i+1}(G)$ *состоит из элементов, коммутирующих со всеми элементами группы, но при факторизации по* $Z_i(G)$, *своего рода это такой супер-центр. В иных терминах* $Z_{i+1}(G) = \pi_i^{-1}(Z(G/Z_i(G)))$, *где* $\pi_i : G \to G/Z_i(G)$ *канонический эпиморфизм, либо определяющее условию записывают как* $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$. *Построенный таким образом ряд* $Z_i(G)$ *называется верхним центральным рядом.*

Оказывается, что для нильпотентных групп как верхний так и нижний ряд являются кратчайшими среди всех возможных центральных рядов, а потому их длины совпадают - а значит в определении ступени нильпотентности не важно, к какому центральному ряду ее привязывать. Однако несмотря на совпадение их длин - члены рядов могут не совпадать, что хорошо видно на примере $G = \mathbb{Z}_2 \times Q_8$*:*

Нижний центральный ряд: $\{e\} \times \{1\} \lhd \{e\} \times \{-1, 1\} \lhd \mathbb{Z}_2 \times Q_8$

Верхний центральный ряд: $\{e\} \times \{1\} \lhd \mathbb{Z}_2 \times \{-1, 1\} \lhd \mathbb{Z}_2 \times Q_8$

В нижнем центральном ряду промежуточный член равен $G_{(1)} = [G, G]$, *а у верхнего* $Z_1(G) = Z(G)$, *и они не совпадают. Однако в общем случае каждый член нижнего центрального ряда является подгруппой соответствующее члена верхнего центрального ряда, а именно верно даже более сильное утверждение:*

Теорема
Если $\{e\} = H_0 \lhd H_1 \lhd H_2 \lhd \dots H_n = G$ произвольный центральный ряд, тогда

$$G_{(n-i)} < H_i < Z_i(G)$$

Поэтому верхний и нижний центральные ряды так и называются: верхний - самый большой, а нижний - самый маленький. В частности из этой теоремы вытекает, что если верхний и нижний центральные ряды совпали, то им будут равны и все остальные центральные ряды. При первом ознакомлении я советую глубоко не погружаться в тонкости этих рядов, так как с ними очень легко запутаться, и на первых порах хорошо хотя бы почувствовать разницу между разрешимыми и нильпотентными группами. Также уточню, что ряд $G_{(i)}$ *на порядок более простой и конструктивный чем* $Z_i(G)$, *и с ним в большинстве случаем намного проще работать.*

Скажу пару слов об аналогичном подходе и к определению разрешимых групп: их можно определять как группы, допускающие нормальный ряд с абелевыми факторами, а именно:

$$\{e\} = H_0 \lhd H_1 \lhd \dots H_n = G$$

такие что H_{i+1}/H_i *является абелевой. Центральные ряды являются частными случаями таких, потому что в случае центральных рядов* H_{i+1}/H_i *не просто абелева, а даже изоморфна центру некоторой связанной с рядом группы (поэтому из нильпотентности вытекает разрешимость). В роли* H_i *всегда можно взять* $H_i = G^{(n-i)}$, *и это единственная универсальная естественная конструкция в отличие от нильпотентных групп, для которых есть два естественных центральных ряда.*

Как мы уже поняли, вопрос проверки разрешимости трудный даже для конечных групп, однако очень многие случаи покрываются следующей теоремой:

Теорема (Фейта-Томпсона)
Пусть порядок G нечетен - тогда G разрешима.

Теорема очень мощная: к примеру, спрашивают вас: разрешима ли группа порядка 16257, а вы говорите: "по теореме Фейта-Томпсона она разрешима".

Однако доказывается теорема очень сложно, она была доказана в 1963 года на 250 страниц и лишь относительно недавно математики сошлись во мнении, что в доказательстве нет ошибок. За эти десятилетия доказательство пытались привести в более презентабельный вид, но улучшались лишь небольшие локальные кусочки, оставляя общую структуру доказательства неизменной. Отмечу, что эта теорема также являются частью доказательства "Классификации" на 10000 страниц, так как из этой теоремы вытекает, что неабелева группа нечетного порядка не может быть простой, иначе она не могла бы быть разрешимой (т.к. в ней не было бы нетривиальных нормальных подгрупп). Отмечу также, что один из авторов Томпсон не является тем самым Томпсоном, в честь которого назвали группу Томпсона F, играющую огромную роль в теории аменабельных групп. Кстати, Томпсон (который автор теоремы) нашел одну из спорадических простых групп, и она обычно обозначается Th и тоже называется группой Томпсона. Порядок Th примерно равен 10^{17}.

В связи с конечными разрешимыми группами хочется упомянуть теорему Бернсайда:

Теорема
Пусть $|G| = p^a q^b$, где p, q - простые числа. Тогда G разрешима.

Эта теорема тоже очень сильная и не является частным случаем теоремы Фейта-Томпсона, потому что одно из простых чисел в формулировке может быть равно 2. В частности из этой теоремы вытекает, что порядок простой конечной группы должен содержать как минимум 3 различных простых делителя. В учебных задачах пользоваться этими теоремами неправильно - так как они сложные, а задачи нужны для того, чтобы отработать базовые навыки (да и вообще я придерживаюсь концепции, что можно использовать лишь те теоремы, доказательство которых вы знаете хотя бы на уровне идей). Мы с вами разберем несколько довольно сильных методов проверки группы на разрешимость в главе, посвященной силовским подгруппам.

*Возвращаясь к нормальным рядам скажу, что в теории групп является популярной следующая концепция: назовем групп G поли***, если существует нормальный ряд:*

$$\{e\} = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$$

*такой что факторы H_{i+1}/H_i являются группами из класса ***, в роли этих звездочек можно подставить практически что угодно: к примеру если ряд такой, что H_{i+1}/H_i циклические - то группа G называется поли-циклической, если факторы свободные группы - то группа называется поли-свободной. При таком подходе разрешимые группы можно назвать поли-абелевыми. Бывает, что этот подход не дает ничего интересного, к примеру поли-конечные группы являются конечными, или легко понять, что поли-разрешимые группы являются разрешимыми. Советую подумать над описанием класса поли-нильпотентных групп.*

Также никто не запрещает быть нормальным рядам бесконечными, что открывает дорогу к существенным обобщениям понятий нильпотентности и

разрешимости. К пример, можно на бесконечности определить:

$$Z_\infty = \bigcup_n Z_n(G)$$

$$G_{(\infty)} = \bigcap_n G_{(n)}$$

$$G^{(\infty)} = \bigcap_n G^{(n)}$$

Группы, для которых $G^{(\infty)} = \{e\}$ состоят в точности из так называемых остаточно разрешимых (то есть групп, для любого нетривиального элемента в которых найдется гомоморфизм в разрешимую группу, переводящий этот элемент не в 1, иными словами это группы, для которых гомоморфизмы в разрешимые группы разделяют элементы), группы, для которых $G_{(\infty)} = \{e\}$ состоят в точности из остаточно нильпотентных. Кстати, замечу, что в случае бесконечного индекса подходы через верхний и нижний центральный ряд приводят уже к разным понятиям, и равенство $Z_\infty(G) = G$ не эквивалентно остаточной нильпотентности: чтобы это понять нужно рассмотреть некоторые нильпотентные группы G_n ступени n и взять группу:

$$G = \prod_n G_n$$

Из-за того, что G это прямое произведение нильпотентных - сама она будет остаточно нильпотентной, но при этом $G \neq Z_\infty(G)$, к примеру, если рассмотреть $x_n \in Z_n(G_n) \backslash Z_{n-1}(G_n)$, то $x = (x_1, x_2, \ldots) \notin Z_\infty(G)$. С одной стороны эти обобщения во многом сохраняют свойства своих прототипов, но с другой стороны они начинают покрывать качественно более содержательные и интересные примеры: к примеру, свободная группа $\mathbb{F}_2$ не является разрешимой, но является остаточно разрешимой: ее последовательные коммутанты за конечное число итераций не тривиализуются, но пересечение все же тривиальное; и все эти конструкции очень важные для теории групп.

Вы не поверите, но можно пойти даже дальше бесконечности, и по трансфинитной индукции определить все эти ряды для произвольного ординала α, для примера производного ряда:

$$G^{(\alpha+1)} = [G^{(\alpha)}, G^{(\alpha)}] \qquad \text{для непредельного } \alpha$$

$$G^{(\alpha)} = \bigcap_{\beta<\alpha} G^{(\beta)} \qquad \text{для предельного } \alpha$$

иными словами для непредельных ординалов обычная рекуррентная формула, а когда доходим до предельного ординала - берем пересечение всего скопившегося до этого. Напомню, что ординалы имеют более тонкую структуру чем кардиналы (кардинал - это мощность ординала), с которыми мы обычно работаем и которые отвечают за мощность, первые ординалы выглядят так:

$$\{1, 2, 3, \ldots, \omega, \omega+1, \omega+2, \omega+3, \ldots, 2\omega, 2\omega+1, \ldots\}$$

Хотя с точки зрения мощности и ω, и $\omega+1$ отвечают счетному множеству - но на уровне ординалов они различны. И оказывается, что существуют группы,

для которых, к примеру, $G^{(\omega+1)} \neq G^{(\omega)}$ (возможно, может показаться, что в этом нет ничего удивительного, что некоторая группа не совпадает со своим коммутантом, но по построению $G^{(\omega)}$ - это бесконечное пересечение коммутантов, и обманчиво может показаться, что такая конструкция дает группу, не меняющуюся при взятии нового коммутанта; честно признаюсь, что я долгое время ошибочно думал, что уже на первой бесконечности ω производный ряд обязан стабилизироваться). Из соображений мощности для каждой группы найдется ординал α, что $G^{(\alpha)} = G^{(\alpha+1)}$ (а значит после этого ординала этот производный ряд стабилизируется, причем этот ординал легко оценить: до тех пор пока мы не придем к стабилизации производного ряда - на каждом шаге теряется минимум один элемент группы, а всего их $|G|$, поэтому кардинал ординала α не будет превосходить $|G|$). Такое α, что $G^{(\alpha)} = G^{(\alpha+1)}$, называют трансфинитной длиной производного ряда. По аналогии можно определить трансфинитные члены рядов и их длины для оставшихся рядов. То, что там ничего не тривиализуется и на бесконечности разрастается красивая и интересная теория, очень хорошо иллюстрирует следующая теорема:

Теорема (Мальцев)
Для любого ординала α существует группа G с трансфинитной длиной производного ряда равной α.

Аналогичные результаты верны и для оставшихся двух рядов. Если для некоторого ординала α выполнено $Z_\alpha(G) = G$ (соответственно $G_{(\alpha)} = \{e\}$ или $G^{(\alpha)} = \{e\}$), то группа G называется гиперцентральной, трансфинитно-нильпотентной и трансфинитно-разрешимой соответственно.

Гулять так гулять: хочется сказать еще об одной плодотворном направлении обобщения: для любой группы G рассмотрим:

$$FC(G) = \{g \in G; |[g]| < \infty\} \lhd G$$

то, что это подгруппа проверяется довольно просто из равенства: $g^{-1}(h_1h_2)g = (g^{-1}h_1g)(g^{-1}h_2g)$, откуда получаем $[h_1h_2] \subset [h_1][h_2]$, поэтому класс сопряженности произведения будет содержаться в произведении классов сопряженности сомножителей, и если те конечны, то и класс сопряженности произведения h_1h_2 тоже будет конечным. Также очевидно, что $[h^{-1}] = [h]^{-1}$, поэтому $FC(G)$ замкнута относительно взятия обратного, нормальность $FC(G)$ совсем очевидна. Такое обозначение от английского finite conjugacy. Группа G называется FC-группой, если $G = FC(G)$, то есть это группы, каждый класс сопряженности которых конечен, что является очень ярким и интересным обобщением абелевых групп, где каждый класс сопряженности состоит из одного элемента, а в общем случае подгруппа $FC(G)$ является обобщением центра группы $Z(G)$, который опять-таки состоит из элементов, класс сопряженности которых состоит из одного элемента. Так как нильпотентные группы во многом строились вокруг центра: фактически они определялись через ряды, фактор последовательных членов которого равен центру некоторой группы, то это определение можно обобщить, заменив центр на FC, и получить следующий

определяющийся индуктивно ряд:

$$F_1(G) = FC(G)$$

$$F_{n+1}(G)/F_n(G) = FC(G/F_n(G))$$

$$F_\infty(G) = \bigcup_n F_n(G) = FCH(G)$$

рекуррентное равенство можно также более строго переписать как $F_{n+1}(G) = \pi_n^{-1}(G/F_n(G))$, *где* $\pi_n : G \to G/F_n(G)$ *канонический эпиморфизм. И группа называется FC-гиперцентральной, если* $FCH(G) = G$. *И опять-таки, с одной стороны эти группы по свойствам и методам работы напоминают обычные нильпотентные группы, но с другой стороны это понятие существенно обобщает понятие не только нильпотентных, но даже* ω*-гиперцентральных групп, так как* $Z_n(G) < FC_n(G)$, *а потому* $Z_\infty(G) < FCH(G)$, *а значит* ω*-гиперцентральная группа является FC-гиперцентральной, но к примеру если* A_5 *совсем не нильпотентна, даже не гиперцентральная, потому что у нее тривиальный центр, а потому* $Z_n(A_5) = \{e\}$ *для любых n (у любой нетривиальной нильпотентной группы нетривиальный центр: в подходе через* $Z_n(G)$ *это очевидно, а через* $G_{(n)}$ *легко доказывается: если n ступень нильпотентности, то используя* $\{e\} = G_{(n)} = [G_{(n-1)}, G]$ *мы для любого* $x \in G_{(n-1)}$ *и для любого* $y \in G$ *получаем* $[x, y] = e$, *иными словами* $x \in Z(G)$*). Но при этом* A_5 *очевидно является FC-группой, так как она конечна, а потому и любой ее класс сопряженности конечен, а значит* $FC(A_5) = A_5$, *то есть не понадобилось уходить даже дальше первого члена. Замечу, что и здесь можно рассматривать трансфинитную версию этой теории: определить ряд* $F_\alpha(G)$ *для произвольного ординала* α *и назвать группу FC-*α*-гиперцентральной, если* $F_\alpha(G) = G$. *Очевидно, что* α*-гиперцентральная группа будет FC-*α*-гиперцентральной. FC-гиперцентральные группы особенно популярны в разделах, сильно связанных с сопряжениями: например при анализе дифференцирований или следов на групповых алгебрах, потому что, к примеру, тот же след инвариантен относительно взятия сопряжения: а значит след на групповой алгебре - это фактически произвольная функция на множестве классов сопряженности. Для пополненных групповых алгебр часто бывает очень актуальным замечание, что если у вас конечный класс сопряженности - то вы сможете избегать сложностей, возникающих при необходимости работать с бесконечными суммами, потому что они всегда будут конечными, к примеру: всегда можно усреднить функцию по классу сопряженности безо всяких погружений в меры и бесконечные суммы простым взятием среднего арифметического. Творческое задание - подумайте над свойствами FCH-групп: уважается ли этими группами прямое произведение, фактор, взятие подгруппы, какие вы сможете построить интересные примеры FCH-групп?*

Свободные группы

Свободной группой $\mathbb{F}_n$ называется множество приведенных слов (где нет подряд идущих букв b и b^{-1}) в алфавите $A = \{a_1, a_1^{-1}, a_2, a_2^{-1}, \ldots, a_n, a_n^{-1}\}$. Умножение двух слов задается по формуле: $\omega_1 \cdot \omega_2 =$ приведение$(\omega_1\omega_2)$, где операция приведения сокращает до победного конца все фрагменты вида bb^{-1}, например:

$$(ab^2a^{-3}) \cdot (a^3b^{-2}a^2b) = a^3b$$

Нейтральным элементом служит пустое слово. Обратный элемент задается формулой:

$$(x_1x_2 \ldots x_k)^{-1} = x_k^{-1} \ldots x_2^{-1}x_1^{-1}$$

где $x_i \in A$. Можно сказать, что $\mathbb{F}_n$ - это группа, порожденная $\{a_1, \ldots, a_n\}$, не удовлетворяющие никаким нетривиальным соотношениям. Свободные группы определяются и для бесконечных n, в экзотических случаях используют свободные группы даже с несчетным n. Свободная группа ранга один изоморфна $\mathbb{F}_1 \cong \mathbb{Z}$.

Важной характеристикой произвольного слова $\omega = a_{i_1}^{k_1}a_{i_2}^{k_2} \ldots$ является его длина, определяемая формулой $|\omega| = |k_1| + |k_2| + \ldots$

Основной прием работы со свободными группами - это универсальное свойство: пусть дана произвольная группа G с элементами $b_1, \ldots, b_n$, тогда отображение $a_i \mapsto b_i$ продолжается до корректного гомоморфизма

$$\mathbb{F}_n \to G$$

Иными словами, *ИЗ свободной группы легко строить гомоморфизмы.*

Также нужно знать о теореме Нильсена-Шрайера, утверждающей что подгруппа любой свободной группы сама свободная, более того: если $H < \mathbb{F}_n$, причем если также $e = [\mathbb{F}_n : H] < \infty$ и $n < \infty$, то $H \cong \mathbb{F}_{1+e(n-1)}$ (например в случае $e = 1$ мы получаем, что ранг подгруппы совпадает с рангом группы, как и должно быть). Доказательство даже того, что подгруппа свободна (не говоря уже о вычислении ранга) нетривиально; хотя и интуитивно понятно, что в раз в группе не было соотношений, то откуда им взяться в подгруппе? Для бесконечных рангов или индексов теорема не работает: например, в случае $\mathbb{F}_2 < \mathbb{F}_\infty$ индекс подгруппы бесконечен, но ранг подгруппы равен 2. Также если рассмотреть стандартный пример вложения $\mathbb{F}_\infty < \mathbb{F}_2$ бесконечного индекса и каноническое вложение $\mathbb{F}_n < \mathbb{F}_\infty$, то получим:

$$\mathbb{F}_n < \mathbb{F}_\infty < \mathbb{F}_2$$

иными словами в $\mathbb{F}_2$ есть свободные подгруппы бесконечного индекса как *конечного* так и *бесконечного* ранга.

Задача

Доказать, что $\mathrm{ord}(\omega) = \infty$ *для нетривиального* $\omega \in \mathbb{F}_n$.

Воспользуемся здесь следующей хитростью: для каждого слова ω в некоторых задачах удобно работать не просто с приведенной его формой (когда нет сокращений вида bb^{-1} внутри слова), а с *циклически приведенной формой*, по определению равной результату обычного приведения, но только если слово ω мы рассматриваем как циклическое слово, записанное вдоль окружности, то есть слово, после последней буквы которого вновь идет первая буква и все зацикливается. Более формально: если слово имеет вид $\omega = yxy^{-1}$ для некоторого $y \in A$, то операцией циклического приведения назовем сопряжение на y, а именно $\omega \mapsto y^{-1}\omega y = x$. И циклически приведенная форма - это результат применения этих операций до тех пор, пока это возможно. К примеру:

$$aba^4b^{-2}a^{-1} \mapsto ba^4b^{-2} \mapsto a^4b^{-1}$$

то есть a^4b^{-1} есть результат циклического приведения слова $aba^4b^{-2}a^{-1}$. Полученное слово уже не обязано равняться ω в группе, но оно все равно будет лежать в классе сопряженности $[\omega]$, так как получается из исходного многократными сопряжениями, но часто этого бывает достаточно.

Вернемся к задаче: пусть $\mathrm{ord}(\omega) = m < \infty$, и вместе с приведенной формой ω (где внутри слова нет сокращений) рассмотрим его циклическое приведение ω_0. Так как $\omega_0 \in [\omega]$, то и $\mathrm{ord}(\omega_0) = m$. Таким образом $\omega_0^m = e$, но так как внутри ω_0 нет сокращений (потому что их не было в ω), то сокращения могут возникнуть лишь на стыке слов в произведении ω_0^m. Значит $\omega_0 = bxb^{-1}$ для некоторой буквы $b \in A$, и мы приходим к противоречию с циклической приведенностью.

Задача

Пусть $u, v \in \mathbb{F}_n$ *- некоторые коммутирующие слова. Доказать, что они лежат в общей циклической подгруппе.*

Стандартное решение этой задачи состоит в хардкорном анализе слов и букв. Но можно схитрить и воспользоваться теоремой Нильсена-Шрайера: подгруппа $\langle u, v\rangle$ является свободной, а так как она абелева, то изоморфна $\mathbb{Z}$.

Утверждение

Пусть $n \neq m$. *Докажите, что* $\mathbb{F}_n \ncong \mathbb{F}_m$.

Разделяющим инвариантом в данном случае служит количество гомоморфизмов в двух-элементную группу $\#\{\pi : \mathbb{F}_n \to \mathbb{Z}_2\}$. Каждая порождающая буква может отправиться либо в 0, либо в 1, всего 2^n вариантов. По свойству универсальности если задать отображение на порождающих - то оно корректно продолжится до гомоморфизма свободной группы, поэтому гомоморфизмов $\mathbb{F}_n \to \mathbb{Z}_2$ тоже в точности 2^n.

Утверждение

Доказать, что $\mathbb{F}_\infty < \mathbb{F}_2$.

То, что свободные группы с бóльшим рангом вкладываются в свободные группы с меньшим рангом, не должно казаться удивительным, так как такое поведение в теории групп на самом деле типично.

Пусть $\mathbb{F}_\infty = \langle x_1, x_2, \ldots \rangle$, $\mathbb{F}_2 = \langle a, b \rangle$. Зададим вложение на порождающих:

$$x_i \mapsto b^{-i} a b^i$$

По свойству универсальности оно продолжается до гомоморфизма. Докажем его инъективность. Рассмотрим нетривиальное приведенное слово $\omega = x_{i_1}^{k_1} x_{i_2}^{k_2} \ldots$. Тогда:

$$\omega \mapsto b^{-i_1} a^{k_1} b^{i_1} b^{-i_2} a^{k_2} b^{i_2} \ldots$$

Так как ω - приведенное, то $i_1 \neq i_2$, $i_2 \neq i_3$ и т.д. то есть "стыкующиеся" степени b не могут полностью сократиться и распространить "вирус сокращения" до a^{k_1} и a^{k_2}. Таким образом образ ω будет нетривиален и построенный гомоморфизм инъективен.

Что касается важнейших структурных подгрупп, то нетрудно понять, что $Z(\mathbb{F}_n) = \{e\}$ при $n \geq 2$. Описание коммутанта чуть сложнее:

Задача

Доказать, что $[\mathbb{F}_n, \mathbb{F}_n] = \{\omega \in \mathbb{F}_n : \text{сумма степеней при каждой букве} = 0\}$.

Обозначим через $H = \{\omega \in \mathbb{F}_n : \text{сумма степеней при каждой букве} = 0\}$. Так как в любом коммутаторе сумма степеней при каждой букве равна 0 и это условие сохраняется при произведении, то $[\mathbb{F}_n, \mathbb{F}_n] < H$. С другой стороны для произвольного $\omega \in H$ мы можем многократно использовать тождество $xy = [x, y]yx$, чтобы с точностью до коммутатора сгруппировать каждую букву в одном мономе, а именно привести слово к следующему виду:

$$\omega = [*, *] \ldots [*, *] x_1^{N_1} \ldots x_n^{N_n}$$

Этот процесс чем-то напоминает применение "мясорубочного тождества", проиллюстрирую как это работает на конкретном примере: здесь, мы пытаемся утащить все b максимально вправо, но при этом, чтобы все коммутаторы были слева:

$$a^2 b a^3 b^2 a = [a^2 b, a^3] a^3 a^2 b b^2 a = [a^2 b, a^3] a^5 b^3 a = [a^2 b, a^3][a^5 b^3, a] a^6 b^3$$

Но с учетом того, что сумма степеней при таких преобразованиях при каждой букве сохраняется, получаем $N_i = 0$, а значит $\omega = [*, *] \ldots [*, *]$, т.е. $H < [\mathbb{F}_n, \mathbb{F}_n]$. Таким образом $H = [\mathbb{F}_n, \mathbb{F}_n]$. Замечу, что в рассуждениях мы нигде не пользовались тем, что $n \geq 2$, а потому утверждение верно и для $\mathbb{F}_1 = \mathbb{Z}$.

Замечание:

По теореме Нильсена-Шрайера H должна быть свободной (на самом деле $[\mathbb{F}_n, \mathbb{F}_n] \cong \mathbb{F}_\infty$ хотя из-за того, что индекс бесконечен из формулы Нильсена-Шрайера сам ранг найти нельзя).

Также отмечу, что свободная группа $\mathbb{F}_n$ не является разрешимой группой (как при бесконечном, так и конечном $n \geq 2$): так как довольно легко предъявить

два некоммутирующих элемента из коммутанта, а значит $[\mathbb{F}_n, \mathbb{F}_n]$ является свободной неабелевой, в свою очередь уже ее коммутант снова является свободным неабелевым: и так далее до бесконечности. Иными словами легко понять, что $(\mathbb{F}_n)^{(k)}$ является неабелевой свободной группой для любого k, а значит коммутант никогда не может обнулиться. Однако все равно ситуация с разрешимостью не является безнадежной, и свободные группы являются остаточно-разрешимыми, в том смысле, что для них $\bigcap_{n=1}^{\infty} G^{(n)} = \{e\}$. Остаточно-разрешимых группы мы вскользь коснемся в конце методички.

Абеленизация: $\mathbb{F}_n/[\mathbb{F}_n, \mathbb{F}_n] \cong \mathbb{Z}^n$. Доказать эту изоморфность можно многими способами, проще всего это сделать через копредставления:

$$\mathbb{F}_n/[\mathbb{F}_n, \mathbb{F}_n] \cong \langle x_1, x_2, \ldots, x_n | \, [x_i, x_j] = 1 \text{ для всех } i, j \rangle \cong \mathbb{Z}^n$$

Но можно рассуждать и так: рассмотрим гомоморфизм $\alpha : \mathbb{F}_n \to \mathbb{Z}^n$, такой что:

$$\omega \mapsto (\text{сумма степеней при } x_1, \quad \ldots \quad , \text{сумма степеней при } x_n)$$

По теореме о гомоморфизме $\mathbb{Z}^n \cong \mathbb{F}_n / \ker \alpha$, но при этом из предыдущей задачи мы знаем, что $\ker \alpha = [\mathbb{F}_n, \mathbb{F}_n]$. Абеленизация - это второй стандартный способ доказательства $\mathbb{F}_n \ncong \mathbb{F}_m$ при $n \neq m$.

Для доказательства, что некоторая группа является свободной, чаще всего пользуются Леммой о пинг-понге:

Лемма (о пинг-понге)
Дано действие группы $G \curvearrowright \Omega$, два непересекающиеся подмножества $X, Y \subset \Omega$ и $a, b \in G$. Если для любого $k \neq 0$ выполнено $a^k(X) \subset Y$ и $b^k(Y) \subset X$, то $\langle a, b \rangle \cong \mathbb{F}_2$.

Предположим противное: что существует нетривиальное $\omega = a^{k_1} b^{m_1} \ldots b^{m_p} = e$ в группе G. Переходя от ω к $b^{-N} \omega b^N$ при достаточно большом N можно считать, что $b^{-N} \omega b^N$ как приведенное слово начинается и заканчивается с некоторой степени b (приведение - это сокращение всевозможных xx^{-1}, и важно рассматривать именно слова, так как $b^{-N} \omega b^N = e$ как элемент группы G; для элементов произвольной группы вообще нет такого понятия "элемент начинается с b"). И теперь если $b^{-N} \omega b^N$ рассмотреть как элемент группы G, тогда для него мы получим:

$$b^{-N} \omega b^N (Y) \subset X$$

(отсюда и такое название леммы: степени a и b словно играют в пинг-понг, перебрасывая мяч друг другу от X к Y и обратно), что из непересекаемости X, Y противоречит $\omega = e$. Таким образом между a и b нет никаких соотношений, а потому $\langle a, b \rangle \cong \mathbb{F}_2$. Есть версия этой леммы и для $\mathbb{F}_n$.

Чтобы понимать насколько это сильный и фактически безальтернативный способ проверки того, что группа является свободной - расскажу историю из свой жизни: однажды у меня возникла задача из теории групп, где нужно было проверить, что какая-то очень сложная и хитрая группа является свободной. И я очень долго описывал и ситуацию, и саму группу своей коллеге, после чего она сказала: "я не очень поняла, что это за группа, но ты лемму о пинг-понге не пробовал?" И я

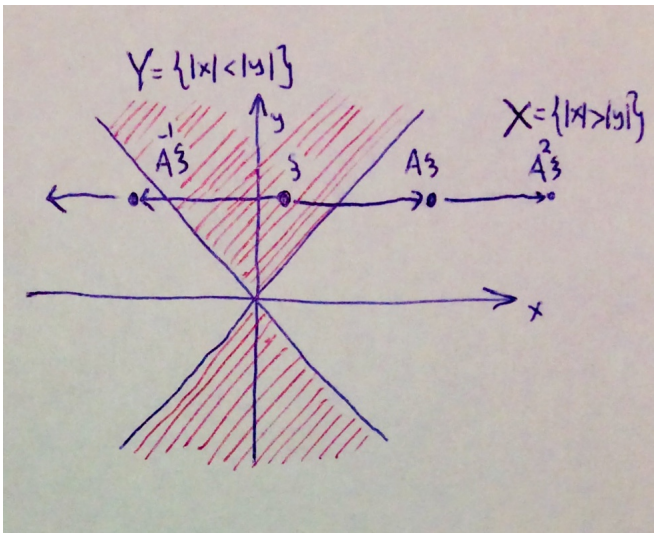
полностью разделяю ее точку зрения: если и есть какие-то способы проверки, что группа является свободной, кроме леммы о пинг-понге, то скорее всего через нее они сами и доказываются.

Задача

Доказать, что $\left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle \cong \mathbb{F}_2$.

Это классический пример применения леммы о пинг-понге.

Обозначим $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. Матрицы как в линале действуют умножением на $\mathbb{R}^2$. Рассмотрим $X = \left\{ \begin{pmatrix} x \\ y \end{pmatrix}; |x| > |y| \right\}$, $Y = \left\{ \begin{pmatrix} x \\ y \end{pmatrix}; |x| < |y| \right\}$. Непосредственно проверяется, что $A^k(Y) \subset X$ и $B^k(X) \subset Y$ для $k \neq 0$. В этом легко убедиться, проверим, например, первое вложение: ясно, что $A^k \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 2ky \\ 0 \end{pmatrix}$, иными словами A^k сдвигает точку параллельно оси O_x на $\pm 2k|y|$, но так как $|y| > |x|$, то сдвиг достаточно большой, чтобы выбросить точку из красной области:



Таким образом по лемме о пинг-понге получаем, что $\langle A, B \rangle \cong \mathbb{F}_2$.

Замечание:

Эту задачу можно сделать на порядок более сложной и содержательной, если спросить, при каких $\lambda \in \mathbb{C}$ *верно:*

$$G_\lambda = \left\langle \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \right\rangle \cong \mathbb{F}_2$$

К примеру, И.Н. Санов доказал, что при $|\lambda| \geq 2$ *выполняется* $G_\lambda \cong \mathbb{F}_2$ *(а потому эти матрицы принято называть матрицами Санова), также при* $\lambda = 1$ *группа не является свободной, и на матрицы Санова с таким параметром довольно легко можно записать соотношение, что оставляется читателю в качестве простого, но очень полезного упражнения. В общем же случае ситуация очень сложная: к примеру для трансцендентного* λ *группа* G_λ *свободная (понять появление здесь трансцендентных чисел можно: так как если матрицы удовлетворяют некоторому соотношению - то матричные коэффициенты соответствующего*

произведения матриц Санова являются многочленами от λ - и если произведение тривиально - это дает 4 некоторых полиномиальных уравнений на λ, правда, возможно вырожденных вроде 1=1), а значит множество λ, для которых G_λ свободная - плотно в $\mathbb{C}$; с другой стороны множество λ в единичном круге, для которых G_λ уже не является свободной, тоже будет плотным.

==========

Группы, заданные копредставлением

По определению $G = \langle a_1, \ldots, a_n | R_1, R_2, \ldots \rangle := \mathbb{F}_n / N$, где $N = \langle\langle R_1, R_2, \ldots \rangle\rangle$ - нормальное замыкание соотношений. Неформально: это группа всевозможных слов, в которых помимо тривиальных соотношений $bb^{-1} = e$ можно сокращать "с помощью" R_i. Эта конструкция работает без изменений для бесконечного n. Замечу, что для $\omega \in \mathbb{F}_n$ верно $\omega = e$ в G iff $\omega = (x_1 R_{i_1} x_1^{-1})(x_2 R_{i_2} x_2^{-1}) \ldots$, что непосредственно вытекает из определения нормального замыкания. Когда пишете слово ω - задумывайтесь с элементом из $\mathbb{F}_n$ или $G = \mathbb{F}_n / N$ в данный момент вы работаете. Ясно, что $\langle a_1, \ldots, a_n | \emptyset \rangle \cong \mathbb{F}_n$.

Основная связанная с копредставлениями теорема - это универсальное свойство:

Пусть $G = \langle a_1, \ldots, a_n | R_1, R_2, \ldots \rangle$ и $b_1, \ldots, b_n \in H$ - некоторые элементы в некоторой группе H, удовлетворяющие соотношениям R_i. Тогда отображение $a_i \mapsto b_i$ продолжаются до корректного гомоморфизма $G \to H$.

Техника работы с группами, заданными копредставлением:

• Хороший вид слов + соображения мощности. Иногда (довольно редко) с использованием соотношений можно произвольное слово свести к хорошему и удобному для работы виду (типичный пример - это $a^n b^k$, обычно такой вид возможен, когда в группе есть соотношения, позволяющие запускать некоторый аналог "мясорубочного процесса") - в таком случае легко вычислять центры/коммутаторы и прочие характеристики группы, писать ограничения на порядок группы и т.д. Соображение мощности для конечных групп вопрос биективности часто сводят лишь к вопросу сюръективности или инъективности.

• Универсальное свойство позволяет строить гомоморфизмы *ИЗ группы, заданной копредставлением.* Обычно это удобно, если мы

1) Строим изоморфизм между двумя заданными копредставлениями группами,

2) Пытаемся доказать нетривиальность некоторого элемента (или даже группы в целом). В таком случае удобно построить некоторый гомоморфизм, чтобы образ этого элемента был нетривиален - тогда и сам элемент будет нетривиален. Обычно соотношения бывают очень запутанными, а с нормальными замыканиями сложно работать - поэтому в словесном контексте такие вопросы почти невозможно решить. Поясню, в чем основная сложность прямого подхода через слова: пусть у вас есть условно группа $G = \langle a, b | a^2 = b^2 = 1 \rangle$, и вы хотите доказать, что $a \neq 1$, но для этого вам нужно убедиться, что $a \neq (x_1^{-1} R_{i_1} x_1)(x_2^{-1} R_{i_2} x_2) \dots$ как элемент свободной группы $\mathbb{F}_2$, где R_i это либо a^2, либо b^2. Можно попытаться ухватиться за то, что справа есть квадраты, а слева их нет, но в слове справа между скобками могут быть сокращения, которые могут распространиться до квадратов. Скажем R_{i_2} может сократиться частично за счет первого, а частично за счет третьего блоков. Там может происходить самый настоящий кошмар, поэтому всегда стараются искать пути либо к хорошим свойствам группы, либо к универсальному свойству для гомоморфизмов.

Пример

Доказать, что $D_n = \langle a, b | ab = ba^{-1}, a^n = b^2 = e \rangle$.

Рассмотрим $G = \langle a, b | ab = ba^{-1}, a^n = b^2 = e \rangle$. Используя соотношение $ab = ba^{-1}$ и вытекающее из него $a^{-1}b = ba$ вы можете любое слово ω привести к виду $b^k a^m$ (нужны оба соотношения, так как первое может направо переносить только неотрицательные степени a). С учетом ограничения на порядок получаем, что $|G| \leq 2n$. Так как поворот и симметрия из группы Диэдра удовлетворяют соотношениям из копредставления группы G, то используя универсальное свойство можем построить гомоморфизм $\pi : G \to D_n$, такой, что a переходит в поворот группы Диэдра, а b в симметрию группы Диэдра. Так как поворот и симметрия порождает группу Диэдра, то π - эпиморфизм. Используя соображения мощности, получаем, что π - изоморфизм.

Утверждение

Доказать, что каждая группа G задается некоторым копредставлением.

Для технического удобства будем работать со счетной группой $G = \{e, g_1, g_2, \dots\}$. Тогда рассмотрим

$$H = \langle g_1, g_2, \dots | g_i g_j = g_{p(i,j)} \rangle$$

у которой в качестве порождающих берутся все нетривиальные элементы G, а в качестве соотношений - вся таблица умножения. Здесь тоже есть удобная форма для всякого элемента: так как произведение любых двух элементов группы G можно, используя таблицу умножения, заменить на один элемент, то $\omega = g_{i_1} g_{i_2} \dots = g_i$.

Используя универсальное свойство можно построить гомоморфизм $\pi : H \to G$, $g_i \mapsto g_i$. Он будет сюръективным (потому что образ даже порождающих и e дает все G). Он будет инъективным, так как с использованием упомянутой удобной формы получаем: если $\omega \neq e$, то $\omega = g_i$ для некоторого i, тогда $\pi(\omega) = \pi(g_i) = g_i \neq e$. Таким образом $H \cong G$.

Пример

Доказать, что $\langle x, y | x^2 = y^3 \rangle \cong \langle a, b | aba = bab \rangle$ (эта группа играет большую роль в топологии узлов и называется группой трилистника: она совпадает с фундаментальной группой дополнения трилистника в $\mathbb{R}^3$).

Короткое доказательство Рассмотрим "замену переменных" $x = ab^2, y = ab$, проверяется, что при такой "замене" первое копредставление переходит во второе (т.е. единственное соотношение первой группы превратится в соотношение второй) - значит группы изоморфны. Чтобы додуматься до этой замены нужно было заметить, что из $bababa = babbab$, сопряжением на b вытекает $ababab = abbabb$, т.е. $(ab)^3 = (abb)^2$. Также нужно проверить, что это настоящая "замена переменных", то есть что через x, y выражаются a и b.

Максимально аккуратное доказательство Фактически- это дотошное обоснование "замены переменных", идейно здесь нет ничего нового. Пусть $G = \langle x, y | x^2 = y^3 \rangle$, $H = \langle a, b | aba = bab \rangle$. Используя универсальное свойство строим гомоморфизм $\alpha : G \to H$, $x \mapsto ab^2, y \mapsto ab$, так как единственное соотношение переходит в:

$$x^2y^{-3} \mapsto abbabbb^{-1}a^{-1}b^{-1}a^{-1}b^{-1}a^{-1} = ababaa^{-1}b^{-1}a^{-1}b^{-1}a^{-1} = e$$

Аналогично используя универсальное свойство можно построить гомоморфизм $\beta : H \to G$, $a \to yx^{-1}y, b \mapsto y^{-1}x$. Непосредственно проверяется, что $\alpha \circ \beta = \mathrm{id}$ и $\beta \circ \alpha = \mathrm{id}$. Значит группы изоморфны.

Есть теорема Титце, утверждающая, что два копредставления задают одну и ту же группу, когда из одного можно получить другое с помощью довольно естественных преобразований Титце. Правда, увы, этот процесс неалгоритмичен.

Пример

Доказать, что в группе Баумслага-Солитера $B(2,3) = \langle a, b | b^{-1}a^2b = a^3 \rangle$ *коммутатор* $[a,b] \neq e$ *(в частности группа неабелева).*

Замечу, что у этой группы нет хорошей общей формы для произвольного слова. Чтобы "отделить" элемент от единицы обычно строят гомоморфизм в несложную, но довольно богатую группу, где образ тестового элемента будет отличен от e. Несложная - чтобы было легко работать, богатая - чтобы легко было элементы от e отделять. Обычно в роли такой группы берут либо группу перестановок S_n, либо матричную группу $GL_n(F)$. Гомоморфизмы в матричную группу обычно называют *представлениями группы* (не путайте с копредставлениями).

Построим "разделяющий" гомоморфизм двумя способами:

• Матричный способ. Обычно, если есть соотношение на сопряженность степеней a - то a отправляют в диагональную матрицу, а b - в матрицу сдвига (перемешивания базисных векторов).

$$a \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & \omega^2 & 0 & 0 \\ 0 & 0 & 0 & \omega^3 & 0 \\ 0 & 0 & 0 & 0 & \omega^4 \end{pmatrix}$$

$$b \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

где $\omega = e^{\frac{2\pi}{5}}$ (5 взяли, потому что 5 взаимно просто с 3, а потому a^2 и a^3 имеют те же собственные значения), убедитесь, что эти матрицы удовлетворяют соотношению $b^{-1}a^2b = a^3$, тогда по свойству универсальности это отображение можно продолжить до гомоморфизма $\pi : B(2,3) \to GL_5(\mathbb{C})$. Перемножив матрицы, убедитесь, что $\pi([a,b]) \neq e$, значит $[a,b] \neq e$.

• Перестановочный метод. Рассмотрим

$$a \mapsto (12345)$$

$$b \mapsto (34)(25)$$

Убедитесь, что эти перестановки удовлетворяют соотношению Баумсалага-Солитера, тогда по универсальному свойству получаем гомоморфизм $\pi : B(2,3) \to S_5$, также убеждаемся, что $\pi([a,b]) \neq e$.

Замечание:

Есть еще один очень эффективный и простой способ, однако сильно теоретически перегруженный, которого мы коснемся в конце методички: представить группу Баумслага-Солитера в виде HNN-расширения и применить лемму Бриттона.

Задача

Докажите, что группа $\mathcal{B} = \langle a, b | a^{a^b} = a^2 \rangle$ не является разрешимой.

Группу $\mathcal{B}$ иногда называют *группой Баумслага*, и она является своего рода мега-версией групп Баумслага-Солитера, всплывая примерно в тех же сюжетах что и они, но являясь намного более богатым источником для самого разного рода контрпримеров. Через $a^b := b^{-1}ab$ иногда обозначают сопряжение, когда хотят большей лаконичности в формулах, т.е. подробно соотношение группы $\mathcal{B}$ записывается как $(b^{-1}ab)^{-1}a(b^{-1}ab) = a^2$. Докажем по индукции, что $a \in \mathcal{B}^{(n)}$. База индукции очевидна, так как $a \in \mathcal{B}^{(0)} = \mathcal{B}$. Шаг индукции: пусть $a \in \mathcal{B}^{(n)}$, тогда $b^{-1}ab \in \mathcal{B}^{(n)}$; и из группового соотношения получаем:

$$a = (b^{-1}ab)^{-1}a(b^{-1}ab)a^{-1} = [b^{-1}a^{-1}b, a] \in [\mathcal{B}^{(n)}, \mathcal{B}^{(n)}] = \mathcal{B}^{(n+1)}$$

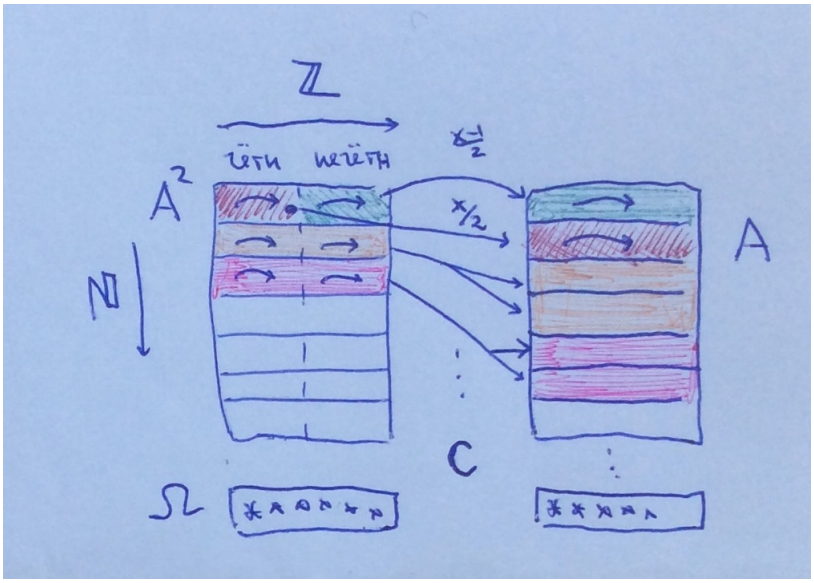
Доказательство, что $a \neq e$ сложнее, чем в предыдущих случаях, сложность с поиском гомоморфизма заключается в том, что a должно быть сопряжено не только a^2, но и сопрягающему элементу. Рассмотрим группу $S((\mathbb{Z} \times \mathbb{N}) \sqcup \Omega)$ для некоторого фиксированного бесконечного множества Ω (пусть для определенности оно будет счетным, но это не существенно); и рассмотрим перестановку A, определенную формулой $A(n, m) = (n + 1, m)$ на $\mathbb{Z} \times \mathbb{N}$ и тождественную на Ω; фактически A каждую точку не из Ω сдвигает по горизонтали (то есть вдоль строчек). Легко понять, что циклический тип A состоит из бесконечного числа циклов бесконечной длины (соответствующих точкам $\mathbb{Z} \times \mathbb{N}$) и бесконечного числа циклов длины 1 (соответствующих точкам Ω), а в A^2 каждый независимый бесконечный цикл A разбивается на два бесконечных цикла (A^2 в каждой строчке сдвигает числа на 2, а потому один цикл - это сдвиг четных чисел, а второй цикл - сдвиг нечетных чисел), циклы длины 1 остаются такими же. Так как циклические типы A и A^2 совпадает - то они сопряжены, сопрягающая перестановка строится по тем же правилам и принципам, что и в конечном случае, мы рассмотрим сопрягающую перестановку $C \in S((\mathbb{Z} \times \mathbb{N}) \sqcup \Omega)$, заданную формулой:

$$C(x) = \begin{cases} \left(\frac{i}{2}, 2j\right) & , \text{ если } x = (i, j) \in \mathbb{Z} \times \mathbb{N} \text{ и } i \text{ четное} \\ \left(\frac{i-1}{2}, 2j - 1\right) & , \text{ если } x = (i, j) \in \mathbb{Z} \times \mathbb{N} \text{ и } i \text{ нечетное} \\ x & , \text{ если } x \in \Omega \end{cases}$$

иными словами множество нечетных и множество четных чисел первой строчки перестановка S отправляет биективно и с сохранением порядка во все числа соответственно первой и второй строчки (под сохранением порядка имеет в виду то, что последовательные нечетные числа $2k - 1$ и $2k + 1$ переходят в последовательные числа n и $n + 1$, то же и для четных). Аналогично действие устроено и на второй строчке: нечетные биективно отправляются во всю третью строку, а четные в четвертую и так далее. Ясно, что так определенная C является перестановкой, т.е. биективной.

То, что $C^{-1}AC = A^2$ непосредственно вытекает из формулы для сопряжения перестановок, либо это можно легко проверить непосредственно: перестановки A и CA^2C^{-1} тождественны на Ω, а потому совпадают; что же касается $\mathbb{Z} \times \mathbb{N}$, то A просто сдвигает точку (i, j) на 1 вправо, перестановка же CA^2C^{-1} сначала с помощью C^{-1} переводит ее в четные/нечетные на некоторой строчке, A^2 сдвигает ее до следующего

четного/нечетного, а потом C возвращает ее обратно в изначальную строчку j, и сдвигая изначальный элемент на 1 (потому что перестановка C так строилась, что сдвиг вправо на 2 на левой картинке переходит в сдвиг на 1 на правой картинке), таким образом они совпадают на всех элементах, иными словами $C^{-1}AC = A^2$.



Независимые циклы C устроены так: заметим, что по построению если $j \neq 1$, то C всегда переводит (i, j) в элемент строки с номером строго больше чем j. То же касается $(i, 1)$ с четным i, так как по построению они уходят во вторую строчку. А значит все такие элементы будут соответствовать циклам бесконечной длины, так как они постоянно уходят вниз и никогда не будут зацикливаться. Что касается $(i, 1)$ из первой строки с нечетным i, то возможны две ситуации: первая - это $|i| > 1$; так как $C(i, 1) = \left(\frac{i-1}{2}, 1\right)$, и раз $\left|\frac{i-1}{2}\right| < \left|\frac{i}{2}\right| + \left|\frac{i}{2}\right| = |i|$, то число первой строки под действием C строго уменьшается либо пока не станет четным, и на следующем шаге уходя во вторую строку, а потому порождая бесконечный цикл C; либо пока не попадет в зону $|i| \leq 1$. Вторая ситуация - это когда $|i| \leq 1$, и только 1 и -1 из нечетных удовлетворяют этому условию. Так как $C(1, 1) = \left(\frac{1-1}{2}, 1\right) = (0, 1)$, и так так 0 - четное - на следующем шаге он отправится во вторую строчку, а значит цикл, содержащий этот элемент, бесконечен. Что касается -1, то легко понять, что $C(-1, 1) = (-1, 1)$; неподвижный элемент соответствует циклу длины 1. Таким образом внутри $\mathbb{Z} \times \mathbb{N}$ перестановка C разбивается в бесконечное число циклов бесконечной длины и один цикл длины 1. Именно поэтому мы добавили множество Ω, там C на каждом из элементов Ω тождественна, а значит Ω добавит еще бесконечное число циклов длины 1, и таким образом на всем $(\mathbb{Z} \times \mathbb{N}) \sqcup \Omega$ циклический тип перестановки C будет совпадать с циклическим типом A, а потому будет существовать некоторая еще более страшная перестановка B, такая что $C = B^{-1}AB$, иными словами $A^{A^B} = A^2$, а значит из свойства универсальности существует гомоморфизм $\pi : \mathcal{B} \to S((\mathbb{Z} \times \mathbb{N}) \sqcup \Omega)$, такой что $a \mapsto A, b \mapsto B$. Так как $\pi(a) = A \neq e$, то и $a \neq e$, значит $\mathcal{B}^{(n)} \neq \{e\}$ для любого n, и группа неразрешима.

Замечания:

Замечу, что раз $a \in \mathcal{B}^{(n)}$ *для любого* n, *то* $\bigcap\limits_n \mathcal{B}^{(n)} \neq \{e\}$, *а значит группа* $\mathcal{B}$ *не просто не является разрешимой группой, но даже не является остаточно разрешимой.*

Также хочется рассказать и о следующем очень мощном и красивом приеме, который бы нам помог, если бы мы вдруг оказаться в дословно такой же ситуации лишь за исключением, что $C^{-1}AC$ *и* A^2 *совпадают всюду кроме конечного множества: вдруг бы нам не повезло. Тогда уже нельзя построить гомоморфизм* $\mathcal{B} \to S(X)$, *где* $X = (\mathbb{Z} \times \mathbb{N}) \sqcup \Omega$; *и казалось бы ситуация безнадежная. Но можно пойти на хитрость и рассмотреть:*

$$S_0(X) = \{\sigma \in S(X) : \text{носитель } \sigma \text{ конечный}\}$$

ясно, что $S_0(X) \lhd S(X)$ *так как циклический тип сохраняется при сопряжении. И если* $C^{-1}AC$ *и* A^2 *совпадают всюду кроме конечного множества, то* $C^{-1}ACA^{-2} = \sigma \in S_0(X)$, *а значит "почти соотношение" уже будет выполняться в точности в факторе* $S(X)/S_0(X)$, *иными словами отображение* $a \mapsto AS_0(X)$, $b \mapsto BS_0(X)$ *продолжается до настоящего гомоморфизма:*

$$\pi : \mathcal{B} \mapsto S(X)/S_0(X)$$

Ясно, что $\pi(a) \neq 1$, *потому что перестановка* A *сдвигает бесконечное число элементов, иными словами имеет бесконечный носитель, а значит* $A \notin S_0(X)$. *На этой идее, когда при правильной факторизации что-то похожее на гомоморфизм превращается в настоящий гомоморфизм, построена большая теория аппроксимаций в группах, в частности, к примеру, теория софических групп, которую мы разберем в самом конце методички.*

Пример

Докажите, что $\langle a, b : b^{-1}ab = a^2, a^{-1}ba = b^2\rangle = \{e\}$.

Очень многие группы шифруются под нетривиальные, хотя сами таковыми не являются: например, эта - несмотря на нетривиальность и запутанность соотношений - из них выводится тривиальность всех порождающих:

$$b^{-2}ab^2 = b^{-1}a^2b = a^4$$

$$b^{-2}ab^2 = (a^{-1}b^{-1}a)a(a^{-1}ba) = a^{-1}(b^{-1}ab)a = a^2$$

Таким образом $a^4 = a^2$, а значит $a^2 = e$. Отсюда вытекает, что $a = ba^2b^{-1} = e$. Пользуясь симметрией группы относительно a и b, или же соотношением $a^{-1}ba = b^2$, мы получаем, что $b = e$, т.е. группа тривиальна.

Важнейшие конструкции комбинаторной теории групп

Пусть $G = \langle g_1, g_2, \dots | R_G \rangle, H = \langle h_1, h_2, \dots | R_H \rangle$, где через R_G, R_H мы обозначим набор определяющих соотношений из копредставления G и H соответственно.

$$G \times H = \langle g_1, g_2, \dots, h_1, h_2, \dots | R_G, R_H, [g_i, h_j] = e \text{ для всех } i, j \rangle$$

$$G * H = \langle g_1, g_2, \dots, h_1, h_2, \dots | R_G, R_H \rangle$$

$$G/N = \langle g_1, g_2, \dots | R_G, n = e \text{ для всех } n \in N \rangle$$

Хотя в G/N достаточно в список соотношений включать лишь некоторые n; главное, чтобы их нормальное замыкание было равно N. В частности для абеленизации получаем копредставление:

$$G_{ab} = G/[G, G] = \langle g_1, g_2, \dots | R_G, [g_i, g_j] = e \text{ для всех } i, j \rangle$$

Здесь достаточно факторизовать лишь по коммутаторам порождающих, так как $[ab, x] = a(bxb^{-1}x^{-1}xa^{-1}x^{-1}a)a^{-1} = a([b, x][a^{-1}, x]^{-1})a^{-1}$ и $[a^{-1}, x] = a^{-1}[a, x]^{-1}a$, и из этих формул вытекает, что нормальное замыкание коммутаторов всех порождающих в точности равно коммутанту.

Если задано действие автоморфизмами: $\varphi : H \to \mathrm{Aut}(G)$, то:

$$G \rtimes H = \langle g_1, g_2, \dots, h_1, h_2, \dots | R_G, R_H, \varphi_{h_i}(g_j) = h_i^{-1} g_j h_i \text{ для всех } i, j \rangle$$

Пример

Изоморфны ли $\mathbb{F}_2 \rtimes_\alpha \mathbb{Z}$ и $\mathbb{F}_2 \rtimes_\beta \mathbb{Z}$, где автоморфизмы свободной группы на порождающих заданы $\alpha(a) = a^2b$, $\alpha(b) = a^2bab$ и $\beta(a) = a^2b$, $\beta(b) = ab$.

В этой задаче я хочу оставить за скобками методы проверки того, является ли некоторый гомоморфизм $\mathbb{F}_2 \to \mathbb{F}_2$ автоморфизмом - потому что эта задача главным образом посвящена умению проверять неизоморфность групп с помощью их абеленизаций. Скажу лишь, что в свое время Я. Нильсен доказал, что $\mathrm{Aut}(\mathbb{F}_n)$ порождается 4 автоморфизмами A, B, C, D:

$$A : x_1 \leftrightarrow x_2$$

$$B : (x_1, x_2, \dots, x_n) \to (x_2, x_3, \dots, x_n, x_1)$$

$$C : x_1 \leftrightarrow x_1^{-1}$$

$$D : x_1 \mapsto x_1 x_2$$

иными словами A меняет местами порождающие x_1 и x_2, оставляя остальные элементы неподвижными, B переставляет порождающие по циклу $(12 \dots n)$ (в этих терминах можно сказать, что A переставляет порождающие по циклу (12)), C обращает x_1, не трогая остальные порождающие, а D переводит x_1 в x_1x_2, тоже не трогая остальные порождающие. Очень легко проверяется, что эти отображения, продолженные до гомоморфизма, являются автоморфизмами. Мы помним, что S_n порождается (12) и $(123 \dots n)$, а потому автоморфизмами A и B на самом деле порождаются все автоморфизмы перемешивания порождающих. Также замечу, что

в случае $\mathrm{Aut}(\mathbb{F}_2)$ верно $A = B$. Если обозначить через T автоморфизм, заданный на порождающих $T(a) = a$, $T(b) = ab$, и напомню, что $D(a) = ab$, $D(b) = b$, то тогда автоморфизмы TDT и T^2D на порождающих будут действовать следующим образом:

$$TDT: \quad \begin{matrix} a \mapsto a & \mapsto ab & \mapsto & aab \\ b \mapsto ab & \mapsto abb & \mapsto a(ab)(ab) & \end{matrix}$$

$$T^2D: \quad \begin{matrix} a \mapsto & ab \mapsto & aab \\ b \mapsto & b & \mapsto & ab \end{matrix}$$

Поэтому гомоморфизмы из формулировки задачи будут автоморфизмами, так как они являются композицией автоморфизмов. Доказательство в высшей степени нечестное, так как догадаться, что нужно было брать именно эти композиции - невозможно, но повторюсь: для меня было главное рассказать про автоморфизмы Нильсена и показать, как использовать абеленизации для проверки неизоморфности.

Итак, запишем копредставления обоих полупрямых произведений, а также их абеленизаций:

$$\mathbb{F}_2 \rtimes_\alpha \mathbb{Z} = \langle a, b, c | c^{-1}ac = a^2b, c^{-1}bc = a^2bab \rangle$$

$$\mathbb{F}_2 \rtimes_\beta \mathbb{Z} = \langle a, b, c, | c^{-1}ac = a^2b, c^{-1}bc = ab$$

$$(\mathbb{F}_2 \rtimes_\alpha \mathbb{Z}_2)_{ab} = \langle a, b, c | c^{-1}ac = a^2b, c^{-1}bc = a^2bab, [a,b] = [a,c] = [b,c] = 1 \rangle =$$

$$= \langle a, b, c | a = a^2b, b = a^3b^2, \Omega \rangle = \langle a, b, c | ab = 1, a^3b = 1, \Omega \rangle = \langle a, c | a^2 = 1, \Omega \rangle \cong \mathbb{Z} \oplus \mathbb{Z}_2$$

где через $\Omega = \{[a,b] = [a,c] = [b,c] = 1\}$ мы обозначим условия тотальной коммутации всех порождающих, также условие $ab = 1$ можно фактически воспринимать как определяющее $b = a^{-1}$, что делает переменную b фиктивной. Процесс абеленизации нужно мыслить себе так, словно на группу вы смотрите сквозь розовые коммутативные очки, и в этих розовых очках все на свете коммутирует: грубо говоря вы смотрите на $c^{-1}ac = abab$ сквозь эти очки - и со школьной наивностью видите $a = a^2b^2$. Проделываем то же для второй группы:

$$(\mathbb{F}_2 \rtimes_\beta \mathbb{Z})_{ab} = \langle a, b, c | c^{-1}ac = a^2b, c^{-1}bc = ab, [a,b] = [a,c] = [b,c] = 1 \rangle =$$

$$= \langle a, b, c | ab = 1, a = 1, \Omega \rangle = \mathbb{Z}$$

То есть эта абеленизации получилась в некоторым смысле тривиальной, т.к. при абеленизации полупрямых произведений c всегда выживает и дает $\mathbb{Z}$. Таким образом раз абеленизации различны, то и $\mathbb{F}_2 \rtimes_\alpha \mathbb{Z} \ncong \mathbb{F}_2 \rtimes_\beta \mathbb{Z}$.

Замечания:

Автоморфизмы Нильсена чем-то напоминают преобразования Гаусса из линейной алгебры, но на самом деле их внутренняя структура намного сложнее и богаче: так как группа $\mathbb{F}_n$ некоммутативна; и группа $\mathrm{Aut}(\mathbb{F}_n)$ очень сложная, но все равно небольшая связь с линалом у нее все же есть: легко заметить, что

$$\varphi([\mathbb{F}_n, \mathbb{F}_n]) = [\mathbb{F}_n, \mathbb{F}_n]$$

для любого $\varphi \in \mathrm{Aut}(\mathbb{F}_n)$ (так как коммутаторы переходят в коммутаторы), а потому любой автоморфизм опускается до автоморфизма абеленизаций:
$\varphi_{ab} : \mathbb{F}_n/[\mathbb{F}_n, \mathbb{F}_n] \to \mathbb{F}_n/[\mathbb{F}_n, \mathbb{F}_n]$, а значит существует естественный гомоморфизм:

$$\mathrm{Aut}(\mathbb{F}_n) \to \mathrm{Aut}(\mathbb{Z}^n) = \{x \in GL_n(\mathbb{Z}) : \det(x) = \pm 1\}$$

$$\varphi \mapsto \varphi_{ab}$$

Хотя этот гомоморфизм очень далек от изоморфизма, он является эпиморфизмом: действительно, образом автоморфизмов Нильсена будут в точности матрицы элементарных целочисленных преобразований Гаусса, ранее мы с вами выясняли, что любую целочисленную матрицу с определителем равным ± 1 *можно представить как произведение таких матриц, а потому любая матрица будет в образе. Подумайте над тем, чему равно ядро этого гомоморфизма? Куда под действием этого гомоморфизма перейдет* $\mathrm{Inn}(\mathbb{F}_n)$*?*

Также отмечу, что обе группы $\mathbb{F}_2 \rtimes_\alpha \mathbb{Z}$ *и* $\mathbb{F}_2 \rtimes_\beta \mathbb{Z}$ *содержат* $\mathbb{F}_2$ *в качестве нормальной подгруппы, и в обоих случаях фактор по ней изоморфен* $\mathbb{Z}$*; иными словами получаем еще один пример двух различных групп, состоящих из одинаковых строительных кирпичиков; или более по-научному двух неизоморфных расширений* $\mathbb{F}_2$ *с помощью* $\mathbb{Z}$*.*

Пример

Докажите, что $\mathbb{Z}_2 * \mathbb{Z}_2 \cong \mathbb{Z} \rtimes \mathbb{Z}_2$ *где нетривиальный* $x \in \mathbb{Z}_2$ *действует на* $\mathbb{Z}$ *как автоморфизм* $z \mapsto -z$ *в аддитивной записи.*

Имеем

$$G = \mathbb{Z}_2 * \mathbb{Z}_2 = \langle a, b | a^2 = b^2 = 1 \rangle$$

$$H = \mathbb{Z} \rtimes \mathbb{Z}_2 = \langle x, y | x^2 = 1, x^{-1}yx = y^{-1} \rangle$$

Изоморфизм строится явно:

$$x \mapsto a$$

$$y \mapsto ab$$

С обратным

$$a \mapsto x$$

$$b \mapsto x^{-1}y$$

Можно показать, что при этих отображениях соотношения переходят в соотношения, из универсального свойства эти отображения продолжаются до гомоморфизма, ясно, что они взаимно обратные. Таким образом получаем $G \cong H$.

Либо можно эту же идею оформить через замену переменных: рассмотрим задание группы H в новых порождающих a, b, где $x = a, y = ab$ (ясно, что они порождают группу, так как через них можно выразить x, y). Имеем:

$$H = \langle a, b : a^2 = 1, a^{-1}aba = b^{-1}a^{-1} \rangle$$

С учетом $a^2 = 1$ получаем, что второе соотношение можно преобразовать к $ba = b^{-1}a$ или $b^2 = 1$, таким образом: $H = \langle a, b | a^2 = 1, b^2 = 1 \rangle = G$.

Замечание:

Группу $\mathbb{Z} \rtimes \mathbb{Z}_2$ *обычно называют бесконечной группой Диэдра и обозначают* D_∞*, потому что она является бесконечным аналогом конечных групп Диэдра* $D_n = \langle x, y | x^2 = y^n = 1, x^{-1}yx = y^{-1} \rangle$*. Существует естественный гомоморфизм* $D_\infty \to D_n$*, так как тождественно определенное на порождающих отображение*

$x \mapsto x$, $y \mapsto y$ продолжается до гомоморфизма групп из универсального свойства. Группа D_∞ очень часто встречается в теории групп, так как с одной стороны она достаточно нетривиальна, а с другой стороны про нее известно практически все, и все ее свойства лежат на поверхности: так что она часто является тестовым примером, на котором обкатываются теории и теоремы. Группа $\mathbb{Z}_2 * \mathbb{Z}_2$ тоже в некотором роде исключительная, потому что она является очень частым исключением в формулировках теорем про свободные произведения $G * H$, эдакий гадкий утенок (потому что за счет только что доказанного утверждения это тот случай, когда свободное произведение почти равно прямому произведению: что близко к аномалии, так как никакое нетривиальное свободное произведение не может быть изоморфно нетривиальному прямому произведению). Многие теоремы про свободные произведения звучат так: "что-то там про $G * H$ верно, только если это не $\mathbb{Z}_2 * \mathbb{Z}_2$". Например, нетривиальное свободное произведение $G * H$ является неаменабельным во всех случаях кроме $\mathbb{Z}_2 * \mathbb{Z}_2$ (под нетривиальностью понимаем, что ни один из сомножителей не является тривиальной группой).

Утверждение

Докажите, что элемент конечного порядка группы $G * H$ сопряжен элементу из G или H (причем во всех случаях, даже в случае $\mathbb{Z}_2 * \mathbb{Z}_2$).

Теория свободных произведений очень похожа на теорию свободных групп $\mathbb{F}_k$, фактически эта задача является обобщением ранее доказанного факта, что в группе $\mathbb{F}_k$ нет нетривиальных элементов конечного порядка, причем идея доказательства остается примерно такой же.

Элементы $G * H$ можно понимать как слова (или просто формальные произведения) из букв, где буквами являются элементы либо G, либо H. Взятие обратного - это просто побуквенное взятие обратного вместе с разворотом слова, произведение - формальное приписывание одного слова к другому. Если встречаются буквы из одной группы (G или H) - то они перемножаются обычным умножением этой группы. Если перемножаются элементы из разных групп - то они так и остаются формальным произведением (вида gh). По аналогии со свободными группами слово, которое получается, когда произведены все умножения последовательных букв из одного сомножителя, называется *приведенным*. Иными словами приведенное - это такое слово, где сократить уже ничего нельзя. К примеру $g_1 h g_2$ - приведенное слово, а $g_1 g_2 h$ приведенным не является (здесь $g_i \in G \backslash \{1\}$, $h \in H \backslash \{1\}$). Любой элемент $\omega \in G * H$ имеет один из следующих приведенных видов в зависимости от того, какому из сомножителей принадлежит первая и последняя буква:

$$\omega = g_1 h_1 g_2 \dots g_n h_n$$

$$\omega = g_1 h_1 g_2 \dots g_n h_n g_{n+1}$$

$$\omega = h_1 g_1 h_2 \dots g_n h_n$$

$$\omega = h_1 g_1 h_2 \dots g_n h_n g_{n+1}$$

где $g_i \in G, h_i \in H$, причем все $g_i \neq 1$ и все $h_i \neq 1$. Но в задачах редко рассматривают все 4 варианта: если группы G и H равноправны - то часто можно отбросить 2 варианта, оставив только 2. Но чаще ограничиваются только одним, когда во втором случае рассуждения оказываются аналогичными. Приведенная форма хорошая и

помогает конструктивно работать со свободными произведениями: например, легко понять, что два элемента, записанные в приведенной форме, совпадают iff они совпадают побуквенно.

Как и в свободных группах в свободных произведениях есть такое понятие как *циклически-приведенная форма*: это приведенная форма, которая не имеет вида $x^{-1}\omega x$ для некоторой буквы или слова x (грубо говоря которую нельзя "сократить сопряжениями"). Минус ее в том, что она является инвариантом не самого элемента группы, а его класса сопряженности; но плюс ее в том, что часто этого хватает, но по свойствам с ней намного проще работать, чем просто с приведенной формой.

Итак пусть $\omega \in G * H$ с $\mathrm{ord}(\omega) < \infty$. Запишем его в виде слова и можем считать, что оно циклически приведено, так как сопряжение не меняет ни порядка, ни класса сопряженности (если оно не является циклически приведенным и имеет вид $x^{-1}\omega x$, то мы можем сопрягать на x^{-1} до тех пор, пока оно не станет циклически приведенным). Из равноправия G и H можем считать, что слово начинается с G и таким образом возможны 2 варианта:

$$\omega = g_1 h_1 g_2 \dots g_n h_n$$

$$\omega = g_1 h_1 g_2 \dots g_n h_n g_{n+1}$$

Рассмотрим случай, когда есть хотя бы 2 буквы. В первом случае невозможно получить конечный порядок, так как степеням ω^m будет соответствовать многократное приписывание слова к себе, внутри слова сокращений нет, а на стыках слов будут тоже несокращаемые куски $...h_n g_1...$, таким образом сократить это слово до пустого никак не получится. Но во втором случае конечный порядок тоже невозможен, так как из-за циклической приведенности (видите, как сильно она нам помогла!) мы имеем $g_1 \neq g_{n+1}^{-1}$, а значит внутри слов сокращений нет, а когда при перемножении будем приписывать слова друг к другу, на стыках будут фрагменты $....h_n g_{n+1} g_1 h_1...$, при перемножении $g_{n+1} g_1$ получится какой-то нетривиальный элемент G, и на этом сокращения закончатся. Полученная форма будет приведенной, а значит несократимой. Единственный возможный случай, это когда слово состоит только из одной буквы, то есть $\omega = g_1$, что означает, что исходный элементы был сопряжен элементу одного из свободных сомножителей.

Пример

Вычислить $Z(G)$ для $G = \langle a, b | a^2 = b^2 = e \rangle$.

Произвольный элемент $\omega \in G$ может быть записан с учетом соотношений в следующей простой форме $\omega = abab\dots$ (или $\omega = baba\dots$), так как любая степень буквы редуцируется либо к 0, либо к 1 степени. Покажем, что если ω нетривиально как слово такого вида, то и $\omega \neq e$ в группе G. Без ограничения общности можем считать, что $\omega = (ab)(ab)a\dots$ Рассмотрим изоморфизм из одной из предыдущих задач $\alpha : G \to D_\infty = \langle x, y | x^2 = 1, x^{-1}yx = y^{-1} \rangle$ (напомню, что он задавался на порождающих формулой $a \mapsto x$ и $b \mapsto x^{-1}y$) и тождественный на порождающих гомоморфизм $\beta_n : D_\infty \to D_n = \langle x, y | x^2 = y^n = 1, x^{-1}yx = y^{-1} \rangle$, а также их композицию:

$$G \to D_n$$

Ясно, что при этом гомоморфизме $\omega = (ab)(ab)a\dots$ перейдет либо в y^k, либо в $y^k x$ в зависимости от того, на какую букву заканчивается слово ω, в одном случае это поворот, в другом случае зеркальная симметрий - и оба являются нетривиальными

движениями при достаточно большом n. А значит $\omega \neq 1$ в группе G. Как следствие получаем, что $\omega_1 = \omega_2$ как слова iff $\omega_1 = \omega_2$ как элементы группы G: в одну сторону - очевидно, а в другую: если $\omega_1\omega_2^{-1} = 1$ как элементы G, то по только что доказанному слово $\omega_1\omega_2^{-1}$ должно стать тривиальным после привидения, то есть в нем должно сократиться абсолютно всё, а так как каждое слово в отдельности было несократимым, то они обязаны сократить друг друга, то есть $\omega_1 = \omega_2$ как слова.

Пусть нетривиальный $\omega = abab\ldots \in Z(G)$ (без ограничения общности считаем, что слово начинается с a). Тогда $b\omega$ начинается с b, а ωb начинается с a. Если они как слова различны - то и как элементы они тоже будут различны, как мы только что показали - приходим к противоречию. Таким образом $Z(G) = \{e\}$.

Кстати, второй подход - это строить доказательство не вокруг изоморфизма $G \cong D_\infty$, а вокруг изоморфизма $G \cong \mathbb{Z}_2 * \mathbb{Z}_2$ - и воспользоваться фактом, что любой нетривиальный элемент $\Gamma * H$ единственным образом представляется в виде произведения $x_1x_2\ldots x_k$, где x_i лежит либо в $\Gamma\backslash\{e\}$, либо $H\backslash\{e\}$, этой конструкцией мы пользовались в предыдущей задаче.

==========

Задачи для самостоятельной работы

- Доказать, что группа $S_2 \times S_3$ порождается 2 элементами.
- Доказать, что $S_3 \cong \langle a, b |\ a^2 = b^3 = 1, a^{-1}ba = b^2\rangle$.
- Пусть $F = \langle a, b \mid [ab^{-1}, a^{-1}ba] = [ab^{-1}, a^{-2}ba^2] = 1\rangle$ группа Томпсона. Доказать, что

$$F \cong \langle x_0, x_1, x_2, \ldots \mid x_k^{-1}x_nx_k = x_{n+1} \text{ для } k < n\rangle$$

- Пусть $H_3 = \langle a, b, c \mid a^{-1}ba = b^2, b^{-1}cb = c^2, c^{-1}ac = a^2\rangle$, нужно доказать, что $H_3 = \{1\}$. Группа H_3 является неполноценным аналогом группы Хигмана H_4, где таким образом зацикливается уже не 3, а 4 порождающих. Группа H_4 в отличие от H_3 далеко нетривиальна и является контрпримером для многих сюжетов в теории групп, связанных с аппроксимациями, которые мы обсудим в самом конце методички.

Абелевы группы

Есть очень мощная структурная классификационная теорема, описывающая произвольную конечно-порожденную абелеву группу:

Теорема

Пусть G - конечно-порожденная абелева группа. Тогда

$$\boxed{G \cong \mathbb{Z}^n \oplus \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}}$$

причем если брать в качестве n_i степени простых чисел - то такое разложение единственно с точность до перестановки.

Если абелева группа конечна - то в разложении отсутствует $\mathbb{Z}^n$. Вообще говоря разложение в таком виде неединственно, к примеру: $\mathbb{Z}_n \cong \mathbb{Z}_k \oplus \mathbb{Z}_m$, если $(m,k) = 1$ и $mk = n$, но единственность появляется, когда порядки циклических сомножителей являются степенями простых чисел, иными словам неразложимы в произведение взаимно простых.

Основными инструментами работы с абелевыми группами (помимо этой теоремы) являются *порядки элементов* (допустимые порядки, количество элементов заданного порядка и т.д.) и *подгруппы nG* (часто не нужно выяснять чему они изоморфны, а достаточно просто некоторых их свойств, зачастую хватает порядков этих подгрупп). Замечу, что основная структурная теорема доказывается именно с помощью этих двух инструментов. К примеру, докажем, что $G = \mathbb{Z}_p \oplus \mathbb{Z}_p$ и $H = \mathbb{Z}_{p^2}$ являются неизоморфными. Замечаем, что $|pG| = 1$, но $|pH| = p$ - значит $G \ncong H$. Или можно сказать, что в группе H есть элемент порядка p^2, а в группе G такого элемента нет. Конечно же, здесь можно было бы воспользоваться структурной теоремой, но возможности этих двух инструментов простираются за границы этой теоремы (как минимум, потому что теорема работает только для конечно-порожденных групп) - а потому эту технику нужно освоить.

Задача

Описать все абелевы группы порядка 36.

Удобно, когда порядки прямых сомножителей - степени простых чисел, так как в таком виде соответствующие группы легко сравнивать на изоморфность. Имеем: $36 = 2^2 \cdot 3^2$ - сколькими способами можно разбить это число в произведение степеней простых? Ответ: четырьмя способами: $4 \cdot 9, 2 \cdot 2 \cdot 9, 4 \cdot 3 \cdot 3$ и $2 \cdot 2 \cdot 3 \cdot 3$. Этим разбиениям будут соответствовать группы:

$$\mathbb{Z}_4 \oplus \mathbb{Z}_9$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

Все эти группы неизоморфны по структурной теореме. Обычно в теории абелевых групп чтобы подчеркнуть абелевость пишут $\oplus$ вместо $\times$.

Задача

Описать все абелевы группы порядка 24.

Раскладываем в произведение простых $24 = 3 \cdot 2^3$. Как произведение степеней простых его можно представить тремя способами: $3 \cdot 8$, $3 \cdot 4 \cdot 2$ и $3 \cdot 2 \cdot 2 \cdot 2$, этим разбиениям соответствуют три группы:

$$\mathbb{Z}_3 \oplus \mathbb{Z}_8$$

$$\mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$$

$$\mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Все они неизоморфны по структурной теореме, либо можно с двумя инструментами здесь повозиться.

Задача

Сколько существует абелевых групп порядка 24149664.

Разложим в произведение простых: $24149664 = 11^3 \cdot 7 \cdot 3^4 \cdot 2^5$. Количество таких групп совпадает с количеством разбиений этого числа в произведение степеней простых, такие разбиения проходят независимо в каждом сомножителе p^k. Легко понять, что количество таких разбиений для каждого p^k равно количеству разбиений натурального числа k на слагаемые, обозначаемое через $P(k)$. Имеем:

$$N = P(3)P(1)P(4)P(5) = 3 \cdot 1 \cdot 5 \cdot 7 = 105$$

Т.е. всего таких групп 105 штук. Хотя общей формулы для $P(k)$ записать нельзя, для маленьких k число $P(k)$ можно вычислить вручную перебором. Разложения k на слагаемые иногда удобно графически интерпретировать диаграммами Юнга из k клеток (в частности $P(k)$ равно количеству таких диаграмм).

Пример

Изоморфны ли группы $\mathbb{Z}_6 \oplus \mathbb{Z}_{36} \cong \mathbb{Z}_9 \oplus \mathbb{Z}_{24}$?

Чтобы ответить на этот вопрос - приведем их к каноническому виду, где порядок каждого прямого слагаемого - степень простого числа. Это всегда можно сделать по лемме о разбиении $\mathbb{Z}_n = \mathbb{Z}_k \oplus \mathbb{Z}_m$ при $(m, k) = 1$ и $mk = n$.

$$\mathbb{Z}_6 \oplus \mathbb{Z}_{36} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9$$

$$\mathbb{Z}_9 \oplus \mathbb{Z}_{24} \cong \mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3$$

Разбиения в каноническом виде различны - значит группы неизоморфны.

Пример

Существуют ли вложения групп:

$\mathbb{Z}_2 \oplus \mathbb{Z}_8 \hookrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_{16}$?

$\mathbb{Z}_4 \oplus \mathbb{Z}_4 \hookrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_{16}$?

В первом случае ответ положительный и вложение покоординатное: в аддитивной записи задается формулой $(n, m) \mapsto (n, 2m)$.

Во втором случае вложения *не существует*, порядок группы здесь препятствием не является, но можно заметить, что уравнение $4x = 0$ в аддитивной записи в группе $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ имеет 16 решений (любой элемент - это решение), а в группе $\mathbb{Z}_2 \oplus \mathbb{Z}_{16}$ решений всего 8, а именно:

$$4(x_1, x_2) = 0 \Leftrightarrow \begin{cases} 4x_1 = 0 \\ 4x_2 = 0 \end{cases} \Leftrightarrow \begin{cases} x_1 - \text{ любое} \\ x_2 = 0, 4, 8, 12 \end{cases}$$

Так как решение такого уравнения переходит в решение, то такие количества противоречат инъективности. Число 4 выбрано с учетом специфики этой задачи, в общем случае можно подумать о решениях уравнения $Nx = 0$.

Как мы видим, теория конечных абелевых групп уходит не намного дальше теории разбиений числа в произведение простых.

В жизни не всегда конечно порожденная абелева группа задана как прямая сумма циклических - очень часто она бывает представлена как фактор свободной абелевой группы (то есть $\mathbb{Z}^n$) по некоторой подгруппе - в таком случае нужно уметь переходить к каноническому виду. Порождающие подгруппы записываются в виде линейной комбинации порождающих исходной группы - и коэффициенты разложения обычно записывают в "матрицу подгруппы".

Алгоритм - нужно привести эту матрицу к диагональному виду

Мы можем совершать лишь целочисленной преобразования Гаусса - так как в отличие от линейной алгебры в группах нет операции умножения и деления на число (но есть операция умножения на целое число, так как оно выражается через групповое сложение: $ng = g + \ldots + g$). Со строками мы можем безболезненно делать любые целочисленные элементарные преобразования (вычитание или прибавление одной строки, умноженной на n, к другой; есть возможность умножать строку на -1) - так как этому отвечает переход к эквивалентной системе соотношений. Со столбцами ситуация сложнее: элементарным преобразованиям столбцов соответствует замена базиса по *правилу наоборот*: к примеру, если вы хотите из II столбца вычесть I, то по итогу этого преобразования к первой образующей прибавляется вторая образующая (т.е. дважды наоборот: и сложение меняем на вычитание, и номера тоже меняем). Почему это происходит так - мы увидим на примере, и это нетрудно доказать. Чтобы не запутаться - обычно над столбцами пишут актуальные значения порождающих. Если канонические порождающие находить не нужно - то со столбцами можно не заморачиваться: и преобразования со строками и столбцами становятся в некотором смысле равноправными. Также как и в линале советую подписывать рядом с волной преобразования, которые вы делаете - чтобы не запутаться и чтобы было проще искать арифметическую ошибку, если

она и появится: для определенности будем преобразования со строками отмечать снизу, а со столбцами - сверху. Сразу скажу, что есть алгоритмический метод приведения к диагональному виду: в углу с помощью элементарных преобразований вы получаете НОД всех элементов матрицы, а дальше с помощью этого НОДа зануляете первую строку и первый столбец кроме углового элемента - и переходите к меньшей подматрице. Это 100-процентный метод, но он очень трудоемкий, и на практике пользуются обычно кустарными интуитивными методами "лишь бы после преобразований было побольше нулей" а также "полцарства за единицу" (потому что единицы в таком методе Гаусса на вес золота, из-за того что делить нельзя, а они могут сразу занулить строку и столбец), если не получается получить единицу - то стараются максимально уменьшать матричные коэффициенты - и в простых задачах это часто работает.

Полезное замечание:

Из описанного выше вытекает, что целочисленным методом Гаусса можно любую квадратную матрицу привести к диагональной, причем с учетом происходящего ясно, что на диагонали будут целые числа.

Теперь пусть нам дана целочисленная матрица S, такая что $\det(S) = 1$. *И если ограничиться лишь преобразованиями, преобразующими одну строчку/столбец с помощью других, и обойти стороной перестановки строк/столбцов и умножения строки/столбца на -1 - тогда этими преобразованиями мы можем в некотором месте матрицы получить $\pm$НОД (равный ± 1, так как* $\det(S) = 1$*), а потом занулить строку и столбец, и повторять эти операции для уже меньших подматриц; если у нас нет преобразований перестановок строк/столбцов - не факт, что нам получится получить их именно на диагонали. И в таком случае если нам дана матрица с определителем равным 1, то такими преобразованиями метода Гаусса мы можем эту матрицу привести к перемешанно-диагональной, у которой все ненулевые коэффициенты равны 1 и -1 (то есть матрице, у которой в каждой строке и каждом столбце есть только один ненулевой элемент, иными словами это диагональная матрица, умноженная на матрицу перемешивания базиса). Преобразований перестановок мы избегаем, так как их определитель не обязан быть равен 1.*

Теперь посмотрим на это с другого ракурса: фактически метод Гаусса означает, что мы представляем матрицу S:

$$S = R_k \dots R_1 D T_1 \dots T_m$$

как произведение матриц элементарных преобразований строк и столбцов R_i, T_i и перемешанно-диагональной матрицы D. Все они имеют определитель единица. Более того, всего существует конечное число перемешанно-диагональных матриц с 1 и -1 в качестве ненулевых элементов, а также все элементарные преобразования можно выразить через конечное число элементарных преобразований: прибавление к одной строке другой, умноженной на q, есть в точности q-кратное применение обычного прибавления строки, на уровне матриц в соответствующем индексам этих строк блоке будет происходить следующее:

$$\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^q$$

Иными словами, это означает, что группа $SL_n(\mathbb{Z})$ является конечно-порожденной, и порождается перемешанно-диагональными матрицами, и матрицами

прибавления строк к другим строкам. Такие матрицы имеют блочный вид, где вне i,j координат матрица тождественная, а в i,j-блоке матрица

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$$

Кстати не нужно думать, что это - верхнетреугольные матрицы: потому что такой визуальный вид матрица имеет лишь в случае $i<j$, если же $i>j$, то при нормальном порядке координат блок будет состоять из матрицы, транспонированной к этой.

Пример

Найти канонический вид и канонические образующие для абелевой группы $G=\mathbb{Z}^2/N$, где $\mathbb{Z}^2=\langle a,b\rangle$, $N=\langle a+2b, 2a-4b\rangle$.

Запишем фактические соотношения на порождающие $\begin{cases}a+2b=0\\ 2a-4b=0\end{cases}$ в матрицу (каждому соотношению выделяется строка матрицы) и приведем ее с помощью целочисленных преобразований Гаусса к каноническому виду (заботясь о столбцах, так как требуют канонические образующие):

$$\begin{matrix}a & b\end{matrix}\\ \begin{pmatrix}1 & 2\\ 2 & -4\end{pmatrix}\underset{II-2I}{\sim}\begin{matrix}a & b\end{matrix}\\ \begin{pmatrix}1 & 2\\ 0 & -8\end{pmatrix}\overset{II-2I}{\sim}\begin{matrix}a+2b & b\end{matrix}\\ \begin{pmatrix}1 & 0\\ 0 & -8\end{pmatrix}$$

Вот оно "правило наоборот" в действии: так как фактически первая строка предпоследней матрицы соответствовала соотношению $a+2b=0$, а первая строка последней матрицы - соотношению $x=0$, то понятно, чему должна быть равна новая переменная x (она должна быть в точности равна соотношению). Если вдруг забудете это правило - я вам советую на супер-простой матрице (вроде этой), где и руками можно найти канонические порождающие, это правило восстановить. Таким образом в переменных $x=a+2b$ и $y=b$ имеем $N=\langle x,8y\rangle$, а значит:

$$G=\langle x,y\rangle/\langle x,8y\rangle=(\langle x\rangle/\langle x\rangle)\oplus(\langle y\rangle/\langle 8y\rangle)\cong\mathbb{Z}_8$$

Соответствующими каноническими образующими (т.е. такими, при которых соотношения "расщепляются") будут $a+2b$ и b. Ясно, что выбор канонических образующих неединственный. Замечу, что с помощью канонических порождающих легко отвечать на групповые вопросы об элементах группы. К примеру, если в этой задаче нужно найти порядок элемента a, то в терминах a,b - неясно как к этому подступиться, но если перейти к x,y и выразить $a=a+2b-2b=x-2y$, то

$$\operatorname{ord}(a)=\operatorname{ord}(x-2y)=\operatorname{ord}(x,-2y)=\text{НОК}\{\operatorname{ord}(x),\operatorname{ord}(2y)\}=\text{НОК}\{1,4\}=4$$

Проводя аналогию с линалом, найти канонические образующие - это все равно что матрицу к диагональному виду привести.

Пример

Выяснить, чему изоморфна группа

$$G = \langle a, b, c | a^8b^3c^2 = a^4b^4c^{-4} = a^{-4}bc^{-6} = [a, b] = [a, c] = [b, c] = e\rangle$$

Группа абелева - и чтобы было комфортно сразу перепишем первые три соотношения в аддитивной записи: $8a + 3b + 2c = 4a + 4b - 4c = -4a + b - 6c = 0$. Запишем их в матрицу и с помощью целочисленных преобразований Гаусса приведем ее к диагональному виду (про канонические образующие не спрашивают, а потому одинаково спокойно мы можем работать как со строчками, так и со столбцами. Сразу запишем второе соотношение в первой строчке, так как с него мы и начнем нашу работу):

$$\begin{pmatrix} 4 & 4 & -4 \\ 8 & 3 & 2 \\ -4 & 1 & -6 \end{pmatrix} \underset{\text{II-2I, III+I}}{\sim} \begin{pmatrix} 4 & 4 & -4 \\ 0 & -5 & 10 \\ 0 & 5 & -10 \end{pmatrix} \overset{\text{II-I, III+I}}{\sim} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 5 & -10 \end{pmatrix} \overset{\text{III+2II}}{\sim} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix}$$

Привели матрицу к диагональному виду. Это значит, что в некоторых переменных x, y, z (явными значениями которых мы не интересовались) исходная группа имеет копредставление (я запишу сразу абелево копредставление: без коммутационных соотношений и в аддитивной записи):

$$G = \langle x, y, z \mid 4x = 5y = 0\rangle \cong \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}$$

На z не оказалось никаких соотношений - а потому оно порождает свободную циклическую подгруппу $\mathbb{Z}$.

Достаточно важное замечание:

Пусть конечно-порожденная абелева группа задана своим копредставлением, причем количество порождающих равно количеству соотношений (дополнительных к коммутационным, например как в этом примере) - тогда матрица соотношений будет квадратной. Тогда для того, чтобы понять чему изоморфна группа - методом Гаусса мы приводим матрицу к диагональному виду, и то что окажется на диагонали скажет чему изоморфна группа. Также отметим, что преобразования метода Гаусса не меняют модуля определителя матрицы, причем нетрудно заметить, что если матрица соотношений диагональна - тогда модуль определителя в точности равен порядку группы. Таким образом, если A - квадратная матрица исходных соотношений абелевой группы G, то $|G| = |\det(A)|$. Если же $\det(A) = 0$, то методом Гаусса такая матрица приводится к диагональной как минимум с одним 0 на диагонали, это будет означать, что группа бесконечная, таким образом для любой матрицы (не обязательно диагональной) верно, что если $\det(A) = 0$, то $|G| = \infty$. Наблюдение это не очень полезное, так как в большинстве случае определитель как раз через метод Гаусса вычисляется, и когда мы получаем определитель - у нас как правило матрица уже в диагональной форме. Хотя все-таки некоторая польза от этого утверждения есть: и в случаях, когда нормальный человеческий метод Гаусса (вещественнозначный, то есть с делениями) оказывается существенно проще нашего целочисленного, а также в случаях, когда определитель вычисляется каким-то хитрым способом, например, на основании рекуррентных соотношений.

Также можно быстро получить дополнительное подтверждение правильности ответа в каких-нибудь совсем простых ситуациях типа матриц 2×2; и если определитель равен, скажем, 4, а порядок полученной группы равен 6, то значит где-то есть ошибка. Или скажем, это наблюдение позволяет сразу сказать, что группа

$$G = \langle a, b | a^7 b^5 = a^3 b^2 = 1, [a, b] = 1 \rangle$$

является тривиальной, так как:

$$\begin{vmatrix} 7 & 5 \\ 3 & 2 \end{vmatrix} = -1$$

Задача

Доказать, что группа $G = \langle a, b \mid \ ab^{222}a = ba^{28} \rangle$ нетривиальна.

Когда вы исследуете тривиальность группы, заданной копредставлением - в первую очередь нужно проверить, является ли нетривиальной ее абеленизация, так как она вычисляется почти устно, и в совсем простых ситуациях, когда она нетривиальна, вы сразу сможете сделать вывод, что и исходная группа нетривиальна. Имеем:

$$G = \langle a, b \mid \ ab^{222}a = ba^{28} \rangle$$

$$G_{ab} = G/[G, G] \cong \langle a, b \mid \ ab^{222}a = ba^{28}, [a, b] = 1 \rangle$$

или в аддитивной записи $G_{ab} = \langle a, b \mid 221b = 26a, [a, b] = 0 \rangle$. Но так как $\text{НОД}(221, 26) = 13$, то из нашей теории вытекает, что 1×2-матрицу соотношений $(-26, 221)$ можно привести преобразованиями Гаусса к виду $(13, 0)$, а значит $G_{ab} \cong \mathbb{Z} \oplus \mathbb{Z}_{13}$, в частности группа G нетривиальна.

Хочется сказать несколько слов про бесконечно-порожденные абелевы группы. Есть две важные конструкции: пусть G_i произвольные группы, тогда *прямой суммой* и *прямым произведением* мы назовем соответственно группы:

$$\bigoplus_{n=1}^{\infty} G_i = \{(g_1, g_2, \ldots) : g_i \in G_i \text{ и существует } n \text{ что для любого } i > n \text{ выполнено } g_i = 1\}$$

$$\prod_{n=1}^{\infty} G_i = \{(g_1, g_2, \ldots) \ \ g_i \in G_i\}$$

где условие $g_i = 1$ в случае абелевых G_i в аддитивной форме можно переписать как $g_i = 0$. Операции в этих группах покоординатные. Обе эти конструкции являются бесконечным обобщением обычного прямого произведения $G \oplus H = G \times H$, но при этом их зона применения и свойства в бесконечном случае в корне отличаются от конечного случая. К примеру $\oplus G_i$ часто используется как самостоятельная группа, тогда как $\prod G_i$ часто используется как вместилище для других групп. Также $\prod G_i$ чаще встречается в теории топологических групп и наделяется топологией Тихонова. Также $\oplus G_i$ счетна в случае счетных G_i (а потому для нее можно записать счетное копредставление), группа же $\prod G_i$ типично, что несчетна. Кстати, используя

соображения мощности легко показать, что группы $\oplus_n \mathbb{Z}_2$ и $\prod_n \mathbb{Z}_2$ не являются изоморфными, так как первая счетная, а вторая континуальная. Также очевидно, что всегда $\oplus G_i < \prod G_i$. Теоретически можно рассматривать сумму и произведение с не обязательно счетным числом прямых сомножителей или слагаемых:

$$\bigoplus_{\lambda\in\Lambda} G_\lambda = \{(g_\lambda) : \ g_\lambda \in G_\lambda \text{ все } g_\lambda = 1 \text{ кроме конечного числа}\}$$

$$\prod_{\lambda\in\Lambda} G_\lambda = \{(g_\lambda) : \ \ g_\lambda \in G_\lambda\}$$

Следующая задача поможет лучше прочувствовать прямые суммы и произведения:

Задача

Пусть Λ - континуальное множество. Доказать, что

$$\bigoplus_{\lambda\in\Lambda} \mathbb{Z}_2 \cong \prod_{n=1}^{\infty} \mathbb{Z}_2$$

$$\bigoplus_{\lambda\in\Lambda} \mathbb{Z} \ncong \prod_{n=1}^{\infty} \mathbb{Z}$$

В этой задаче будем работать в аддитивной форме. Соображения мощности в чистом виде ничего не дадут, так как мощность всех четырех групп континуальная. Первое утверждение практически очевидно: пусть $G = \bigoplus\limits_{\lambda\in\Lambda} \mathbb{Z}_2$ и $H = \prod\limits_{n=1}^{\infty} \mathbb{Z}_2$. Если рассматривать эти группы в аддитивной записи, то ясно, что если добавить к операции сложения операцию умножения на элементы из $\mathbb{Z}_2$ по правилу $0x = x$ и $1x = x$, то группы превращаются в векторные пространства над полем $\mathbb{Z}_2$ (то есть такое умножение на скаляр согласуется с групповыми операциями). Принимая аксиому выбора, мы получаем, что у каждого пространства есть базис, и легко понять, что в обоих случаях он будет континуальным. Таким образом G и H оказываются изоморфными как линейные пространства (линейный изоморфизм просто отображает векторы одного базиса в соответствующие векторы другого базиса и линейным образом продолжается на их линейные комбинации), а значит и с более бедной только групповой структурой они будут изоморфны.

Перейдем ко второму пункту, пусть $A = \bigoplus\limits_{\lambda\in\Lambda} \mathbb{Z}$ и $B = \prod\limits_{n=1}^{\infty} \mathbb{Z}$. И предположим, что существует изоморфизм $\pi : B \to A$. Элемент g абелевой группы группы G мы будем называть 2^∞-*делимым*, если для любого n существует h, такой что $g = 2^n h$, иными словами этот элемент можно делить на 2 сколь угодно много раз. К примеру в группе $\mathbb{Z}$ нет ненулевых 2^∞ делимых элементов, а в группе $\mathbb{Q}$ каждый элемент является 2^∞-делимым. И легко понять, что не только в $\mathbb{Z}$, но и в любой их прямой сумме также не может быть ненулевых 2^∞-делимых элементов, так как если элемент прямой суммы допускает деление на любую степень двойки, то и любая координата должна допускать такое деление, то есть любая координата нулевая. Рассмотрим $C = \bigoplus\limits_{n=1}^{\infty} \mathbb{Z} < B$. Если π - изоморфизм, то и группы B/C и $A/\pi(C)$ должны быть изоморфны, но анализируя 2^∞-делимые элементы мы докажем, что это не так.

Так как C счетная группа, и каждый элемент A имеет по определению конечный носитель, то существует некоторое счетное $\Lambda_0 \subset \Lambda$, что носители всех элементов из $\pi(C)$ содержатся в Λ_0, иными словами $\pi(C) < \bigoplus\limits_{\lambda\in\Lambda_0} \mathbb{Z} < \bigoplus\limits_{\lambda\in\Lambda} \mathbb{Z}$ (причем отмечу, что $\pi(C)$ не обязана быть некоторым $\bigoplus\limits_{\lambda\in\Omega} \mathbb{Z}$ в этом разложении для некоторого $\Omega \subset \Lambda$ и она может отображаться как-то криво и поперек координат). А значит раз $\Lambda\backslash\Lambda_0$-координаты всех $\pi(C)$ равны 0, то:

$$A/\pi(C) = \left(\bigoplus_{\lambda\in\Lambda_0} \mathbb{Z}/\pi(C)\right) \oplus N$$

где $N = \bigoplus\limits_{\lambda\in\Lambda\backslash\Lambda_0} \mathbb{Z}$. Как мы уже обсуждали в N только нулевой элемент является 2^∞-делимым, а потому любой 2^∞-делимый элемент $A/\pi(C)$ имеет вид $(x, 0)$, где x это 2^∞-делимый элемент группы $\left(\bigoplus\limits_{\lambda\in\Lambda_0} \mathbb{Z}/\pi(C)\right)$. Но эта группа счетная, а потому и таких элементов может быть только счетное число. Значит в группе $A/\pi(C)$ не более чем счетное число 2^∞-делимых элементов.

При этом элемент $x = (1, 2, 4, 8, \ldots) \in B$ хотя сам и не является 2^∞-делимым, но ясно, что он становится таковым в факторе B/C (к примеру для $y = (0, 0, 1, 2, 4, \ldots)$ верно $x = 4y$ в B/C, так как факторизация на C игнорирует любое конечное число координат). И чтобы из него наплодить континуум 2^∞-делимых элементов - полезно вспомнить крайне важную теоретико-множественную лемму Серпинского. Очень часто в математике в счетном множестве нужно построить несчетное число попарно непересекающихся бесконечных множеств. К сожалению или к счастью этого сделать нельзя, но математики идут на компромисс и часто в задачах достаточно непересекаемости с точностью до конечного множества. И согласно лемме Серпинского такое уже возможно, а именно она утверждает, что *в* $\mathbb{N}$ *существует несчетное семейство бесконечных множеств* $\Omega \subset 2^{\mathbb{N}}$*, любые два различные множества из которого пересекаются только по конечному множеству.* Эта лемма очень популярна и имеет миллиард доказательств. Мне больше всего нравится такое: биекцией отождествим $\mathbb{N}$ и $\mathbb{Q}$ и в качестве Ω рассмотрим континуальный набор $\{M_x\}_{x\in\mathbb{R}}$, где $M_x \subset \mathbb{Q}$ некоторая строго монотонная последовательность, сходящаяся к x. Ясно, что их попарные пересечения конечны, так как если бы $M_x \cap M_y$ было бы бесконечным, то эти две последовательности имели бы общую подпоследовательность, что невозможно, так как у них различные пределы $x \neq y$. Так вот, чтобы расплодить эту нашу последовательность - построим множество Серпинского $\Omega \subset 2^{\mathbb{N}}$ и рассмотрим континуальное множество $\{x_I\}_{I\in\Omega}$, где x_I - это последовательность, такая что его координаты с индексами из I равны в некотором порядке $\{1, 2, 4, 8, \ldots\}$, а координаты с индексами из $\mathbb{N}\backslash I$ равны нулю. Принципиально такие элементы ничем не отличаются от их прародителя x, а потому они тоже будут 2^∞-делимыми в B/C. С другой стороны они все различны в B/C, так как при $I \neq J \in \Omega$ по построению $I \cap J$ конечно, а потому элемент $x_I - x_J$ будет иметь бесконечное число ненулевых координат, а значит $x_I - x_J \notin C$, иными словами x_I и x_J различны в B/C. Таким образом группа B/C допускает континуальное число 2^∞-делимых элементов, а значит $A \ncong B$.

Теория абелевых групп богата и интересна. Даже в счетном случае (который во многом изучен) могут возникать аномалии, существенно отличающие его от только что изученного нами конечно-порожденного случая; хотя и многие важные классы счетных абелевых групп полностью классифицируются инвариантом Ульма. Некоторый модельный тестовый источник самого разного рода контрпримеров - это группа $\mathbb{Q}$ а также все ее подгруппы и факторы. К примеру, группа $\mathbb{Q}$ не допускает никакого нетривиального разбиения в прямую сумму, что сильно контрастирует с классификационной теоремой о конечно-порожденных группах. Поэтому если хотите перейти на следующий уровень понимания абелевых групп после теоремы о классификации конечно-порожденных абелевых групп - почаще размышляйте о $\mathbb{Q}$. К примеру, можно ли что-нибудь хорошее сказать про $\mathbb{Q}/\mathbb{Z}$? Есть ли там элементы бесконечного порядка? Конечного порядка? Допускает ли она разложение в прямую сумму? Изоморфна ли она чему-нибудь другому хорошему? Какая ситуация с делимостью элементов: есть ли там 2-делимые элементы или даже 2^∞-делимые? В общем, полезно вести с группами такие диалоги. В случае же континуальных абелевых групп вопросов еще больше, а ответов еще меньше.

Счетные абелевы группы, разумеется, тоже можно задавать копредставлением, но увы работать с ним с помощью метода Гаусса по аналогии с конечно-порожденными группами уже не получится (за исключением совсем примитивных случаев; и самая главная возникающая проблема заключается в том, что новые "порождающие" не обязаны порождать нашу группы. Если матрица конечная - то можно раскрутить с конца метод Гаусса и восстановить исходные порождающие, в случае же с бесконечными матрицами такого конца может не быть).

Пример

Выяснить, чему изоморфна группа

$$G = \langle x_i |\ [x_i, x_j] = 0, 2x_1 + x_2 = 0, x_i + 2x_{i+1} + x_{i+2}; i, j \in \mathbb{N} \rangle$$

Матрица определяющих соотношений имеет вид (в пустующих местах всегда стоит 0):

$$\begin{pmatrix} 2 & 1 & & & & \\ 1 & 2 & 1 & & & \\ & 1 & 2 & 1 & & \\ & & 1 & 2 & 1 & \\ & & & & & \ddots \end{pmatrix}$$

Если по наивности мы решим воспользоваться методом Гаусса, то по индукции можно проверить, что преобразованиями Гаусса такую матрицу можно привести к блочному виду:

$$\left(\begin{array}{cc|cccccc} 1 & & & & & & & \\ & \ddots & & & & & & \\ & 1 & & & & & & \\ \hline & & n+2 & n+1 & & & & \\ & & 1 & 2 & 1 & & & \\ & & & 1 & 2 & 1 & & \\ & & & & 1 & 2 & 1 & \\ & & & & & & & \ddots \end{array}\right)$$

где левый угловой блок представляет собой тождественную $n \times n$-матрицу. И очень сильно неформально хочется сказать, что такую процедуру можно провести "бесконечное число раз" - и тогда матрица соотношений будет тождественной, а значит группа $G = 0$. Но в реальности же "порождающие", в которых матрица соотношений будет единичной, выглядят так:

$$y_n = x_n - nx_{n+1} - nx_{n+2}$$

и из этих соотношений восстановить $\{x_n\}$ по $\{y_n\}$ не очень-то получается: проблема, как я уже сказал, заключается в том, что невозможно провести обратные преобразования Гаусса, так как их нужно начинать с последнего шага, то есть с бесконечного, которого как такового и нету (хотя, как видите, матрица перехода в данном случае является даже треугольной - куда уж лучше).

С другой стороны, на наше везение в данной задаче то, что нам мешает - на самом деле сильно помогает: давайте выпишем все соотношения:

$$2x_1 + x_2 = 0$$

$$x_1 + 2x_2 + x_3 = 0$$

$$x_2 + 2x_3 + x_4 = 0$$

$$x_3 + 2x_4 + x_5 = 0$$

$$\cdots\cdots\cdots$$

и как видно каждое из этих соотношений можно воспринимать как выражение следующего порождающего через предыдущие (например из первого $x_2 = -2x_1$, из второго $x_3 = -2x_2 - x_1 = 3x_1$ и так далее). И фактически это означает, что группа порождается только x_1, на который нет никаких соотношений, а соотношения нужно воспринимать просто как обозначение специфических элементов и не более, либо просто как определение другого набора порождающих (строго можно использовать копредставления, и из свойства универсальности построить взаимно обратные гомоморфизмы $G \leftrightarrow \langle x_1 \rangle$, причем $x_1 \mapsto x_1$, а остальные порождающие переходят туда, куда им диктуют определяющие соотношения, к примеру $x_2 \mapsto -2x_1$, ясно, что при таком отображении соотношения переходят в соотношения). Причем отмечу, что для конечных матриц такое бы не сработало, так как на последнем шаге эта закономерность бы нарушилась - и вместо определения нового порождающего мы получили бы соотношения на предыдущие - и пришлось бы разбираться, как именно они через друг друга выражались. Иными словами в бесконечности не только минусы, но и плюсы. Таким образом $G \cong \langle x_1 \rangle \cong \mathbb{Z}$. И напомню, что применение метода Гаусса в лоб давало $G = 0$. Также из линейной алгебры, наверное, многие помнят, что определитель аналогичной конечной матрицы равен $n+1$, таким образом если рассмотреть соответствующую конечно-порожденную группу, то ее порядок как мы с вами отмечали будет равен модулю определителя, то есть $n + 1$ и опять-таки ничего общего с окончательным ответом.

==========

Задачи для самостоятельной работы

- *Изоморфны ли группы* $\mathbb{Z}_6 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$ *и* $\mathbb{Z}_{60} \oplus \mathbb{Z}_{10}$*?*
- *Сколько элементов порядка 2, 4 и 5 в группе* $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5$*?*
- *Разложить группу* A/B *в прямую сумму циклических (а также найти соответствующие канонические образующие), где* A *свободная абелева группа с базисом* x_1, x_2, x_3*, а* $B = \langle y_1, y_2, y_3 \rangle$*, причем*

$$\begin{cases} y_1 = 7x_1 + 2x_2 + 3x_3 \\ y_2 = 21x_1 + 8x_2 + 9x_3 \\ y_3 = 5x_1 - 4x_2 + 3x_3 \end{cases}$$

- *Доказать, что* $G = \langle a, b \,|a^7 b = b^7 a, ababa = babab \rangle$ *является нетривиальной.*
- *Обозначим* $\mathbb{Z}\left[\frac{1}{p}\right] = \left\{\frac{n}{p^k} : n, k \in \mathbb{Z}\right\} < \mathbb{Q}$*. Доказать, что*

$$\mathbb{Z}\left[\frac{1}{2}\right] \ncong \mathbb{Z}\left[\frac{1}{3}\right]$$

- *Пусть* A, B, C *конечно-порожденные абелевы группы. Доказать, что если выполнено* $A \oplus B \cong A \oplus C$*, то* $B \cong C$*. Верен ли этот факт для произвольных абелевых групп?*
- *Пусть* Λ *континуально. Верно ли, что*

$$\bigoplus_{\lambda \in \Lambda} \mathbb{Z}_4 \cong \prod_{n=1}^{\infty} \mathbb{Z}_4$$

Теорема Силова

Ключевой в этом разделе будет следующая теорема:

Теорема (Питера-Людвига Мейделля Силова)

Пусть $|G| = p^k m$, причем $(p, m) = 1$ и p - простое. Тогда

- *Существует $P < G$ с $|P| = p^k$ (такие подгруппы мы будем называть p-силовскими).*
- *Любая p-подгруппа вложена в некоторую силовскую.*
- *Для любых p-силовских подгрупп $P_1, P_2 < G$ существует g, что $g^{-1}P_1 g = P_2$ (иными словами все p-силовские подгруппы сопряжены).*
- *Пусть N_p - количество p-силовских подгрупп. Тогда*

1) $N_p = 1 + pq$ для некоторого q.

2) N_p является делителем m. Можно сказать большее: из орбитальной теоремы легко вытекает $N_p = \frac{|G|}{|N_G(P)|}$, где $N_G(P) = \{g \in G : gPg^{-1} = P\}$ - нормализатор некоторой p-силовской подгруппы $P < G$. Замечу, что $P < N_G(P)$.

Почти бесполезная для бесконечных групп, но невероятно мощная и эффективная для конечных групп. Вообще-то фамилию его автора правильно произносить как "Сюлов", но у нас обычно так не говорят (в принципе, у нас и Ляйбница обычно называют Лейбницем). В теореме условие на порядок подгруппы существенно: к примеру, мы знаем, что в A_4 нет подгрупп порядка 6. На самом деле зеленый пункт верен в более сильной формулировке: а именно в исходной группе есть подгруппа порядка $p^{k'}$ для любого $k' \leq k$, и часто теорему формулируют и доказывают в такой усиленной формулировке. Мы приведем идею доказательства, основанного для каждого пункта на рассмотрении некоторого действия и формулы орбит для него. Если $\Gamma \curvearrowright X$, причем $|\Gamma| = p^n$ для некоторого n, то:

$$|X| = |Fix(X)| \mod p$$

где $Fix(X)$ множество неподвижных точек: потому что X расслаивается на орбиты, одноэлементные - это в точности неподвижные точки, которые все вместе дадут вклад $|Fix(X)|$ в итоговую мощность, а мощности остальных орбит из орбитальной теоремы $|\operatorname{Orb}(x)| = \frac{|\Gamma|}{|\operatorname{St}(x)|}$ будут делиться на p, таким образом не будут давать вклада по модулю p - и для доказательства каждого пункта используется либо это следствие формулы орбит, либо орбитальная теорема. То, какое действие в каких пунктах используется, лаконично можно записать в следующей табличке (через $\operatorname{Syl}_p(G)$ мы обозначим множество всех p-силовских подгрупп группы G):

Утверждение	Действующая группа	Множество	Действие
для любого p существует силовская p-подгруппа	p-подгруппа H	G/H	лев. умножение
любая p-подгруппа вложена в силовскую	p-подгруппа H	G/H	лев. умножение
силовские сопряжены	p-силовская Q	G/P	лев. умножение
$N_p = 1 \mod p$	p-силовская P	$\operatorname{Syl}_p(G)$	сопряжение
m делится на N_p	G	$\operatorname{Syl}_p(G)$	сопряжение

Опишем идею доказательства: в первых пунктах, как отражено в табличке, для некоторой p-подгруппы H рассматриваем действие левым умножением $H \curvearrowright G/H$. На основании упомянутого выше следствия формулы орбит $|G/H| = |Fix(G/H)| \mod p$, причем $Fix(G/H) = \{gH : g \in N(H)\} = N(H)/H$.

Пусть $|H| = p^i$ и $i < k$, тогда $[G : H]$ делится на p, а значит и $|N(H)/H|$ делится на p, причем $H \lhd N(H)$, то есть $N(H)/H$ является группой. Тогда по теореме Коши в ней найдется элемент $x \in N(H)/H$ порядка p. Пусть $\pi : N(H) \to N(H)/H$ каноническая проекция, тогда $\pi^{-1}(x) = H \cup xH \cup \dots x^{p-1}H < N(H)$ подгруппа порядка p^{i+1}. Таким образом, стартуя с тривиальной группы, мы получаем цепь p-групп:

$$\{e\} < H_p < H_{p^2} < \ldots < H_{p^k} < G$$

Для доказательства сопряженности силовских p-подгрупп рассмотрим произвольные две силовские p-подгруппы Q и P и действие левым умножением $Q \curvearrowright G/P$. Из формулы орбит вытекает, что $|G/P| = |Fix(G/P)| \mod p$, но $|G/P|$ не делится на p. Значит существует неподвижная точка gP для этого действия, иными словами $qgP = gP$ для любого $q \in Q$. Простые алгебраические выкладки позволяют вывести из этого, что $Q = gPg^{-1}$.

Для доказательства того, что $N_p = 1 \mod p$ рассмотрим действие некоторой силовской p-подгруппы $P \curvearrowright \mathrm{Syl}_p(G)$ сопряжением. Опять из формулы орбит мы получаем, что $N_p = |Fix(\mathrm{Syl}_p(G))| \mod p$, если расписать, что значит для силовской p-подгруппы Q быть неподвижной точкой для этого действия, мы получим $P < N(Q)$, также ясно, что $Q \lhd N(Q)$. Таким образом P, Q - это две p-силовские подгруппы в $N(Q)$, которые по предыдущему пункту оказываются сопряженными, то есть $P = n^{-1}Qn$. Но так как $Q \lhd N(Q)$, то из свойств нормальных подгрупп мы получаем $P = Q$, иными словами неподвижная точка только одна, а значит $N_p = 1 \mod p$. С делимостью еще проще: так как все силовские p-подгруппы сопряжены, то действие $G \curvearrowright \mathrm{Syl}_p(G)$ сопряжением имеет только одну орбиту. А значит из орбитальной теоремы получаем, что мощность этой единственной орбиты $|N_p|$ делит $|G|$, но так как по предыдущему пункту $|N_p|$ и p является взаимно простыми, то $|N_p|$ делит и m. С другой стороны стабилизатор орбиты точки $P \in \mathrm{Syl}_p(G)$ есть просто $N(P)$, таким образом орбитальная теорема дает и $N_p = [G : N(P)]$.

В некотором смысле теорема Силова - это теорема Лагранжа в обратную сторону. Отмечу, что из оранжевого пункта о сопряженности любых силовских подгрупп в частности вытекает, что силовские подгруппы оказываются изоморфными. Это очень мощный результат: к примеру, для группы порядка $|G| = 7^2 \cdot 5 \cdot 3$ вы на основании теоремы сразу и задаром получаете, что любые две подгруппы порядка 49 обязаны быть изоморфными. Просто для p-подгрупп этот результат неверен: к примеру в S_4 есть подгруппы, изоморфные $\mathbb{Z}_4$ (подгруппа, порожденная циклом длины 4), и изоморфные $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (возьмите V_4).

В учебных задачах теорема Силова нужна главным образом для доказательства непростоты и разрешимости. Как для непростоты, так и для разрешимости (если доказывать с помощью критерия, а не через построение коммутационного ряда) - нужны нормальные подгруппы, и основной их источник базируется на следующем наблюдении:

$$\boxed{N_p = 1 \iff P \lhd G}$$

Факт этот почти очевиден: если $N_p = 1$, то gPg^{-1} для любого g тоже должна быть p-силовской подгруппой, в силу ее единственности совпадающей с P, что доказывает

нормальность. Если $P \lhd G$, то так как любые две силовские подгруппы сопряжены, то $P' = gPg^{-1}$ для любой p-силовской подгруппы при некотором g. Из условия нормальности получаем $P' = P$. Поэтому в задачах, где что-то нужно сказать про группу и дан только ее порядок - обычно пытаются вычислить N_p при разных p в надежде, что один из них будет равен 1, т.к. это дает нам нормальную подгруппу, которая, типично, упрощает задачу.

Как искать N_p?

• *В самых простых случаях хватает анализа N_p на делимость (про N_p мы знаем, что $N_p \equiv 1 \mod p$, а также N_p делит m).*

• *В более сложных - метод "ромашки", обсудим его на примере (суть его сводится к тому, что N_p при разных p одновременно не могут быть большими, так как силовские подгруппы при разных p пересекаются лишь по $\{e\}$, но при этом вместе должны уместиться в G).*

• *В самых сложных - вспоминаем про нормализатор и включаем творчество для других конструкций и оригинальных соображений.*

Задача

Доказать, что если $|G| = 35$, то G - абелева.

Имеем для 5-силовской подгруппы $P_5 \cong \mathbb{Z}_5$, так как 5 - простое число. По поводу количества N_5 силовских 5-подгрупп на основании только делимости можно сказать:

$$N_5 = 1, 6, 11, \ldots$$

и N_5 должно делить 7 (ясно, что числа большие 7 делить 7 не могут, а потому список не нужно продолжать дальше мультипликативного дополнения до степени соответствующего простого числа, иными словами если $|G| = p^k m$, то $N_p \leq m$) - этим двум условиям удовлетворяет только 1, значит $P_5 \lhd G$.

Аналогично для 7-силовских подгрупп: $P_7 \cong \mathbb{Z}_7$, $N_7 = 1, 8, \ldots$ но при этом N_7 должно делить 5, значит $N_7 = 1$, т.е. $P_7 \lhd G$.

Дальше нужно вспомнить обсуждения внутреннего прямого произведения, имеем $P_5 \cap P_7 = \{e\}$, так как нетривиальный элемент из пересечения по теореме Лагранжа должен иметь порядок 5 с одной стороны и порядок 7 с другой, таким образом $|P_5 \cdot P_7| = |P_5| \cdot |P_7| = 35$, значит по теореме о внутреннем прямом произведении:

$$G \cong P_5 \times P_7 = \mathbb{Z}_5 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_{35}$$

т.е. мы доказали не только абелевость, но и что исходная группа циклична.

Задача

Доказать, что если $|G| = pq$, где $p < q$ - простые числа, причем $q-1$ не делится на p - тогда $G \cong \mathbb{Z}_{pq}$.

Аналогично предыдущей задаче попытаемся найти количество силовских подгрупп: $N_q = 1, 1+q, 1+2q, \ldots$ причем N_q делит p. Так как $p < q$, то $N_q = 1$, причем $P_q \cong \mathbb{Z}_q$.

Далее $N_p = 1 + kp$, причем оно должно делить q. Так как q - простое, то у него 2 делителя: 1 и q. Ситуация $N_p = q$ невозможна из-за условия задачи на делимость, поэтому $N_p = 1$, а значит $P_p \lhd G$. Замечу, что из простоты p вытекает $P_p \cong \mathbb{Z}_p$.

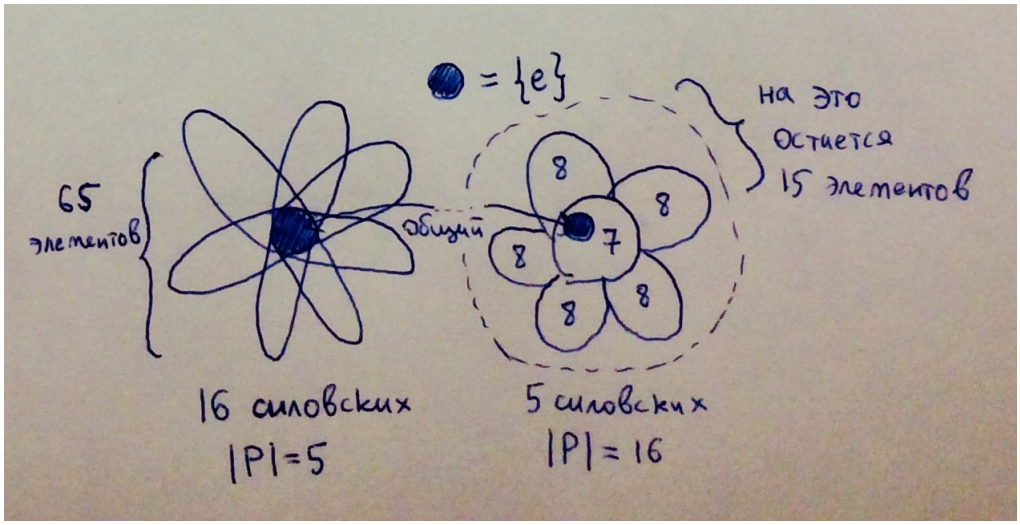
Из теоремы о внутреннем прямом произведении (аргументы возможности применения этой теоремы обсуждались в предыдущем примере и здесь остаются без изменений) получаем:

$$G \cong P_p \times P_q \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$$

Задача (на метод ромашки)

Доказать, что если $|G| = 80$, то группа G не является простой.

Источник нормальных подгрупп - это $N_p = 1$. Разложим порядок $80 = 2^4 \cdot 5$ и предположим, что группа является простой, т.е. не имеет нетривиальных нормальных подгрупп. Имеем $N_5 = 1, 6, 11, 16, \ldots$ причем должно делить 16. С учетом нашего предположения $N_5 = 16$. Далее $N_2 = 1, 3, 5, \ldots$ причем должно делить 5, опять-таки с учетом предположения получаем $N_2 = 5$. Посмотрим, как могут быть расположены силовские подгруппы в нашей группе: так как 5 простое число, то силовские 5-подгруппы пересекаются только по $\{e\}$, таким образом суммарно они дают вклад в виде $1+4\cdot 16 = 65$ элементов (1 - от единицы и 4 от каждого "лепестка" соответствующего некоторой силовской 5-подгруппе). Ясно, что 5-силовские и 2-силовские подгруппы могут пересекаться только по $\{e\}$ - это вытекает из теоремы Лагранжа. Таким образом за вычетом этих 65 элементов в группе остается лишь 15 элементов, которые в точности соответствуют неединичным элементам 2-силовской подгруппы - и на больше чем одну 2-силовскую подгруппу элементов не хватит (в общем случае, если бы теоретически мы хотели разместить 5 восьмиэлементных подгрупп, то меньше всего места они бы занимали в случае, если общая подгруппа была бы общей для всех, а не для каждой пары в отдельности; а также чтобы общая подгруппа была бы максимально большого порядка. С учетом этих замечаний для 5 силовских 8-подгрупп с учетом нейтрального элемента потребовалось бы зарезервировать как минимум $8 + 5 \cdot 8 = 48$ элементов). Таким образом, мы приходим к противоречию, а значит в исходной группе есть некоторая нетривиальная нормальная подгруппа, какая именно - сказать на основании этих рассуждений не получится.



Отмечу, что не всякий элемент обязан попасть в некоторую силовскую подгруппу, так как по теореме Лагранжа порядок элемента должен быть степенью простого числа, значит элемент порядка 6 никогда не попадет ни в какую силовскую подгруппу.

Задача

Доказать, что группа порядка 12 является разрешимой.

Имеем $12 = 2^2 \cdot 3$. Тогда $N_2 = 1, 3, 5, 7, 9, \ldots$ и делит 9, т.е. $N_2 = 1$ или $N_2 \geq 3$. Далее $N_3 = 1, 4, \ldots$, при этом должно делить 4, значит либо $N_3 = 1$, либо $N_3 = 4$. Если $N_2 = 1$, то $P_2 \lhd G$, и P_2 - разрешима, так как абелева (потому что раньше доказывали, что группа порядка p^2 обязана быть абелевой), и G/P_2 тоже разрешима, потому что имеет простой порядок, а значит циклична. Поэтому G тоже будет разрешима. Совершенно аналогично разбирается случай $N_3 = 1$. Поэтому предположим, что $N_3 = 4$ и $N_2 \geq 3$. Так как 3 - простое число, то силовские 3-подгруппы могут пересекаться только по $\{e\}$, тогда их пересечение будет состоять из 1 элемента, плюс каждая силовская подгруппа принесет с собой 2 новых элемента. Итого суммарно $1 + 2 \cdot 4$. Что касается силовских 2-подгрупп, то это подгруппы порядка 4, и меньше всего места они занимают если пересекаются по одной единственной подгруппе порядка 2 - если пересечение будет меньше, или подгруппа пересечения не общая - то получится больше элементов. Поэтому самый маленький вклад, какой внесут эти подгруппы - это $(2 - 1)$ от пересечения (вычитаем 1, потому что нейтральный элемент мы уже раньше учитывали) и $3 \cdot 2 = 6$ от лепестков (минимум подгрупп 3, каждая подгруппа приносит к их общему пересечению дополнительный вклад в $(4 - 2)$ элемента). В общем, ситуация похожая на ту, что изображена на картинке к предыдущей задаче. Таким образом в силовских подгруппах суммарно окажется самое малое элементов:

$$1 + 2 \cdot 4 + (2 - 1) + 3 \cdot 2 = 16$$

И все они не уместятся в исходной группе порядка 12 - мы приходим к противоречию.

Задача

Доказать, что группа порядка p^2q является разрешимой (p, q - простые числа).

Фактически, эта задача является обобщением предыдущей задачи.

Если $p = q$, то ранее мы доказывали, что такая группа даже нильпотентна.

Если $p > q$, то $N_p = 1, 1 + p, 1 + 2p, \ldots$ Так как N_p делит q и $q < p$, то получаем $N_p = 1$. Таким образом $P_p \lhd G$ - разрешима так как имеет порядок p^2, и G/P_p разрешима потому что циклична, значит по критерию разрешимости G - разрешима.

Если $p < q$, то $N_q = 1, 1 + q, 1 + 2q, \ldots$ и делит p^2. У p^2 только 3 делителя: $1, p, p^2$.

Если $N_q = p$, то мы приходим к противоречию, так как для отличного от единицы N_q выполнено $N_q \geq 1 + q \geq 1 + p$.

Если $N_q = p^2$, то так как q - простое число, то силовские q-подгруппы пересекаются только по 1, и каждая q-силовская группа дает вклад в $(q - 1)$ неединичных элементов. Таким образом все q-силовские подгруппы суммарно дадут вклад в $p^2(q - 1) = p^2q - p^2$ неединичных элементов. Остается лишь p^2 элементов, которых максимум хватит только на одну p-силовскую подгруппу. Таким образом в этом случае мы получаем $N_p = 1$, а этот случай ранее уже разбирался.

Если $N_q = 1$, то $P_q \lhd G$ - разрешимая подгруппа (потому что циклическая), и G/P_q тоже разрешимая, потому что имеет порядок p^2; таким образом G разрешима по критерию разрешимости.

Есть довольно много теорем, которые обеспечивают разрешимость группы при некоторых условиях на порядок, к примеру группы порядка: p^n, p^2q, pqr являются разрешимыми - желающие могут это доказать. Напомню, что по теореме Фейта-Томпсона любая группа нечетного порядка разрешима: это очень мощная и в то же время очень сложная теорема. Также известно, что A_5 - это единственная неразрешимая группа порядка p^2qr (здесь p, q, r - простые числа).

Задача

Доказать, что если $|G| = 255$, то группа G - циклична.

Разложим порядок на простые сомножители: $255 = 17 \cdot 5 \cdot 3$. Используя пункт делимости из теоремы Силова попытаемся найти количество силовских подгрупп. Анализ я всегда советую начинать с p, которые достаточно большие (чтобы множество $\{1, 1 + p, 1 + 2p, \ldots\}$ было маленьким), но при этом чтобы мультипликативное дополнение m было маленьким (чтобы у него было мало делителей; замечу, что маленькие m не всегда соответствуют большим p, к примеру для $2^5 \cdot 5$, маленькое $m = 5$ соответствует маленькому $p = 2$) - в этих случаях остается очень мало вариантов для возможных значений N_p. Учитывая это наблюдение - поиск начнем с $N_{17} = 1, 18, \ldots$, причем N_{17} должно делить 15. Единственным возможным вариантом остается $N_{17} = 1$, поэтому $P_{17} \cong \mathbb{Z}_{17}$ нормальна в G. Что касается N_5 и N_3, то из соображений делимости не получается так просто отсеять отличные от 1 случаи, а потому нужно найти другой подход (нормализаторы тут бессильны, так как группа задана только порядком и про структуру нельзя ничего сказать, ромашка здесь тоже не работает).

Рассмотрим $K = P_5P_{17}$, это будет подгруппой в G, так как $P_{17} \lhd G$; причем $K \lhd G$, так как индекс подгруппы равен 3, а мы ранее в разделе про действия доказывали, что подгруппа, индекс которой равен наименьшему простому делителю порядка

группы, обязательно является нормальной. Так как $|K| = 85$, то из теорем Силова нетрудно понять, что $K \cong \mathbb{Z}_{85}$, действительно, для уже ее силовских подгрупп верно $N_{17} = 1, 18 \ldots$ и делит 5, т.е. $N_{17} = 1$; и $N_5 = 1, 6, 11, 16, \ldots$ и делит 17 (числа большие 17 перебирать не нужно, т.к. они заведомо не являются делителями 17), т.е. $N_5 = 1$, из теоремы о внутреннем прямом произведении и простоты 5 и 17 заключаем:

$$K \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{17} \cong \mathbb{Z}_{85}$$

Из соображений мощности получаем, что $P_3K = G$ (т.к. $P_3 \cap K = \{e\}$). Докажем, что $P_3 \times K \cong P_3K$ причем изоморфизм задается формулой $(p, k) \mapsto pk$. Фактически нужно проверить, что $p_1k_1p_2k_2 = p_1p_2k_1k_2$, иными словами $p^{-1}kp = k$ для всех $p \in P_3$ и $k \in K$. Так как $K \lhd G$, то P_3 действует на K сопряжениями, обозначим это действие через $\pi : P_3 \to \mathrm{Aut}(K)$. Так как:

$$|\mathrm{Aut}(K)| = |\mathrm{Aut}(\mathbb{Z}_{85})| = \varphi(85) = \varphi(5)\varphi(17) = 4 \cdot 16 = 64$$

и так как образ группы порядка 3 должен быть делителем 64, то $\mathrm{Im}\,\pi = \{e\}$, иными словами действие π тривиально, что на уровне групповых элементов означает $k^{-1}pk = p$. Таким образом:

$$G = P_3K \cong P_3 \times K \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{85} \cong \mathbb{Z}_{255}$$

Задача

Докажите, что группа порядка 36 не является простой.

Раскладываем $36 = 2^2 \cdot 3^2$. Ни метод ромашки, ни условия на делимость не смогут довести решение задачи до победного конца. Рассмотрим следующее соображение: $N_3 = 1, 4, \ldots$ и должно делить 4, значит подходит только 1 и 4. Если $N_3 = 1$, то $P_3 \lhd G$ искомая нормальная подгруппа. Если $N_3 = 4$, то заметим, что сопряжением группа G действует на четырех-элементном множестве 3-силовских подгрупп (по теореме Силова любые две силовские подгруппы сопряжены, значит действие транзитивно). Обозначим это действие через:

$$\pi : G \to S_4$$

заметим,что $\ker \pi \neq G$, так как действие транзитивно, а значит в образе должны быть нетривиальные перестановки. А также $\ker \pi \neq \{e\}$, так как группа порядка 36 не может быть инъективно отображена на группу порядка 24. Таким образом $\ker \pi \lhd G$ искомая нетривиальная нормальная подгруппа.

Замечу, что группа порядка 36 обязана быть разрешимой, т.к. если рассмотреть найденную нетривиальную нормальную подгруппу $N \lhd G$, то нетрудно заметить, что как ее порядок, так и порядок G/N может быть лишь p^2q, либо p, либо p^2 - во всех этих случаях мы может гарантировать разрешимость N и G/N, таким образом по критерию разрешимости получаем разрешимость G.

Задача

Вычислите количество 2-силовских и 5-силовских подгрупп в A_5.

Условия на делимость - это не панацея, в конкретных группах зачастую эффективнее работают нормализатор и явное предъявление всех или некоторых подгрупп.

Раскладываем порядок на простые сомножители: $60 = 2^2 \cdot 3 \cdot 5$. Из теоремы Силова получаем $N_2 = 1, 3, 5, 7, 9, 11, 13, 15, \ldots$ и должно делить 15, таким образом остается довольно много вариантов. Заметим, что порядок 2-силовской подгруппы равен 4, и что мы можем сразу предъявить 5 силовских подгрупп: $V_4 < A_4 < A_5$, где $A_4 < A_5$ может вкладывается посредством выбора неподвижного элемента: таких способов, разумеется, 5. Совершенно неочевидно, есть ли другие способы "нестандартно" вложить V_4 в A_5.

Далее воспользуемся формулой через нормализатор: $N_2 = \frac{60}{|N(V_4)|}$, где $V_4 < A_5$ вкладывается стандартно. Заметим, что $A_4 < N(V_4)$ из-за $V_4 \lhd A_4$, таким образом $12 = |A_4| \leq |N(V_4)|$, а значит:

$$N_2 = \frac{60}{|N(V_4)|} \leq \frac{60}{12} = 5$$

Т.е. чем больше нормализатор одной фиксированной силовской подгруппы - тем меньше силовских подгрупп. Объединяя это неравенство с тем, что мы уже нашли 5 силовских подгрупп получаем $N_2 = 5$, иными словами V_4 может быть вложено в A_5 только стандартным способом.

Далее $N_5 = 1, 6, 11, \ldots$ и делит 12, т.е. подходит только 1 и 6. Случай 1 невозможен, т.к. A_5 простая и в ней не может быть нетривиальных нормальных подгрупп. Таким образом $N_5 = 6$. Давайте докажем это еще одним способом, отражающим важную связь *циклических силовских подгрупп* с *количеством элементов заданного порядка*. Заметим, что $P_5 \cong \mathbb{Z}_5$, а значит 5-силовских подгрупп столько, сколько циклических подгрупп порядка 5 в A_5. Так как 5 - простое число, то любые две такие подгруппы могут пересекаться только по нейтральному элементу, причем все нетривиальные элементы в $\mathbb{Z}_5$ имеют порядок 5. Таким образом каждая 5-силовская подгруппа дает вклад в виде 4 новых элементов порядка 5 (вспомните ромашку). Иными словами:

$$N_5 = \frac{\#\{x : \mathrm{ord}(x) = 5\}}{4}$$

Циклический тип элемента порядка 5 из A_5 состоит из одного цикла длины 5. Циклов длины n в S_n всего $\frac{n!}{n} = (n-1)!$ штук (первый элемент цикла выбирается n способами, второй $(n-1)$ способами и т.д., дальше нужно поделить на n, так как не имеет значения, с какого элемента вы цикл запустите). Таким образом получаем:

$$N_5 = \frac{4!}{4} = 6$$

Задача

Вычислить количество p-силовских подгрупп в $SL_2(\mathbb{Z}_p)$.

Так как матрица $g \in GL_2(F)$ iff ее столбцы образуют базис F^2, то

$$|GL_2(\mathbb{Z}_p)| = (p^2-1)(p^2-p)$$

в качестве первого базисного вектора можно взять любой ненулевой, для второго базисного вектора запрещена целая прямая, которая в этом случае состоит из p элементов. Далее $SL_2(\mathbb{Z}_p) = \ker\det$, и так как $\operatorname{Im}\det = \mathbb{Z}_p^*$ состоит из $(p-1)$ элементов, то по теореме о гомоморфизме имеем:

$$|SL_2(\mathbb{Z}_p)| = \frac{(p^2-1)(p^2-p)}{p-1} = p(p-1)(p+1)$$

Ясно,что $|P_p| = p$, причем мы можем явно предъявить одну из p-силовских подгрупп:

$$P = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{Z}_p \right\}$$

Попытаемся что-нибудь сказать про нормализатор: хотя в данном случае его нетрудно вычислить, но заведомо можно утверждать, что $P < N(P)$ и $\left\{ \begin{pmatrix} y & 0 \\ 0 & \frac{1}{y} \end{pmatrix} \right\}_{y \in \mathbb{Z}_p^*} < N(P)$, таким образом, рассматривая подгруппу, порожденную этими двумя подгруппами, получаем, что:

$$K = \left\{ \begin{pmatrix} y & x \\ 0 & \frac{1}{y} \end{pmatrix} \right\}_{x \in \mathbb{Z}_p, y \in \mathbb{Z}_p^*} < N(P)$$

В частности получаем, что $|N(P)| \geq |K| = p(p-1)$, таким образом:

$$N_p = \frac{p(p^2-1)}{|N(P)|} \leq \frac{p(p^2-1)}{p(p-1)} = p+1$$

Из пункта теоремы Силова про делимость вытекает $N_p = 1, 1+p, 1+2p, \ldots$. Так как $N_p = 1$ невозможно, из-за того, что P не является нормальной в G (либо можно привести очевидный пример второй силовской подгруппы $\left\{ \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \right\}$), то получаем, что $N_p = 1+p$. Задним числом мы получили, что $|N(P)| = |K|$, таким образом K - это не часть нормализатора, а весь нормализатор.

Замечание:

Кстати, $|SL_2(\mathbb{Z}_3)| = 24$ и возникает естественный вопрос, изоморфна ли эта группа S_4. Ответ отрицательный, так как у S_4 тривиальный центр, тогда как $Z(SL_2(\mathbb{Z}_3)) = \{I, 2I\}$, где I - единичная матрица. Отмечу, что $\det(2I) = 2^2 = 1$.

Спектр применения теоремы Силова в теории конечных групп нельзя описать словами, а потому приведу один пример за рамками стандартных задач:

Задача

Привести пример $\theta \in \mathrm{Aut}(S_6)$, не являющегося внутренним.

Ранее мы с вами обсуждали, что $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ при $n \neq 2, 6$. Существует множество способов построения автоморфизма S_6, не являющегося внутренним; но мы рассмотрим способ с помощью теоремы Силова. Отмечу, что $\mathrm{Out}(S_6) \cong \mathbb{Z}_2$, так что с точностью до подкрутки на внутренний автоморфизм построенный будет единственным автоморфизмом, не являющимся внутренним.

Заметим, что в S_5 всего 6 силовских 5-подгрупп (потому что они состоят из четных перестановок, а потому лежат в A_5, а количество силовских 5-подгруппы в A_5 мы уже ранее вычисляли). Таким образом возникает естественное действие сопряжениями на шести-элементном множестве силовских 5-подгрупп, которое мы обозначим через:

$$\pi : S_5 \to S_6$$

Заметим, что раз действие π транзитивно (ведь любые силовские подгруппы сопряжены, и в образе должны быть перестановки, переводящие заданную силовскую подгруппу в любую другую), то $|\operatorname{Im}\pi| \geq 6$, а значит $|\ker\pi| \leq \frac{120}{6} = 20$. Так как A_5 -простая, то нетрудно проверить, что A_5 - это единственная нетривиальная нормальной подгруппа S_5 (любая другая N должна содержать A_5, так как в противном случае $(N \cap A_5) \lhd A_5$, но по теореме Лагранжа между A_5 и S_5 нет промежуточных подгрупп). Таким образом, раз $|\ker\pi| \leq 20$, то $\ker\pi = \{e\}$, т.е. π является вложением. Особенность этого вложения в том, что оно транзитивно действует на 6-элементном множестве, в отличие от 6 стандартных вложений $S_5 \hookrightarrow S_6$, оставляющих неподвижным заранее выбранный элемент. Обозначим через $H = \operatorname{Im}\pi$ образ этого нестандартного вложения, имеем $[S_6 : H] = 6$, и рассмотрим действие S_6 левыми умножениями на смежных классах:

$$\theta : S_6 \to S(S_6/H) \cong S_6$$

Так как действие транзитивное, то $|\operatorname{Im}\theta| \geq 6$, и из-за того, что A_6 - это единственная нетривиальная нормальная подгруппа S_6, мы получаем, что θ - это вложение, и с учетом соображений мощности - θ является автоморфизмом. Докажем, что он не является внутренним: пусть для определенности $[H] = 6$ при отождествлении $S_6/H = \{1, 2, 3, 4, 5, 6\}$ и $S(S_6/H) \cong S_6$. Тогда нетрудно понять, что $\{g \in S_6 : gH = H\} = H$, иными словами для действия $S_6 \curvearrowright S_6/H$ выполняется $H = \mathrm{St}([H]) = \mathrm{St}(6)$, иными словами $\theta(H) = S_5 < S_6$, где вложение $S_5 < S_6$ стандартное в перестановки, оставляющие 6 неподвижной. То есть автоморфизм θ переводит нестандартно вложенную H в стандартно вложенную S_5, мы покажем, что это невозможно для внутреннего автоморфизма. Действительно, пусть для некоторого $\sigma \in S_6$ выполнено $\theta = \mathrm{Ad}_\sigma$, в таком случае $\sigma^{-1}H\sigma = S_5$, а значит:

$$H = \sigma S_5 \sigma^{-1} = \sigma\{\tau \in S_6 : \tau(6) = 6\}\sigma^{-1} = \{\tau \in S_6 : \tau(\sigma(6)) = \sigma(6)\}$$

иными словами, подгруппа H состоит в точности из перестановок, оставляющих неподвижным $\sigma(6)$, что соответствует стандартному вложению, тогда как по построению H - это образ нестандартного вложения $S_5 \hookrightarrow S_6$. Приходим к противоречию.

Замечание:

Если кратко описать идею доказательство - то произошло следующее: нестандартно вложенная $S_5 \cong H < S_6$, которая получена из действия сопряжением S_5 на множестве своих силовских 5-подгрупп, дает автоморфизм $S_6 \to S_6$, полученный действием уже S_6 левыми умножениями на S_6/H, и этот автоморфизм не может быть внутренним, так как он переводит нестандартно вложенную H в стандартно вложенную $S_5 < S_6$. Хотя, как мы отмечали, $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ при $n \neq 2, 6$, а потому область применения этого приема для построения автоморфизмов, не являющихся внутренними, очень ограничена; зато эта техника позволяет строить нестандартные вложения $S_k \hookrightarrow S_n$, если n - это количество силовских p-подгрупп группы S_k для некоторого p (любое такое действие будет транзитивным). Советую самостоятельно построить несколько таких вложений.

==========

Задачи для самостоятельной работы

- *Доказать, что любая группа порядка 185 коммутативна.*
- *Выяснить, чему изоморфна силовская 2-подгруппа группы $SL_2(\mathbb{Z}_3)$.*
- *Найти все силовские 2-подгруппы и 3-подгруппы группы A_4.*
- *Доказать разрешимость произвольной группы порядка 42.*
- *Доказать, что не существует простых групп порядка 200.*
- *Сколько элементов порядка 7 в простой группе порядка 168? Сколько в такой группе силовских 7-подгрупп?*

Аменабельные группы

Своему появлению аменабельные группы обязаны так называемому парадоксу Банаха-Тарского, который является не сколько парадоксом, сколько фактом, с существованием которого элементарной геометрической интуиции трудно смириться: а именно, что единичный шар в $\mathbb{R}^3$ можно разбить на 5 кусков, из которых можно "собрать" два единичных шара сдвигая куски движениями пространства, т.е. комбинациями сдвигов и вращений. Такая своеобразная магия как один шар превратить в два такого же радиуса. Причем изюминка и пафос этого факта в том, что два шара получаются именно движениями кусков, т.к. если движения заменить произвольными отображениями пространства - то этот факт становится очевидным, т.к. и шар, и пара шаров - континуальны, а значит между ними можно установить биекцию, которая легко продолжается до биекции всего пространства. Второй важный момент - это то, что конструкция Банаха-Тарского существенно использует аксиому выбора. И от этой зависимости никак не избавиться, так как если заменить аксиому выбора на ту же аксиому детерминированности - то любое множество будет измеримо по мере Лебега. И тогда простейшие операции с аддитивностью меры Лебега приведут к невозможности подобного разбиения шара (для простоты нормируем меру так, чтобы мера единичного шара была равна 1):

$$B = \bigsqcup_i X_i$$

$$1 = \mu(B) = \sum_i \mu(X_i) = 2\mu(B) = 2$$

И самое важное следствие этого парадокса: несуществование (при принятии аксиомы выбора) конечно аддитивной меры на $\mathbb{R}^3$ определенной на всех подмножествах, при этом нетривиальной и инвариантной относительно движений. Причем интересно, что на плоскости $\mathbb{R}^2$ такая мера существует и впервые была построена Банахом, а значит там такой парадокс нельзя реализовать (к сожалению, для построения этой меры нужно принятие аксиомы выбора).

И вот математики решили разобраться, в чем причина того, что в $\mathbb{R}^3$ такая аномалия есть, а в $\mathbb{R}^2$ ее нет. Ясное дело, что дело не в самих голых пространствах (потому что они - это лишь набор точек и равномощны, а значит неотличимы), а именно в группе их движений, т.к. инвариантную меру мы ищем именно относительно движений, и ключик к разрешению этой проблемы нашел фон Нейман (блестящий ученый, подаривший миру теорию алгебр фон Неймана, теорию игр, первую атомную бомбу и многое другое).

Сразу же отмечу, что в этой методичке мне больше хотелось бы сосредоточиться на именно групповых вопросах, по минимуму погружаясь в теорию меры. А потому во всем этом разделе без упоминания группы будут считаться **дискретными**, т.е. с тривиальной топологией. Даже при определении (а уж тем более при работе) с топологическими группами всплывает масса нюансов и тонкостей; и если моя методичка поможет разобраться хотя бы с дискретным случаем - уже будет очень хорошо.

Определение

Дискретная группа G называется аменабельной, если на ней существует конечно-аддитивная вероятностная инвариантная относительно сдвигов мера $m : 2^G \to \mathbb{R}^+$

То есть такую функцию, что:

$$m(X \sqcup Y) = m(X) + m(Y)$$

$$m(G) = 1$$

$$m(gX) = m(X)$$

Под 2^G мы имеем в виду множество всех подмножеств группы G. С теоретической точки зрения эта мера является очень удобным инструментом - так по этой мере интегрированием при желании можно усреднять величины и доказывать абстрактные теоремы, но в конкретных практических вопросах, где нужны явные вычисления, с этой мерой работать крайне сложно из-за ее неконструктивности (да и вообще ее существование сильно завязано на аксиому выбору): к примеру для счетных групп мы автоматически из инвариантности получаем, что мера любой точки (а значит и любого конечного множества) равна нулю, что как-то не

очень хорошо. Поэтому более удобным является эквивалентное определение через существование счетно-аддитивной меры, правда лишь почти инвариантной.

Что касается теории счетных аменабельных групп - то для них мотивационная роль теории меры идеологически не так сильна, и для них я бы привел следующий короткий подводящий к их теории сюжет: несмотря на то, что почти весь курс был посвящен конечным группам и несмотря на то, что их теория достаточно богата и многогранна (не так давно люди описали все простые конечные группы, дополнив известные списки нарушающими общие закономерности монстрами, но и вне классификации конечных простых групп вопросов больше чем ответов). И несмотря на это в большинстве математических сюжетов, непосредственно связанных с теорией групп, случай конечных групп как правило оказывается тривиальным: любую группу можно вложить в конечную группу перестановок, выписать конечную таблицу умножения, да и вообще на любой вопрос к конечной группе можно ответить конечным перебором, пусть даже по масштабам вычислений недоступным ни человеку, ни компьютеру. Приведу пример: групповая C^*-алгебра $C^*(G)$ конечной группы G является конечномерной алгеброй - а про них все известно, и они полностью классифицируются. И все же самая мякотка начинается там, где появляются бесконечные группы. И в некотором смысле хотелось бы оформить отдельным классом группы, по своим свойствам наиболее напоминающие конечные. Есть много подходов, но наиболее общепризнанный класс, который с одной стороны достаточно широк, а с другой больше других похож на конечные группы - это группы, для которых выполняется условие Фёльнера.

Определение

Будем говорить, что в G выполняется условие Фёльнера, если для всякого конечного множества $E \subset G$ и всякого $\varepsilon > 0$ существует конечное множество $F \subset G$, такое что:

$$\boxed{\max_{s \in E} \frac{|sF \triangle F|}{|F|} < \varepsilon}$$

Фёльнеровской последовательностью для группы G называется такая последовательность конечных множеств $\{F_n\}$, что $G = \bigcup_n F_n$, при этом $F_n \subset F_{n+1}$ и для любого $g \in G$ выполнялось бы:

$$\lim_{n \to \infty} \frac{|gF_n \triangle F_n|}{|F_n|} = 0$$

Здесь $\triangle$ - симметрическая разность. Фактически и очень-очень грубо: условие Фёльнера означает, что F похожа на почти подгруппу: с одной стороны замкнутость умножения внутри F заменяется на умножение на внешние элементы, но с другой стороны и сама замкнутость заменяется на почти-замкнутость: то есть сдвиги лишь малое количество элементов (относительно мощности $|F|$) выводят за рамки F (потому что симметрическая разность в точности состоит из выброшенных за борт элементов).

Что касается фёлноровских последовательностей - то в литературе нет общепризнанного определения, хотя все они приводят к эквивалентным определениям. К примеру, в некоторых источниках не требуют условия вложенности $F_n \subset F_{n+1}$, но и нетрудно из невложенной последовательности Фёлнера сделать вложенную: для этой цели рассмотрим произвольную последовательность

исчерпывающих конечных множеств $A_n \subset A_{n+1}$ с $G = \cup A_n$ и заметим, что из условия $|F_n| \to \infty$ вытекает, что если $\{F_n\}$ - фёльнерова, то и $\{F_n \cup A\}$ тоже фёльнерова для фиксированного конечного A. Теперь вложенную последовательность Фёлнера $\hat{F}_n$ строим рекуррентно следующим образом:

$$\hat{F}_1 = F_1$$

$$\hat{F}_2 = F_{n_2} \cup A_{m_2}$$

$$\hat{F}_3 = F_{n_3} \cup A_{m_3}$$

$$\dots\dots$$

Причем m_j мы выбираем таким образом, чтобы $A_{m_j} \supset \hat{F}_{j-1}$ - это можно сделать из-за исчерпываемости A_n и это обеспечивает $\hat{F}_j \supset \hat{F}_{j-1}$. А n_j будем выбирать так, чтобы своей массой F_{n_j} полностью забило только что выбранный A_{m_j}, и оно совершенно не чувствовалось в симметрической разности, а именно с использованием предельного соотношения выберем n_j так, чтобы с одной стороны:

$$\frac{|gF_{n_j} \triangle F_{n_j}|}{|F_{n_j}|} < \frac{1}{j}$$

для любого $g \in A_{m_j}$, а с другой стороны чтобы $|F_{n_j}|$ было существенно больше $|A_{m_j}|$. Построенные $\{\hat{F}_n\}$ будут искомыми вложенными фёльнеровскими множествами. Также отмечу, что если исходная последовательность $\{F_n\}$ не исчерпывала G, то новая последовательность $\hat{F}_n$ уже будет исчерпывающей, иными словами $\bigcup\limits_n \hat{F}_n = G$. Таким образом даже требование исчерпываемости в определении не обязательно.

Утверждение

Счетная группа G удовлетворяет условию Фёльнера $\Leftrightarrow$ она допускает последовательность Фёльнера.

$\Rightarrow$ Пусть $G = \{g_1, g_2, \dots\}$. Тогда нетрудно заметить, что F_n, построенные по $E = \{g_1, \dots, g_n\}$ и $\varepsilon = \frac{1}{n}$, являются фёльнеровской последовательностью. Для нее может не выполняться вложение $F_n \subset F_{n+1}$, также $\{F_n\}$ могут не исчерпывать G - но это можно исправить, используя упомянутое выше наблюдение.

$\Leftarrow$ Для любого $s \in E$ выполнено: $\lim\limits_{n\to\infty} \frac{|sF_n \triangle F_n|}{|F_n|} = 0$. Тогда для любого конечного множества E выполнено:

$$\lim_{n\to\infty} \max_{s\in E} \frac{|sF_n \triangle F_n|}{|F_n|} = 0$$

А значит для любого $\varepsilon > 0$ можно подобрать такое n, что $\max\limits_{s\in E} \frac{|sF_n \triangle F_n|}{|F_n|} < \varepsilon$. Это завершает доказательство.

Удивительно, но оказывается, что класс групп, для которых выполняется условие Фёльнера, в точности совпадает с классом аменабельных групп, то есть для работы с аменабельными группами это совпадение открывает фантастические возможности: с одной стороны можно пытаться решить задачу с помощью мер (с полным спектром всевозможных усреднений и интегрирований), а с другой - работать с множествами Фёльнера (и оперировать конечными аппроксимациями). По этому поводу в своей книжке Brown и Ozawa *"C^*-algebras and Finite-Dimentional Approximations"* авторы очень хорошо сказали, что существует около $10^{10^{10}}$ определений аменабельных групп

- эта говорящая шутка показывает как плотно аменабельные группы вросли в самые разные разделы математики, и что они могут появляться там, даже где их изначально никто не ждет: от ядерности групповых алгебр до неподвижных точек аффинных преобразований. Мы дадим не все, а лишь два эквивалентных определения для дискретных групп. Также отметим, что теорема, а значит и все последующие утверждения, зависят от аксиомы выбора. Я не хочу вдаваться в логику, а потому внимательному и неравнодушному к логике читателю предлагается в последующем изложении самостоятельно разобраться, для каких утверждений аксиома выбора нужна, а для каких - нет. Я лишь скажу, что зависимость от нее может быть в самых неожиданных местах: так как от аксиомы выбора в математике зависит намного больше утверждений, чем может изначально показаться. К примеру, от аксиомы выбора зависит теорема Хана-Банаха, а на ней строится почти весь функциональный анализ.

Теорема

Для произвольной (дискретной) группы G следующие условия эквивалентны:

1) G - аменабельна, т.е. допускает конечно аддитивную вероятностную инвариантную меру $m : 2^G \to \mathbb{R}^+$

2) В G выполняется условие Фёльнера.

В двух словах на уровне идей и без деталей опишу, откуда берется эта эквивалентность:

(1) $\Rightarrow$ (2) Если у вас есть мера $m : 2^G \to \mathbb{R}^+$ - то по ней естественным образом строится линейный функционал $\hat{m} : \ell^\infty(G) \to \mathbb{R}$, определенный на плотном множестве последовательностей $f = \sum_i f_i \chi_{G_i}$ с конечным множеством значений

$$\hat{m}(f) = \sum_i f_i m(G_i)$$

где $\{f_i\}$ конечное множество всех возможных значений f, а $G_i = f^{-1}(\{f_i\})$. Так как $\ell^1(G)$ плотно в $\ell^\infty(G)^*$ в *-слабой топологии, то $\hat{m}$ можно хорошо аппроксимировать элементами $\lambda \in \ell^1(G)$, представляющими собой почти инвариантные и законные счетно-аддитивные вероятностные меры на G (в отличие от конечно-аддитивной m; неотрицательной последовательности $\lambda \in \ell^1(G)$ соответствует мера $E \mapsto \sum\limits_{g \in E} \lambda(g)$).

С каждой такой аппроксимацией связываем конечное множество:

$$F(\lambda, n) = \left\{ g \in G : \lambda(g) > \frac{1}{n} \right\}$$

Правильно подбирая аппроксимацию λ и параметр n, среди них можно найти множество F для условия Фёльнера.

(2) $\Rightarrow$ (1) Чтобы лучше донести идею - рассмотрим лишь случай счетной G; тогда условие Фёльнера эквивалентно условию существования фёльнеровской последовательности F_n. И нам нужно построить меру $m : 2^G \to \mathbb{R}^+$. Для этого рассмотрим нормированные характеристические меры

$$m_n = \frac{1}{|F_n|} \chi_{F_n}$$

которые являются асимптотически инвариантными из определения фёльнеровских последовательностей (*почти инвариантность* - это когда для любого $\varepsilon > 0$

можно построить аппроксимацию, *асимптотическая инвариантность* - это последовательность некоторых почти аппроксимаций, таких что аппроксимационное соотношение для любого элемента (множества для мер, элемента групп для групповых соотношений и т.д.) стремится к 0 при $n \to \infty$, это очень близкие понятия, но все равно отличаются; в данном случае асимптотическая инвариантность означает, что $m_n(g \cdot M) - m_n(M) \to 0)$. Для получения инвариантной меры нужно перейти к пределу, но проблема в том, что предел $\lim_n m_n(M)$ не обязан существовать. Нельзя перейти к подпоследовательности, т.к. ее выбор должен будет зависеть от множества M; нельзя рассмотреть $\limsup_n m_n(M)$ так как мы потеряем аддитивность. Но на помощь нам приходит функциональный анализ и в частности теорема Банаха-Алаоглу о компактности единичного шара в *-слабой топологии, в частности последовательность $\{m_n\}$ единичного шара в $\ell^\infty(G)^*$ имеет предельную точку $\hat{m} \in \ell^\infty(G)^*$, которая является инвариантной относительно сдвига:

$$\hat{m}(g \cdot f) = \hat{m}(f)$$

из-за того, что последовательность m_n является асимптотически инвариантной, а именно из-за: $m_n(g \cdot f) - m_n(f) \to 0$ для любого $f \in \ell^\infty(G)$ (асимптотическая инвариантность вытекает из условия Фёльнера для F_n). Однако стоит отметить, что *-слабая топология на $\ell^\infty(G)^*$ очень сложная, в частности неметризуемая. Поэтому m не обязана являться пределом некоторой подпоследовательности m_{k_n}, и для доказательства инвариантности m нужны чуть более трудные и аккуратные выкладки со *-слабой топологией. Теперь конечно-аддитивную меру можно построить по формуле:

$$m(M) = \hat{m}(\chi_M)$$

Есть еще один способ построения предельной меры m, скажем так "для взрослых"; причем намного более конструктивный, так как он дает в некотором смысле "явную" формулу для m. На первом курсе изучается понятие предела последовательности $\lim\limits_{n\to\infty} a_n$ - эта функция сопоставляет ограниченным последовательностям некоторое называемое пределом число. Плюс этого подхода в том, что результат инвариантен относительно сдвига: то есть $\lim a_n = \lim a_{n+1}$, но существенный минус, что не у каждой ограниченной последовательности есть предел. Но есть другой подход к пределам - это *предел по ультрафильтрам*. Не буду вдаваться в подробности, в общем это способ по множеству $\mathcal{U} \subset 2^{\mathbb{N}}$ с некоторыми специфическими свойствами (называемому *ультрафильтром*) построить определенную на ограниченных последовательностях функцию:

$$\lim_{n\to\mathcal{U}} a_n$$

обладающую всеми (или почти всеми) свойствами пределов за той лишь разницей, что здесь теряется инвариантность относительно сдвига (т.е. типично, что $\lim\limits_{n\to\mathcal{U}} a_n \neq \lim\limits_{n\to\mathcal{U}} a_{n+1}$) и что у любой ограниченной последовательности есть предел. По определению $a = \lim\limits_{n\to\mathcal{U}} a_n$, если для любого $\varepsilon > 0$ выполнено

$$\{n : |a_n - a| < \varepsilon\} \in \mathcal{U}$$

Не так важно как предел зависит от выбора ультрафильтра $\mathcal{U}$, главное, что ультрафильтры существуют (и очень много, к примеру (принимая аксиому выбора), на $\mathbb{N}$ существует 2^c ультрафильтров, где c - континуум, однако если от аксиомы

выбора отказаться - ультрафильтров может не оказаться совсем). Конструкция ультрафильтров очень слабо осязаема (вживую ультрафильтры никто никогда не видел), а потому пределы по ним чаще всего используют когда нужен предел в теоретических задачах, нежели конкретные числовые характеристики последовательности (как, например, в нашей ситуации: когда нужен предел, чтобы для аменабельности группы доказать существование меры, а ее значение на конкретных множествах не особо нужно). Хорошо знакомым с функциональным анализом читателям ультрафильтры будет проще понять через призму изоморфизма $\ell^\infty(\mathbb{N}) \cong C(\beta\mathbb{N})$, где $\beta\mathbb{N}$ - пространство характеров $\ell^\infty(\mathbb{N})$, оно же Стоун-Чеховская компактификация пространства $\mathbb{N}$. Точки из нароста $\beta\mathbb{N}\backslash\mathbb{N}$ и являются в точности ультрафильтрами, и при этом:

$$\lim_{n\to\mathcal{U}} a_n = \hat{a}(\mathcal{U})$$

где $\hat{a} \in C(\beta\mathbb{N})$ соответствующая последовательности a_n при изоморфизме Гельфанда непрерывная функция - и предел в точности равен значению этой функции в точке $\mathcal{U}$ из нароста. Эта картина, в частности, позволяет понять, почему для предела по ультрафильтру выполняются все арифметические свойства предела, в частности $\lim\limits_{n\to\mathcal{U}}(a_n+b_n) = \lim\limits_{n\to\mathcal{U}} a_n + \lim\limits_{n\to\mathcal{U}} b_n$ - потому что фактически это просто значение функции в определенной точке. Отмечу еще, что всю эту теорию пределов по ультрафильтрам можно построить не только для $\mathbb{N}$, но и для любого пространства Ω, иными словами вычислять предел набора $(x_\omega)_{\omega\in\Omega}$, индексированного некоторым пространством, причем существование порядка на Ω не требуется.

Возвращаясь к нашим мерам и аменабельности, из асимптотически инвариантных мер m_n можно, выбрав предварительно произвольный ультрафильтр $\mathcal{U}$, получить меру как предел по этому ультрафильтру:

$$m(M) = \lim_{n\to\mathcal{U}} m_n(M)$$

для произвольного $M \subset G$. В некотором смысле этот подход эквивалентен подходу с применением теоремы Банаха-Алаоглу, но все же оформление и стиль немножко другие.

Замечание:

• *Отметим, что хотя мы не желая излишне погружаться в функциональный анализ привели лишь идеи доказательства, все же отметим, что если довести до идейного конца доказательство* $\Rightarrow$*, то получится, что конечно-аддитивные вероятностные меры на* G *находятся в естественном взаимно-однозначном соответствии с пространством состояний* $S(\ell^\infty(G))$*, по определению состоящим из таких* $\hat{m} \in \ell^\infty(G)^*$*, что* $\hat{m}(\chi_G) = 1$ *и* $\hat{m}(f) \geq 0$ *для всех* $f \geq 0$*. По такому состоянию* $\hat{m}$ *строится мера по формуле* $m(E) = \hat{m}(\chi_E)$*. И если есть мера - то строится определенное на плотном множестве функций с конечным числом значений* $f = \sum \alpha_i \chi_{E_i}$ *состояние* $\hat{m}(f) = \sum \alpha_i m(E_i)$*, которое может быть продолжено на все* $\ell^\infty(G)$*.*

• *Отметим лишний раз, что импликация* (2) $\Rightarrow$ (1) *верна и в несчетном случае, просто привычные последовательности нужно заменить направленностями, являющимися несчетным аналогом последовательностей. Интуитивно по свойствам они очень напоминают последовательности, и для них строится аналогичная теория, просто нужно аккуратно каждое утверждение передоказать или приспособить, если что-то меняется. Направленность определяется как*

$\{x_\lambda\}_{\lambda\in\Lambda}$, где индексы принадлежат частично упорядоченному множеству $(\Lambda, \leq)$. Фактически, наличие порядка позволяет перезаписать определение предела в этом обобщенном случае: $x = \lim\limits_{\Lambda} x_\lambda$, если для всякого $\varepsilon > 0$ найдется $\lambda_0 \in \Lambda$, такое что для всех $\lambda \geq \lambda_0$ выполнено $|x - x_\lambda| < \varepsilon$ - и по такой аналогии переносится очень многое. В нашем случае множества Фёльнера F параметризуются парами (ε, E) из вещественного положительного числа ε и конечного подмножества $E \subset G$, по которым они по определению строятся. На таких парах можно задать естественный частичный порядок: $(\varepsilon, E) \leq (\varepsilon_0, E_0)$, если $\varepsilon_0 < \varepsilon$ и $E \subset E_0$ (на эпсилоны должно быть именно такое условие, так как "бóльшим" по отношению к этому порядку значением должна соответствовать "меньшая окрестность", иными словами более обременительное условие).

Кратко резюмируем введение: аменабельные группы пришли из теории меры, и в недискретном случае все очень сложно. Но в дискретном случае аменабельность эквивалентна условию Фёльнера, которое в случае счетных групп эквивалентно существованию фёльнеровской последовательности.

Если очень неформально делить группы по степени сложности их структуры относительно конечных групп - то аменабельные группы это что-то вроде первого уровня обобщения конечных групп, хотя класс аменабельных групп очень богат и содержит далеко нетривиальные примеры. В английском языке аменабельные группы называются amenable groups, что в дословном переводе означает "послушные", "податливые", "сговорчивые"; но в русском языке дословный перевод никогда не используется.

Давайте на первых примерах посмотрим, насколько эти группы "податливы": самый просто пример - это *конечные группы*, которые все являются аменабельными. Для произвольной конечной группы G в этом можно убедиться как рассмотрев тривиальную последовательность Фёльнера $F_n = G$, так и построив инвариантную меру $m(A) = \frac{|A|}{|G|}$, где $|A|$ - количество элементов множества A.

Пример

Доказать, что $\mathbb{Z}$ является аменабельной группой.

Для тренировки докажем это двумя способами:

Через последовательность Фёльнера: искомыми фёльнеровскими множествами будут $F_n = \{-n, -(n-1), \ldots, n\} = [-n, n]$. Они очевидно конечные, вложенные и исчерпывают все $\mathbb{Z}$. Для проверки условия Фёльнера рассмотрим произвольное $m \in \mathbb{Z}$, и тогда в аддитивной записи получим при $n > m$:

$$\frac{|(m + F_n) \triangle F_n|}{|F_n|} = \frac{|[-n + m, n + m] \triangle [n, n]|}{|[-n, n]|} = \frac{2m}{2n + 1} \to 0$$

так как при каждом сдвиге отрезка $[-n, n]$ на 1 симметрическая разность увеличивается на 2, значит при сдвиге на m она увеличится на $2m$.

Через меры: для конечных отрезков $F_n = [-n, n]$ рассмотрим нормализованные считающие меры m_n, определяемые как:

$$m_n(A) = \frac{|A \cap F_n|}{|F_n|}$$

То, что F_n были фёльноровскими множествами, на языке мер означает, что меры m_n асимптотически инвариантны. Тогда в качестве искомой для аменабельности меры можно взять $m = \lim\limits_{n\to\mathcal{U}} m_n$ для некоторого ультрафильтра $\mathcal{U}$. Так как меры ограниченные, то этот предел всегда существует, аддитивность m вытекает из аддитивности m_n:

$$m(A \sqcup B) = \lim_{n\to\mathcal{U}} m_n(A \sqcup B) = \lim_{n\to\mathcal{U}} (m_n(A) + m_n(B)) = m(A) + m(B)$$

Заметим, что инвариантность достаточно проверять на порождающих группы, и для произвольного $A \subset \mathbb{Z}$ в аддитивной записи имеем:

$$m(1+A) = \lim_{n\to\mathcal{U}} m_n(1+A) = \lim_{n\to\mathcal{U}} \frac{|(1+A)\cap F_n|}{|F_n|} = \lim_{n\to\mathcal{U}} \frac{|A\cap F_n| + \delta_n}{|F_n|} = \lim_{n\to\mathcal{U}} m_n(A) + \lim_{n\to\mathcal{U}} \frac{\delta_n}{2n+1} = m(A)$$

$$\delta_n = \begin{cases} 0, \text{ если } -(n+1) \in A \text{ и } n \in A \\ 0, \text{ если } -(n+1) \notin A \text{ и } n \notin A \\ 1, \text{ если } -(n+1) \in A \text{ и } n \notin A \\ -1, \text{ если } -(n+1) \notin A \text{ и } n \in A \end{cases}$$

Значит $\lim\limits_{n\to\mathcal{U}} \frac{\delta_n}{2n+1} = \lim\limits_{n\to\infty} \frac{\delta_n}{2n+1} = 0$ (если существует обычный предел, то предел по любому ультрафильтру совпадает с этим классическим пределом). Таким образом полученная мера m является инвариантной.

Замечание:

- *Это естественно и нормально, если у вас остался осадочек из-за того, что через меры аменабельность такой простой группы как $\mathbb{Z}$ доказывается через такие сложные субстанции как ультрафильтры - но это такая специфика, что инвариантные меры почти никогда не получаются осязаемыми.*
- *Но несмотря на то, что меры в большинстве случае получаются очень абстрактными и неконструктивными - это не означает, что с ними вообще невозможно работать: даже несмотря на то, что ультрафильтры никто не видел - используя некоторые базовые свойства пределов можно явно вычислять меры некоторых конкретных множеств. Вернемся к последнему примеру группы $\mathbb{Z}$ и построенной на ней мере m. Пусть M - множество четных чисел. Тогда ясно, что $M \sqcup (1+M) = \mathbb{Z}$, из инвариантности меры получаем $m(M) = m(1+M)$, а значит:*

$$1 = m(\mathbb{Z}) = m(M \sqcup (1+M)) = m(M) + m(1+M) = 2m(M)$$

Таким образом $m(M) = 1/2$, причем ответ (как мы видим) совершенно не зависит от выбранного ультрафильтра.

Пример

Доказать, что $\mathbb{F}_2$ не является аменабельной группой.

Доказать отсутствие фёльнеровских множеств всегда практически невозможно - поэтому неаменабельность как правило доказывают построением "парадоксальных множеств", являющихся групповой версией парадокса Банаха-Тарского. Для построения таких множеств в $\mathbb{F}_2 = \langle a, b\rangle$ для начала рассмотрим для несократимого слова ω множество $W(\omega)$, состоящее из всех несократимых слов, начинающихся с ω. Тогда не так трудно заметить, что:

$$\mathbb{F}_2 = \{e\} \sqcup W(a) \sqcup W(b) \sqcup W(a^{-1}) \sqcup W(b^{-1}) = W(a) \sqcup aW(a^{-1}) = W(b) \sqcup bW(b^{-1})$$

Пусть группа $\mathbb{F}_2$ аменабельная, и m ее инвариантная мера. В силу инвариантности меры получаем:

$$m(W(a) \sqcup W(a^{-1})) = m(W(a)) + m(W(a^{-1})) = m(W(a) \sqcup aW(a^{-1})) =: x$$

$$m(W(b) \sqcup W(b^{-1})) = m(W(b)) + m(W(b^{-1})) = m(W(b) \sqcup bW(b^{-1})) =: y$$

Таким образом, если "навесить" меру на построенное парадоксальное разбиение мы получим:

$$1 = m(\{e\}) + x + y = x = y$$

Откуда вытекает, что $m(\{e\}) = x = y = 0$, а значит мы получили противоречие. Таким образом группа $\mathbb{F}_2$ является неаменабельной. Фактически мы выделили в группе 4 куска, двигая которые (с помощью левого умножения) нам удалось воссоздать две копии исходной группы, то есть парадокс Банаха-Тарского в чистом виде.

Следующее наблюдение нам понадобится в дальнейшем, но при этом мне не хочется слишком глубоко погружаться в теорию интегралов, поэтому вопрос построения интегралов на пространстве с мерой мы выносим за скобки.

Наблюдение

Пусть m - инвариантная относительно действия $G \curvearrowright X$ мера на X. Тогда

$$\int\limits_X f(x)dm = \int\limits_X f(gx)dm$$

Так как

$$\int\limits_X f(x)dm = \lim_{n\to\infty} \sum \frac{k}{n} m\left(\{x : f(x) \in I_{k,n}\}\right)$$

где $I_{k,n} = [\frac{k}{n}, \frac{k+1}{n}]$, то для

$$A = \{x : f(x) \in I\}$$

$$B = \{x : f(gx) \in I\}$$

легко заметить, что $B = g^{-1}A$, а значит $m(A) = m(B)$. Таким образом окончательно имеем:

$$\int\limits_X f(x)dm = \lim_{n\to\infty} \sum \frac{k}{n} m\left(\{x : f(x) \in I_{k,n}\}\right) = \lim_{n\to\infty} \sum \frac{k}{n} m\left(\{x : f(gx) \in I_{k,n}\}\right) = \int\limits_X f(gx)dm$$

В принципе, здесь должно быть мало удивительного: что если меры при сдвиге не меняются - то и интеграл не меняется, так как он есть всегда предел некоторых линейных комбинаций мер. И вот самое важное структурное утверждение про аменабельные группы:

Утверждение

- *Пусть G - аменабельна и $H < G$. Тогда H - тоже аменабельна.*
- *Пусть G - аменабельна и $H \lhd G$. Тогда G/H - аменабельна.*
- *Пусть H и G/H - аменабельны, где $H \lhd G$. Тогда G - аменабельна.*
- *Пусть $G = \bigcup G_i$, где $G_i < G_{i+1}$ и все G_i - аменабельны. Тогда G - аменабельна.*

---

1) Выберем представителя x_λ в каждом правом смежном классе по H и соберем из них множество $S = \{x_\lambda\}$. Из аменабельности на G имеется инвариантная мера m, тогда мера $\mu(A) = m(AS)$ будет искомой инвариантной мерой на H, а значит и H тоже аменабельна.

2) Любое отображение $X \to Y$ позволяет по мере на X построить так называемую "индуцированную" меру на Y. В нашем частном случае эпиморфизма $\pi : G \to G/H$ и инвариантной меры m на G можно построить меру ν на факторе:

$$\nu(A) = m(\pi^{-1}(A))$$

То, что ν является вероятностной мерой очевидно. Для проверки инвариантности заметим, что $\pi^{-1}(gH \cdot A) = g\pi^{-1}(A)$, где $gH \in G/H$. А значит

$$\nu(gH \cdot A) = m(\pi^{-1}(gH \cdot A)) = m(g\pi^{-1}(A)) = m(\pi^{-1}(A)) = \nu(A)$$

из-за инвариантности меры m.

3) Пусть μ - инвариантная мера на H, а ν - инвариантная мера на G/H. Для произвольного выбранного подмножества $A \subset G$ определим функцию

$$f_A(g) = \mu(H \cap g^{-1}A)$$

Нетрудно заметить, что из инвариантности μ для $h \in H, g \in G$ вытекает:

$$f_A(gh) = \mu(H \cap h^{-1}g^{-1}A) = \mu(h^{-1}(H \cap g^{-1}A)) = \mu(H \cap g^{-1}A) = f_A(g)$$

Иными словами функция f корректно определена на G/H так как она постоянна на классах смежности. Тогда искомой инвариантной мерой будет:

$$m(A) = \int\limits_{G/H} f_A(g)d\nu = \int\limits_{G/H} \mu(H \cap g^{-1}A)d\nu$$

Я специально выписал оба интеграла, так как в первом понятнее, что подынтегральная функция определена на G/H, а во втором визуально понятнее

зависимость полученной меры m от исходных μ и ν и от множества A. Так как любой интеграл - это линейный функционал, то m будет мерой, причем в данном случае очевидно вероятностной. Для проверки инвариантности воспользуемся предыдущим наблюдением про неизменность интеграла по инвариантной мере при сдвиге (здесь $q \in G$):

$$m(qA) = \int\limits_{G/H} \mu(H \cap g^{-1}qA)d\nu = \int\limits_{G/H} f_A(q^{-1}g)d\nu = \int\limits_{G/H} f_A(g)d\nu = m(A)$$

Таким образом построенная мера инвариантна, а значит группа G - аменабельна.

4) Для аменабельности группы G нужно для каждого конечного $E \subset G$ и $\varepsilon > 0$ построить конечное $F \subset G$, такое что

$$\max_{s \in E} \frac{|sF \triangle F|}{|F|} < \varepsilon$$

Из конечности E мы получаем, что $E \subset G_n$ для некоторого n. Тогда мы получаем F непосредственно из определения аменабельности для G_n.

Замечания:

• *Это утверждение чрезвычайно важное, и оно показывает, какие групповые конструкции не выводят за класс аменабельных групп. При проверке группы на аменабельность в первую очередь нужно попытаться воспользоваться этим утверждением: и спросить себя, могу ли я получить изучаемую группу с помощью этих конструкций из групп, аменабельность которых мне уже известна? Также это утверждение дает один из самых эффективных способов проверки на неаменабельность: если $\mathbb{F}_2 < G$ то ясно, что G - неаменабельна. И несмотря на невероятную простоту и кажущуюся примитивность этого наблюдения, многие десятилетия оставался открытым вопрос, а существуют ли вообще неаменабельные группы, не содержащие свободные группы в качестве подгруппы. Ответил на этот вопрос А.Ю. Ольшанский, доказавший в 1980 году существование и неаменабельность монстров Тарского: это бесконечные группы, каждая нетривиальная подгруппа которых изоморфна $\mathbb{Z}_p$ для некоторого простого p. Из этого описания ясно, что любой нетривиальный элемент этой группы имеет порядок p, и что группа эта порождена двумя элементами (потому что если взять произвольные нетривиальные a и $b \notin \langle a \rangle$, то в $\langle a, b \rangle$ будет как минимум $p+1$ элемент, а значит по определению эта подгруппа будет совпадать со всей группой). Ее существование как и неаменабельность - это сложные вопросы, но то, что она не содержит $\mathbb{F}_2$ - очевидно, так как в этой группе вообще нет элементов бесконечного порядка. Но повторюсь, это все исключительные ситуации: во многих случаях при проверке неаменабельности достаточно найти подгруппу изоморфную свободной; либо в чуть более сложных ситуациях - непосредственно для самой группы построить парадоксальное разбиение (как мы это делали в случае $\mathbb{F}_2$).*

• *Хотя прямое произведение $G \times H$ является частным случаем расширения G по H, покрываемое пунктом 3, все же в этом частном случае прямого произведения доказательство намного проще и прозрачнее: пусть G, H - аменабельны, а G_i, H_i - их соответствующие множества Фёльнера. Давайте убедимся, что $G_i \times H_i$ будут фёльнеровскими множествами для $G \times H$. Используя "неравенство треугольника*

для множеств" $A \triangle C \subset A \triangle B \cup B \triangle C$ для произвольного $(g,h) \in G \times H$ мы получим:

$$\frac{|(g,h)(F_n \times G_n) \triangle (F_n \times G_n)|}{|F_n \times G_n|} \leq \frac{|(g,h)(F_n \times G_n) \triangle (g,e)(F_n \times G_n)|}{|F_n \times G_n|} + \frac{|(g,e)(F_n \times G_n) \triangle (F_n \times G_n)|}{|F_n \times G_n|} =$$

$$= \frac{|(g,e)\left((e,h)(F_n \times G_n) \triangle (F_n \times G_n)\right)|}{|F_n \times G_n|} + \frac{|(g,e)(F_n \times G_n) \triangle (F_n \times G_n)|}{|F_n \times G_n|} =$$

$$= \frac{|F_n \times (hG_n \triangle G_n)|}{|F_n \times G_n|} + \frac{|(gF_n \triangle F_n) \times G_n|}{|F_n \times G_n|} = \frac{|hG_n \triangle G_n|}{|G_n|} + \frac{|gF_n \triangle F_n|}{|F_n|} \to 0$$

Что доказывает аменабельность $G \times H$.

• *Также отмечу, что хотя $G \times H$ является аменабельной при условии аменабельности прямых сомножителей - бесконечное произведение групп может не быть аменабельным даже при условии аменабельности сомножителей. Позднее мы с вами докажем, что $\mathbb{F}_2 \hookrightarrow \prod\limits_i F_i$ свободная группа вкладывается в бесконечное произведение конечных групп F_i. Конечные группы являются аменабельными, и если бы их произведение тоже было аменабельным, то тогда и свободная группа была бы аменабельной, что неверно. Хотя при этом если G_i аменабельны - то из четвертого пункта вытекает, что аменабельна и $G = \bigoplus\limits_n G_n$, т.к. $G = \bigcup\limits_n (G_1 \times \ldots \times G_n)$.*

Утверждение

Группа G является аменабельной тогда и только тогда, когда каждая ее конечно-порожденная подгруппа является аменабельной.

В одну сторону - очевидно, так как подгруппа аменабельной группы сама является аменабельной. Доказывая в обратную сторону опять вспомним, что для произвольных групп G аменабельность эквивалентна условию: для любого конечного $E \subset G$ и любого $\varepsilon > 0$ существует конечное $F \subset G$, что

$$\max_{s \in E} \frac{|sF \triangle F|}{|F|} < \varepsilon$$

и как нетрудно заметить, что раз конечно-порожденная группа $G_E = \langle E \rangle$ является аменабельной, то в ней можно найти искомое F. Грубо говоря, если любое условие (а не только аменабельности) записывается лишь на конечное число элементов, то для проверки его на всей группе достаточно проверять его на конечно-порожденных подгруппах.

Приведем для счетного случая второе доказательство, которое мне кажется весьма поучительным: воспользуемся идеями, лежавшими в основании доказательства четвертого пункта предыдущего утверждения. Пусть $G = \{g_1, g_2, \ldots\}$. Так как $G_n = \langle g_1, g_2, \ldots, g_n \rangle$ является аменабельной, то в ее последовательности Фёльнера G_n^i можно выбрать такой $F_n = G_n^{j(n)}$, чтобы:

$$\frac{|g_i F_n \triangle F_n|}{|F_n|} < \frac{1}{n}$$

для всех $i \leq n$. Нетрудно увидеть, что построенные F_n являются фёльнеровской последовательностью для G.

Владея теперь всеми этими свойствами можно собирать заслуженный урожай:

Примеры

- *Абелева группа является аменабельной*
- *Разрешимая группа является аменабельной*
- S_∞ *является аменабельной.*
- $SL_n(\mathbb{Z})$ *является неаменабельной при* $n \geq 2$.
- $\mathbb{F}_n$ *является неаменабельной при* $n \geq 2$
- $S(\mathbb{N})$ *является неаменабельной*

---

1) Так как по классификационной теореме любая конечно-порожденная абелева группа является прямой суммой конечных групп и $\mathbb{Z}$, то раз они аменабельны - то тогда и их прямая сумма тоже аменабельна. Ну а раз все конечно-порожденные подгруппы аменабельны, то и сама группа тоже аменабельна.

2) Докажем это по индукции по индукции: пусть это уже доказано для разрешимых групп ступеней вплоть до $n-1$ и пусть G - разрешимая группа ступени n. Тогда G - это расширение $[G,G]$ при помощи $G/[G,G]$, и здесь $G/[G,G]$ - является абелевой, а $[G,G]$ - разрешимая ступени не выше $n-1$, которая аменабельна по предположению индукции - значит по третьему пункту G аменабельна: так как расширения не выводят из класса аменабельных. Кстати, по ходу доказательства стало ясно, что для получения разрешимой группы ступени n понадобится n расширений тривиальной группы абелевыми.

3) Воспользуемся 4-ым пунктом: так как $S_\infty = \bigcup\limits_n S_n$, а все S_n - конечны (а значит аменабельны), то и S_∞ тоже будет аменабельной.

4) Ранее мы проверяли, что подгруппа $\left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle < SL_2(\mathbb{Z})$ изоморфна $\mathbb{F}_2$, а значит является неаменабельной. Тогда согласно первому свойству (подгруппа аменабельной является аменабельной) и вся группа $SL_2(\mathbb{Z})$ является неаменабельной. Так как $SL_2(\mathbb{Z}) < SL_n(\mathbb{Z})$ при $n \geq 2$ (вкладывается формулой $a \mapsto a \oplus 1$), то и $SL_n(\mathbb{Z})$ является неаменабельной.

5) Аналогично четвертому примеру, так как очевидно $\mathbb{F}_2 < \mathbb{F}_n$.

6) Заметим, что группа $S(\mathbb{N})$ всех перестановок существенно отличается от S_∞, состоящей лишь из перестановок с конечным носителем; например уже тем, что S_∞ - счетная, а $S(\mathbb{N})$ континуальная. В замечании к теореме Кэли мы с Вами выяснили, что любая счетная группа G может быть вложена в $S(\mathbb{N})$: достаточно рассмотреть действие левым умножением группы на себе $G \curvearrowright G$ и биективно отождествить $\mathbb{N}$ с G, рассматриваемое как "голое" множество с забытой групповой структурой; и мы получаем искомое вложение $G \hookrightarrow S(G) = S(\mathbb{N})$. В частности можно вложить неаменабельную $\mathbb{F}_2 \hookrightarrow S(\mathbb{N})$, а значит группа $S(\mathbb{N})$ тоже неаменабельна.

Замечания:

- *Напомню, что мы рассматриваем только дискретные группы, но оказывается, что в общем случае топологических групп все абелевы и разрешимые группы тоже являются аменабельными. Разрешимый случай, как мы уже поняли, сводится к абелевому. Доказательство аменабельности произвольной абелевой группы основывается на теореме Маркова-Какутани о неподвижной точке.*

- *Напомню, что нильпотентные группы являются разрешимыми, а потому и они тоже все будут аменабельными.*

• *Четыре доказанных выше свойства, которыми мы воспользовались - являются чрезвычайно эффективным методом проверки на аменабельность; и сложность задачи проверки группы на аменабельность фантастически возрастает, если они окажутся бессильными. Для иллюстрации этого упомянем, что в математике есть даже такое понятие как* **класс элементарно-аменабельные групп**, *который можно определить строго, но неформально он состоит из тех групп, которые можно получить из конечных и абелевых групп с помощью операций взятия подгруппы, бесконечного объединения и расширения группами из этого же класса. И долгое время вообще не было известно примера аменабельной группы, не являющейся элементарно-аменабельной, первый из которых был построен Р.Ю. Григорчуком лишь в 1984 году. Построенным контрпримером (который впоследствии стали называть группой Григорчука) является группа, порожденная 4 элементами, действующими довольно хитро на стандартном бинарном дереве. Кроме того, что это аменабельная группа, не являющаяся элементарно-аменабельной, у этой группы есть масса других удивительных свойств: например эта группа обладает промежуточной скоростью роста: то есть количество элементов в ее единичных шарах с ростом радиуса растет быстрее любого многочлена, но медленнее любой экспоненты.*

• *Проверка аменабельности иногда может быть простой, а иногда сложной задачей. Но для одной группы проверка аменабельности стала историей, достойной увековечивания в музыке и живописи. Речь идет о группе Томпсона кусочно-линейных гомеоморфизмов отрезка* $[0,1]$ *с изломами в двоично-рациональных точках и с производными, равными степеням двойки; группа эта допускает копредставление:*

$$F = \langle a, b | , [ab^{-1}, a^{-1}ba] = [ab^{-1}, a^{-2}ba^2] = e \rangle$$

и ее аменабельность является открытым вопросом по сей день (отмечу, что Томпсон исследовал три похожие группы $F < T < V$, *каждая из которых была группой некоторых кусочно-линейных гомеоморфизмов* $[0,1]$, *но связанные с* F *истории обычно самые интересные и захватывающие. Этим я хотел пояснить, почему эта группа логично не обозначается как* T *в честь его автора - просто группа* F *- это часть большей картины, где* T *тоже присутствует). История с этой группой чем-то мне напоминает историю с Великой Теоремой Ферма, так как и здесь тоже сочетается невероятная простота формулировки с колоссальной реальной сложностью по факту, ради этой группы ученые разрабатывают новые подходы как в теории групп, так и в смежных математических областях. Я знаю один сюжет в операторных алгебрах, который появился и развивался только лишь для проверки аменабельности группы Томпсона. Иногда в печать выходят статьи, где доказывается аменабельность этой группы, иногда статьи, где доказывается ее неаменабельность; но со временем в этих работах всегда на поверхность всплывали ошибки. Про группу эту известно очень многое, наверное, вообще все, что о ней нужно знать кроме лишь ее аменабельности, то есть кроме того, из-за чего эту группу вообще изучают.*

Работая с инвариантной мерой аменабельных групп довольно разумно спросить себя, а единственна ли она. Оказывается, что не единственна; и ответ этот на самом деле немного удивителен, учитывая, что для групп есть такое понятие как *мера Хаара*, по идеологии отдаленно напоминающая меру из определения аменабельности, но все равно существенно другая: она тоже инвариантная, но при этом счетно-

аддитивная и не вероятностная (часто мера всей группы равна бесконечности). Так вот на любой локально компактной группе существует единственная мера Хаара.

Пример

На $\mathbb{Z}$ существует по крайней мере две конечно-аддитивные вероятностные инвариантные меры.

Рассмотрим две последовательности множеств: $I_n = [0, n]$ и $F_n = [-n, n]$ (здесь $[a, b]$ все целые числа между a и b). Обе эти последовательности являются фёльнеровскими (с один небольшим "но", что первая последовательность является фёльнеровской в слабом смысле, когда не требуется, чтобы их объединение покрывало всю группу. Но если хочется чистой фёльнеровской последовательности, то первую можно заменить на что-то вроде $\tilde{I}_n = [-\lfloor\sqrt{n}\rfloor, n]$). По этим отрезкам мы строим соответствующие меры: $m_n = \frac{1}{|I_n|}\chi_{I_n}$ и $h_n = \frac{1}{|F_n|}\chi_{F_n}$. Рассмотрим произвольный ультрафильтр $\mathcal{U}$ на $\mathbb{N}$. Тогда из условия Фёльнера вытекает инвариантность предельных мер $m = \lim\limits_{n\to\mathcal{U}} m_n$ и $h = \lim\limits_{n\to\mathcal{U}} h_n$. Докажем, что эти меры различны.

Рассмотрим множество $M = \mathbb{N}$. Используя замечание, что если классический предел существует, то он равен пределу по ультрафильтру; а также то, что $m_n(M) = 1$ и $h_n(M) = \frac{n}{2n+1}$, мы получаем: $m(M) = 1$ и $h(M) = \frac{1}{2}$. Таким образом эти меры различны.

Замечание:

Если копать поглубже: то основным идейным ядром было построение мер, одна из которых "расходится" в обе стороны, а вторая - только вправо. На самом деле это не изолированный красивый хитрый прием - а часть большой теории, изучающей так называемые "границы групп", которые отвечают за то, что представляет из себя группа "на бесконечности". Существует очень много разных границ, каждая из которых нужна для своих задач: к примеру, граница Фюрстенберга (главным образом связанная с вопросами интегрирования на группах, но в последнее время нашедшая неожиданное применение в вопросах, связанных с простотой редуцированной групповой C^*-алгебры $C^*_r(G)$), или граница Громова для гиперболических групп, которой мы коснемся в следующей главе, и которая фактически является множеством неких классов эквивалентности уходящих в бесконечность путей на группе, для которой задана система порождающих, а потому для которой можно построить граф Кэли и воспринимать группу как метрическое пространство. К примеру, у $\mathbb{Z}$ граница Громова состоит из двух точек, соответствующих $+\infty$ и $-\infty$. В общем случае граница Громова представляет из себя некоторое компактное пространство, отвечающее за качественные геометрические свойства групп асимптотического характера. Типично, что границы всплывают в сюжетах, находящихся на стыке теории групп, функционального анализа и теории динамических систем.

Лично для меня аменабельные группы особенно удивительны тем, что они каким-то непостижимым образом притягивают к себе сюжеты из смежных для теории групп областей, и всплывают в математике там, где их появление не очень-то ожидаемо.

Первый сюжет, где появление аменабельных групп вот прямо на чудо не похоже, но все равно очень интересно и любопытно. Пусть задана конечно-порожденная группа $G = \langle S|R\rangle$ с симметричным набором порождающих $S = \{a_1, \ldots, a_n\}$ (это означает, что если в списке порождающих есть a, то есть и a^{-1} - это предположение удобно, так как не придется каждый раз оговариваться, что при вычислении длины слова за элементарный символ считается как порождающий элемент, так и его обратный). Длиной $\omega \in G$ относительно S мы назовем такое минимальное n, что $\omega = s_1 \ldots s_n$, где $s_i \in S$. *Функцией роста* группы G относительно порождающего набора S мы будем называть функцию $\gamma_S(n) = |B_S(n)|$, где $B_S(n) = S^n = \{a_1 \cdot \ldots \cdot a_n : a_i \in S\}$ - единичный шар графа Кэли радиуса n. Чтобы стало понятнее - рассмотрим 2 стандартных примера: в случае $\mathbb{Z}^2 = \langle a, b|[a, b] = 1\rangle$ ($S = \{a, a^{-1}, b, b^{-1}\}$) имеем $B_S(n) = \{a^j b^i : |i| + |j| \leq n\}$, а значит:

$$\gamma_S(n) = 1 + 4 + 8 + \ldots + 4(n + 1) = 1 + 2n(n + 1)$$

Второй пример: группа $\mathbb{F}_2 = \langle a, b\rangle$ (здесь $S = \{a, a^{-1}, b, b^{-1}\}$). Можно ограничиться только несократимыми словами (так как если сократимое слово лежит в шаре, то результат его сокращения лежит в шаре даже меньшего радиуса), нулевой длины существует всего одно пустое слово, соответствующее нейтральному элементу; все же остальные несократимые слова могут начинаться с любой из четырех букв, а для каждой последующей буквы всего существует три возможности (так как обратная к предыдущей запрещена, ибо она породит сокращение). Таким образом

$$B_S(n) = \{\text{несократимые } \omega \text{ длины} \leq n\}$$

$$\gamma_S(n) = 1 + 4 + 4 \cdot 3 + \ldots + 4 \cdot 3^{n-1} = 1 + 2(3^n - 1)$$

Фактически, функция роста показывает с какой скоростью группа разрастается при последовательном перемножении порождающих элементов: в свободной группе нет нетривиальных соотношений и шары разрастаются экспоненциально в виде деревьев. В $\mathbb{Z}^2$, напротив, многочисленные коммутационные соотношения склеивают многие элементы и вместо полного дерева у нас остаются ромбы, разрастающиеся лишь с полиномиальной скоростью. Неформально говоря, в шарах тем меньше элементов, чем больше в группе соотношений; а потому функция роста в некотором смысле отвечает и за количество соотношений: чем функция роста быстрее - тем соотношений асимптотически меньше. Отмечу, что функция роста не может расти слишком быстро и ее скорость для группы $G = \langle S, R\rangle$ ограничена функцией роста для соответствующей свободной группы $\mathbb{F}_{|S|/2} = \langle S\rangle$, так как в шаре группы без соотношений элементов всегда больше, чем в группе с соотношениями, склеивающими некоторые элементы (здесь мы делили пополам, так как мы договорились, что в S порождающие идут парами - элемент и его обратный). Таким образом для любой группы имеем:

$$\gamma_S(n) \leq 1 + |S|\left(1 + (|S| - 1) + \ldots + (|S| - 1)^{n-1}\right) = 1 + |S| \cdot \frac{(|S| - 1)^n - 1}{|S| - 2}$$

Иными словами быстрее экспоненты функции роста расти никак не могут.

Однако функция роста не является характеристикой группы, так как она существенно зависит от порождающего множества S. Чтобы это исправить вводят следующее отношение эквивалентности: будем писать $f \precsim g$, если существует $C > 0$,

такое что $f(n) \leq g(Cn)$. Тогда функции будем называть *эквивалентными* $f \sim g$, если $f \precsim g$ и $g \precsim f$. Фактически, это отношение эквивалентности определяет как функция растет качественно, и, возможно, это отношение излишне грубо: хотя все многочлены одной степени эквивалентны, а разных - неэквивалентны, что в принципе хорошо, так как в таком случае степень этого многочлена является инвариантом группы; однако $a^n \sim b^n$ для любых $a, b > 1$, и основание показательной функции роста инвариантом группы уже не является. Но хоть что-то - это лучше чем ничего.

Утверждение

Для двух порождающих множеств S и T конечно-порожденной группы выполнено $\gamma_S \sim \gamma_T$, иными словами класс эквивалентности функций роста является инвариантом группы и никак не зависит от порождающего множества.

Действительно, рассмотрим такое C, что $S \subset B_T(C)$ и $T \subset B_S(C)$, то есть C - это количество букв, которое достаточно, чтобы порождающие одного множества записать через порождающие второго множества. Тогда нетрудно понять, что если $\omega \in B_T(n)$, и каждый порождающий из T в этом слове можно записать словом длины не больше C в алфавите S, то получится слово в алфавите S длины не больше Cn. Таким образом $\gamma_T(n) \leq \gamma_S(Cn)$. И дословно повторяя эти рассуждения, поменяв порождающие множества, мы получаем $\gamma_S(n) \leq \gamma_T(Cn)$. Таким образом $\gamma_S \sim \gamma_T$.

По скорости роста функции роста выделяют следующие классы группы:

• Группы полиномиального роста: если $\gamma_S(n) \leq n^\alpha$ для некоторого α

• Группы экспоненциального роста: если $\gamma_S(n) \sim a^n$ для некоторого $a > 1$ (а значит и для любого $a > 1$, как мы уже выясняли: все экспоненты эквивалентны).

• Группы промежуточного роста: это группы не входящие в два описанных выше класса.

• Если группа имеет либо полиномиальный, либо промежуточный рост - то такую группу обычно называют *группой субэкспоненциального роста*. Нетрудно понять, что группа имеет субэкспоненциальный рост $\Leftrightarrow \limsup\limits_{n\to\infty} \sqrt[n]{\gamma_S(n)} = 1$ для некоторого конечного порождающего множества S.

Замечания:

• *Из субмультипликативности $\gamma_S(n)$ вытекает, что предел $\lim\limits_{n\to\infty} \sqrt[n]{\gamma_S(n)}$ всегда существует. Доказательство этого факта не очень сложное, но все равно я предпочту его обойти стороной, и это наблюдение не использовать.*

• *М.Л. Громов доказал, что конечно-порожденная группа имеет полиномиальный рост $\Longleftrightarrow$ она почти нильпотентна, т.е. обладает нильпотентной подгруппой конечного индекса. Используя эту характеризационную теорему можно доказать, что если $\gamma_S(n) \leq n^\alpha$ для некоторого α, то $\gamma_S(n) \sim n^\beta$ для некоторого натурального β. Иными словами в случае групп полиномиального роста, степень многочлена роста которых априори может быть дробной - задним числом оказывается, что такого быть не может - и функция роста эквивалентна настоящему многочлену. Логично будет спросить: является ли она чистым многочленом или только эквивалентна ему? Не знаю, насколько для вас ответ будет ожидаем, но даже в самых простейших случаях степень роста может быть далеко не многочленом. К примеру, если рассмотреть $\mathbb{Z} = \langle a \rangle$ в мультипликативной форме и рассмотреть систему порождающих $S = \{a, a^{-1}, a^3, a^{-3}\}$, то после нетрудных и непродолжительных комбинаторных*

усилий мы получим, что:

$$\gamma_S(n) = \begin{cases} 1, n = 1 \\ 5 + 6(n-2), n \geq 2 \end{cases}$$

Ясно, что эта функция не является линейной (если бы она была линейной, то должно быть $\gamma_S(1) = 5 + 6 \cdot (1-2) = -1$*). Еще один показательный и иллюстративный пример - это конечная группа, функция роста для которой ограничена. Она должна быть эквивалентна многочлену нулевой степени, то есть константе, но ясно, что она не является постоянной.*

• *Но экзотическими бывают не только сами функции роста, но и классы эквивалентностей по скорости. К примеру вышеупомянутая группа Григорчука относится к классу групп промежуточного роста, причем ее скорость роста заключена между* $e^{\sqrt{n}}$ *и* $e^{n^{0,991}}$*. И лишь в 2018 году ученые смогли найти более точные оценки для ее скорости роста, а именно они доказали существование предела:* $\lim\limits_{n\to\infty} \frac{\ln \ln \gamma(n)}{\ln n} = \alpha \approx 0,7674$*, иными словами очень грубо, но можно считать, что ее скорость роста равна* $e^{n^{0,7674}}$*. Сейчас нашли много других групп, похожих на группу Григорчука, с экзотической функцией роста вида* e^{n^α}*, однако во всех существующих примерах* $\alpha > 1/2$*. Математики даже предположили, что эта 1/2 возникла не просто так, и за ней стоит глубокий смысл; поэтому была выдвинута гипотеза (называемая "Gap conjecture"), утверждающая, что если* $\gamma_S(n) \precsim e^{\sqrt{n}}$*, то* G *- полиномиального роста. Иными словами, что среди промежуточных функций роста есть огромная дыра: то есть многочлены и* $e^{\sqrt{n}}$ *разделяет звенящая пустота.*

И вот теперь, когда понятие функции роста групп нам стало немного ближе, мы готовы осознать связь аменабельности с функциями роста:

Задача

Пусть G *- конечно-порожденная группа субэкспоненциального роста. Тогда* G *- аменабельна.*

В принципе, условие конечно-порожденности группы излишне, так как для бесконечно-порожденных групп вообще отсутствует понятие скорости роста. Мы покажем, что некоторая подпоследовательность последовательности всех шаров группы $F_n = B_S(n)$ является последовательностью Фёльнера, что достаточно для проверки аменабельности G.

Сперва сделаем полезное замечание, относящееся не только к этой задаче, но и ко всем аменабельным группам в целом, что на основе элементарных теоретико-множественных выкладок (диаграммы Эйлера - самый простой путь к подобным результатам), что для любых двух множеств A, B выполнено:

$$|A \triangle B| + 2|A \cap B| = |A| + |B|$$

Отсюда легко вытекает, что (если подставить $A = gF_n$ и $B = F_n$):

$$\frac{|gF_n \triangle F_n|}{|F_n|} = 2 - 2\frac{|gF_n \cap F_n|}{|F_n|}$$

Таким образом стандартное условие Фёльнера оказывается эквивалентно:

$$\lim_{n\to\infty} \frac{|gF_n \cap F_n|}{|F_n|} = 1$$

о котором полезно не забывать, так как иногда удобнее работать с пересечениями, а иногда с симметрическими разностями.

Второе полезное наблюдение общего характера: что если мы проверяем аменабельность группы, порожденной множеством S, то условие Фёльнера достаточно проверять не на всех элементах, а только на порождающих. Для проверки этого воспользуемся неравенством треугольника для симметрической разности: пусть S - симметричное множество порождающих, и для простоты восприятия докажем по индукции: пусть мы уже доказали условие Фёльнера для слов длины не больше $n-1$. Докажем для произвольного слова c длины n, которое можно представить в виде $c = ba$, где b слово длины не больше $n-1$, а a - некоторый порождающий (иными словами слово длины 1). Тогда:

$$\frac{|cF_n \triangle F_n|}{|F_n|} \leq \frac{|baF_n \triangle bF_n|}{|F_n|} + \frac{|bF_n \triangle F_n|}{|F_n|} = \frac{|aF_n \triangle F_n|}{|F_n|} + \frac{|bF_n \triangle F_n|}{|F_n|} \to 0$$

последнее равенство выполняется в силу $baF \triangle bF = b(aF \triangle F)$.

Вернемся теперь к исходной задаче, пусть $F_n = B_S(n)$ шар группы субэкспоненциального роста, будем как всегда считать, что S - симметричное (т.е. если $a \in S$, то и $a^{-1} \in S$). Из определения ясно, что для любого порождающего $g \in S$ выполнено $gF_{n-1} \subset F_n$, и что $F_{n-1} \subset F_n$. Таким образом: $gF_n \cap F_n \supset gF_n \cap gF_{n-1} = gF_{n-1}$. А значит:

$$1 = \frac{|F_n|}{|F_n|} \geq \frac{|gF_n \cap F_n|}{|F_n|} \geq \frac{|gF_{n-1}|}{|F_n|} = \frac{|F_{n-1}|}{|F_n|}$$

Из теории степенных рядов вспомним, что для любой последовательности $a_n > 0$ выполняется:

$$\liminf_{n\to\infty} \sqrt[n]{a_n} \geq \liminf_{n\to\infty} \frac{a_n}{a_{n-1}}$$

Таким образом, объединяя наши наблюдения с этой формулой из математического анализа, полагая $a_n = |F_n|$, мы получаем для каждого $g \in S$:

$$1 \geq \limsup_{n\to\infty} \frac{|gF_n \cap F_n|}{|F_n|} \geq \limsup_{n\to\infty} \frac{|F_{n-1}|}{|F_n|} = \frac{1}{\liminf_{n\to\infty} \frac{|F_n|}{|F_{n-1}|}} \geq \frac{1}{\liminf_{n\to\infty} \sqrt[n]{|F_n|}} \geq \frac{1}{\limsup_{n\to\infty} \sqrt[n]{|F_n|}} = 1$$

Иными словами:

$$\limsup_{n\to\infty} \frac{|gF_n \cap F_n|}{|F_n|} = 1$$

Так как S - конечное множество, то

$$\limsup_{n\to\infty} \left(\max_{g\in S} \frac{|gF_n \cap F_n|}{|F_n|} \right) = 1$$

Таким образом раз $\limsup = 1$, то существует некоторая подпоследовательность F_{k_n}, для которой:

$$\lim_{n\to\infty} \left(\max_{g\in S} \frac{|gF_{k_n} \cap F_{k_n}|}{|F_{k_n}|} \right) = 1$$

Объединяя этот факт с наблюдением, что условие Фёльнера можно эквивалентно переписать через пересечения, и что его достаточно проверять на порождающих -

мы получаем, что F_{k_n} удовлетворяют условию Фёльнера в группе G, что доказывает ее аменабельность.

Замечание:

Как я уже писал выше: так как $|F_{n+m}| \leq |F_n||F_m|$ *- то предел* $\lim\limits_{n\to\infty} \sqrt[n]{|F_n|}$ *всегда существует. Из этого факта вытекает очень важное наблюдение: что в случае групп субэкспоненциального роста последовательность шаров является фёльнеровской последовательностью без необходимости перехода к подпоследовательностям (так как тогда бы в доказательстве все* $\limsup$ *и* $\liminf$ *заменились на* $\lim$*).*

Такжже, ставя этот результат в один ряд с теоремой Громова о том, что полиномиальный рост является критерием почти нильпотентности, может сложиться впечатление, что скорость роста группы связана со сложностью структуры группы, и что группы экспоненциального роста без вариантов должны быть максимально неаменабельными, а пример $\mathbb{F}_2$ *должен нас лишь укрепить в этом предположении: но это не так; и импликация только что доказанного утверждения в обратную сторону не работает. То есть если рост группы маленький - то группа имеет простую структуру, но бывают и быстрорастущие группы с очень простым строением (хотя и не настолько простым, чтобы попадать под условие теоремы Громова). И для приведения классического контрпримера нам понадобится немножко обогатить наши познания в комбинаторной теории групп:*

Определение

Сплетением групп G, H *(wreath product на английском языке) называется группа:*

$$G \wr H = \bigoplus_{h\in H} G \rtimes H$$

где полупрямое произведение определяется действием H *на* $\bigoplus\limits_{h\in H} G$ *сдвигом по индексу, т.е.* $\phi : H \to \mathrm{Aut}\left(\bigoplus\limits_{h\in H} G\right)$ *и* $\phi_h((g_\omega)_{\omega\in H}) = (g_{h^{-1}\omega})_{\omega\in H}$.

Существует еще понятие полного сплетения (unrestricted wreath product, обозначается $G \wr\wr H$), когда в предыдущем определении прямую сумму заменяют прямым произведением: с одной стороны такая конструкция типично, что будет давать несчетные группы, так как в таком случае будут рассматриваться все последовательности, а не только финитные. Но с другой стороны $G \wr\wr H$ обладает универсальным свойством, что любое расширение G с помощью H будет вкладываться в $G \wr\wr H$. Также отмечу, что не нужно смущаться, что G никак не зависит от индекса $h \in H$, по которому берется сумма: так и должно быть, чтобы прямые слагаемые были одинаковыми. Сплетения групп обычно являются хорошими источниками контрпримеров и идеально подходят, чтобы на них отработали новую теорию, идею или теоретико-групповую гипотезу. Теперь мы готовы предъявить наш пример:

Пример

Группа $G = \mathbb{Z}_2 \wr \mathbb{Z}$ является аменабельной группой экспоненциального роста.

Группу G обычно называют лампочной группой (иногда я слышал, как ее называли ламповой группой, в английской литературе она называется Lamplighter group), проводя жизненную параллель между ее подгруппой $\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}_2$, элементы которой можно отождествить с последовательностью 0 и 1, и бесконечной улицей с фонарями, где 1 соответствует фонарю с горящим светом, а 0 - с потухшим. В таком контексте порождающий действующей группы $\mathbb{Z}$ можно ассоциировать с фонарщиком, защигающим и тушащим фонари.

Так как группа G является расширением абелевой группы $\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}_2$ абелевой группой $\mathbb{Z}$ - то по нашим свойствам она будет аменабельной. Так как элементы $\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}_2$ представляют собой финитные последовательности, то мы их будем записывать вектором из 0 и 1,и либо будем специально оговаривать, какой набор индексов покрывается координатами этого вектора, либо вообще не будем набор индексов упоминать, в случаях, когда это не сможет привести к недоразумениям или неоднозначности трактовки. К примеру, будем считать, что $(0,1,1,0) \in \bigoplus_{i\in\mathbb{Z}} \mathbb{Z}_2$, и если понадобится, то уточним, что этим вектором покрываются индексы от -2 до 1. Разумеется, в этом случае в индексах, не входящих в $\{-2,-1,0,1\}$, значение координаты будет равно 0. Группа G имеет два стандартных копредставления, получаемых непосредственно из ее определения:

$$G = \langle b, \{a_i\}_{i\in\mathbb{Z}} |\ a_i^2 = e, [a_i, a_j] = e, b^{-1}a_i b = a_{i+1}\rangle = \langle a, b |\ a^2 = e, [b^{-i}ab^i, b^{-j}ab^j] = e\rangle$$

Первое копредставление - это определение в чистом виде, переход ко второму осуществляется $a_i \mapsto b^{-i}ab^i$ и $b \mapsto b$, Ясно, что отображение, заданное на порождающих таким образом, продолжается до изоморфизма групп. Мы будем работать со вторым копредставлением. Рассмотрим $S = \{a, a^{-1}, b, b^{-1}\}$ и попытаемся что-то сказать про функцию роста $\gamma_S(n)$ (на самом деле S - трехэлементное множество, так как $a = a^{-1}$).

Рассмотрим набор индексов от 1 до n, и рассмотрим $Q_n = \{(x_1, \ldots, x_n) : x_i \in \mathbb{Z}_2\}$. Ясно, что $|Q_n| = 2^n$, но этого недостаточно для экспоненциальности роста, так как для записи $x = (x_1, \ldots, x_n) = a_1^{x_1} \cdot \ldots \cdot a_n^{x_n}$ в алфавите S потребуется не n, а квадратичное по n количество букв (так как каждая координата $a_i^{x_i} = b^{-i}a^{x_i}b^i$ может вносит вклад в количестве вплоть до $2i+1$ дополнительных букв). И если все довести до конца, то лучшая при таком подходе оценка для скорости роста получится около $e^{\sqrt{n}}$, что недостаточно. Идеальной ситуацией было бы, если в этих словах было бы как можно больше сокращений, настолько, чтобы полученные слова можно было бы вложить в шары с радиусами, растущими линейно по n. И если рассмотреть две соседние координаты $a_i^{x_i}$ и $a_{i+1}^{x_{i+1}}$, то самые хорошие для нас ситуации - это когда $x_i = x_{i+1} = 0$ - тогда там нет букв в принципе, и $x_i = x_{i+1} = 1$ - тогда в соответствующем фрагменте $b^{-i}ab^ib^{-(i+1)}ab^{i+1}$ видно как много b'шек сократится на стыке. И нужно найти баланс: выбрать множество слов, в которых все хорошо сокращается с одной стороны, но при этом чтобы их количество оставалось экспоненциальным.

И оказывается, что этот баланс можно найти в множестве:

$$\Phi_n = \{x = (x_1, \ldots, x_n) | x_i \in \mathbb{Z}_2 \text{ и в } x \text{ нет двух подряд идущих } 0\}$$

такие множества часто встречаются в самых разных областях математики и их обычно называют множествами Фибоначчи, и скоро вы поймете почему. Также обозначим через $aX = \{ax : x \in X\}$. Тогда простейшие комбинаторные рассуждения показывают, что:

$$\Phi_n = 1\Phi_{n-1} \cup 01\Phi_{n-2}$$

так как если последовательность начинается с 1, то на последующие буквы нет никаких дополнительных ограничений (кроме отсутствия подслова 00), а если начинается с 0 - то следующая обязана быть 1, а уже начиная со второй буквы никаких дополнительных условий нет. Таким образом:

$$|\Phi_n| = |\Phi_{n-1}| + |\Phi_{n-2}|$$

то есть количество таких векторов равно соответствующему члену последовательности Фибоначчи, а значит $|\Phi_n|$ растет экспоненциально. К примеру, по индукции легко проверить, что $|\Phi_n| \geq (\sqrt{2})^n$ (хотя нетрудно выписать и общую формулу).

Теперь оценим радиус шара, в который помещается Φ_n. Пристально посмотрим на произвольный элемент этого множества

$$x = (b^{-1}a^{x_1}b)(b^{-2}a^{x_2}b^2)(b^{-3}a^{x_3}b^3) \cdot \ldots \cdot (b^{-n}a^{x_n}b^n)$$

и заметим, что некоторые отделенные скобками блоки в реальности отсутствуют (в случае, если соответствующее $x_i = 0$). И тогда между оставшимися в живых a'шками после сокращения может остаться либо b^{-1} (что соответствует случаю, когда между блоками никто не исчезал), либо b^{-2} (когда между ними исчез один блок, что соответствует 0 в последовательности). Два блока подряд исчезнуть не могут, так как 00 в нашей последовательности запрещено. Таким образом получаем грубую оценку на длину слова: сначала b^{-1}, в конце максимум b^n, потом еще максимум n штук a'шек, и между каждой из них максимум 2 буквы. Итого получаем, что:

$$\Phi_n \subset B_S(1 + n + n + 2(n-1)) = B_S(4n-1) \subset B_S(4n)$$

А значит:

$$\gamma_S(n) \geq \gamma_S\left(4\left\lfloor\frac{n}{4}\right\rfloor\right) \geq \left|\Phi_{\lfloor\frac{n}{4}\rfloor}\right| \geq \sqrt{2}^{\left\lfloor\frac{n}{4}\right\rfloor} \geq 2^{\frac{n-4}{8}}$$

В принципе, если не вдаваться в дотошные детали формалистики: это означает, что аменабельная G является группой экспоненциального роста.

Замечания:

• *Ну а если все-так вдаваться в технические подробности, то чисто формально нужно получить оценку $\gamma_S(n) \geq a^n$ в чистом виде: разумеется, для функций роста важно только поведения функций начиная с некоторого номера: и возможность игнорировать начальный кусок последовательности предоставляет большую гибкость оценок. Но мы это не проговаривали и тем более не доказывали. Поэтому, чтобы в этом примере дойти до победного конца, можно воспользоваться хитростями математического анализа: написать какую-нибудь довольно грубую оценку начиная с некоторого номера, например $2^{\frac{n-4}{8}} \geq 2^{n/16}$ при*

$n \geq 8$, а дальше подобрать такое $2^{1/16} > q > 1$, чтобы для всех $i \leq 8$ было выполнено $|\Phi_i| \geq q^8$. Таким образом мы получим $\gamma_S(n) > q^n$ для любого n (и в степени q уже находится n вместо некоторой линейной по n функции). Либо как вариант, можно доказать утверждение, что для характеризации скорости роста достаточно оценок начиная с некоторого номера, либо вообще это постулировать изначально в определении. Хотя все-таки лучше работать с классическими определениями, чтобы не было путаницы. И так в математике очень много проблем из-за того, что некоторые понятия разными математиками определяются не совсем идентично - и возникает проблема с синхронизацией результатов. В математике важно каждое предположение, каждый нюанс; и если кто-то работает с каким-нибудь понятием, условно, предполагая счетность группы, а другой счетность не предполагает - сами представляете как сложно им будет читать работы друг друга. Но с другой стороны нужно с пониманием отнестись к этой проблеме: все-таки математика - это живой организм, который развивается благодаря тому, что некоторым людям нравится работать с формулами и проникать в тайны бесконечности. Основа математики - это точность и красота, а вопрос терминологии важный, но все-таки не первостепенный.

• *Еще один комментарий: совершенно неформальный и полностью находящийся в интуитивной плоскости: если рассмотреть какую-нибудь абелеву бесконечно-порожденную группу (например $\mathbb{Q}$ или же $\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}_2$), то она будет аменабельной, но при этом хотя формально для нее не будет определено понятие функции роста, очень грубо и очень приблизительно можно считать, что она будет бесконечной. То есть высокая скорость роста сочетается с простой групповой структурой в этих примерах. На самом деле, пример лампочной группы во многом построен на этой же идее: в основе лежала бесконечно-порожденная группа $\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}_2$, но хитрыми манипуляциями с полупрямым произведением мы пришли к конечно-порожденному случаю, при этом сохранив часть бесконечно-порожденного наследия.*

Второй сюжет: здесь уже появление аменабельных групп куда более удивительно, чем в первом сюжете. Пока, кстати, как следует с ним разбирался перед изложением в методичке: в корне поменял взгляды на топологическую составляющую в теории аменабельности; и в частности по максимуму отказался даже от упоминаний недискретных топологических групп. Сам сюжет сводится к следующей характеризационной теореме:

Теорема

Пусть G - дискретная группа. Тогда G - аменабельна $\Leftrightarrow$ когда каждое действие $G \curvearrowright X$ аффинными преобразовании на выпуклом компактном подмножестве локально выпуклого пространства имеет неподвижную точку.

Формулировка может показаться немного страшной для далеких от продвинутого функционального анализа читателей. Поясню фигурирующие в формулировке теоремы понятия: *аффинными* называют функции f на линейном пространстве L, такие что $f(tx + (1-t)y) = tf(x) + (1-t)f(y)$ для всех $x, y \in L$ и $t \in [0,1]$ (иными словами функции, являющиеся одновременно и выпуклыми, и вогнутыми). Топологическое линейное пространство называется *локально выпуклым*, если оно

хаусдорфово и его топология задается некоторой системой нолунорм (в отличие от нормированных пространств, где топология задается оной полунормой, которая из условия хаусдорфовости обязана быть нормой). Если топология задается счетной системой полунорм $\{p_k\}_{k\in\mathbb{N}}$, то топология метризуема (и можно явно выписать метрику: $\rho(x,y) = \sum\limits_k \frac{1}{2^k}\frac{p_k(x-y)}{1+p_k(x-y)}$). Но в типичных возникающих на практике примерах (например, в случае *-слабой топологии на банаховом сопряженном V^*) система полунорм как правило несчетная, и получаемое локально выпуклое пространство оказывается неметризуемым, то есть ровно тем, чем обычно пугают на математическом анализе. *Неподвижная точка* - это точка x, такая что $g\cdot x = x$ для всех $g\in G$.

$\Leftarrow$ Во введении к этой главе я упоминал, что конечно-аддитивные вероятностные меры $M(G)$ на G находятся в естественном взаимно-однозначном соответствии с пространством состояний $S(\ell^\infty(G)) \subset \ell^\infty(G)^*$. Пространство $\ell^\infty(G)^*$ со *-слабой топологией является локально-выпуклым пространством, задающая топологию система полунорм выглядит так: $p_x(f) = |f(x)|$, где $x\in\ell^\infty(G)$ и $f\in\ell^\infty(G)^*$. По теореме Банаха-Алаоглу единичный шар в *-слабой топологии компактен, тогда в силу замкнутости пространства состояний $S(\ell^\infty(G))$, оно оказывается выпуклым компактом. Так как упомянутая выше биекция $M(G) \leftrightarrow S(\ell^\infty(G))$ уважает линейные комбинации - мы можем перенести построенную топологию на $M(G)$, и оно тоже превратится в выпуклое компактное подмножество локально выпуклого пространства $\ell^\infty(G)^*$. Рассмотрим естественное действие

$$G \curvearrowright M(G)$$

заданное формулой $(g\cdot\mu)(A) = \mu(g^{-1}A)$ (действие $G\curvearrowright X$ это гомоморфизм $G\to S(X)$. Если мы хотим перенести действие с множества на пространство функций любого сорта: обычных функций или, как в случае с мерами, функций определенных на подмножествах - аргумент нужно умножать не на g, а на g^{-1} - иначе отображение $G\to S(?)$ будет не гомоморфизмом, а антигомоморфизмом). По условию у такого действия должна быть неподвижная точка, которая по построению и будет являться инвариантной конечно-аддитивной вероятностной мерой на G.

$\Rightarrow$ Рассмотрим существующую из аменабельности инвариантную меру m на G, и рассмотрим произвольную точку $x\in X$ в нашем выпуклом компакте. Тогда возникает орбитальное отображение $t: G\to X$, заданное формулой $t(g) = g\cdot x$; и рассмотрим образ μ меры m при этом отображении, т.е. меру на X заданную формулой $\mu(A) = m(t^{-1}(A))$, она тоже будет инвариантной. Для этой меры рассмотрим ее барицентр, т.е. точку

$$b_\mu = \int\limits_X x d\mu(x) \in X$$

Тогда элементарные выкладки вкупе с инвариантностью μ доказывают, что она и будет искомой неподвижной точкой:

$$g\cdot b_\mu = \int\limits_X g\cdot x d\mu(x) = [g\cdot x = y] = \int\limits_X y d\mu(g^{-1}\cdot y) =$$

$$= \int\limits_X y d[(g\cdot\mu)(y)] = \int\limits_X y d\mu(y) = b_\mu$$

Замечания:

• *Локальная выпуклость в этой теореме нужна для того, чтобы на пространстве был определен интеграл, и чтобы он обладал стандартными и привычными для нас свойствами интеграла (для построения интеграла нужно суммировать, брать пределы интегральных сумм. К примеру, топология должна быть хаусдорфовой, чтобы предел был единственным, а значит и интеграл был корректно определенной функцией). Множество X должно быть выпуклым и замкнутым, иначе барицентр может не принадлежать X (Заметим, что $\int\limits_X d\mu(x) = 1$, т.е. барицентр можно записать именно как предел выпуклых линейных комбинаций элементов из X), компактность X нужна для существования интеграла (также, напомню, что компактность множества обеспечивает его замкнутость). Аффинность преобразований нужна для того, что действие группы не нарушало эту красивую выпуклую картину происходящего.*

• *На самом деле практическая ценность этого утверждения присутствует только в части $\Rightarrow$, никто не будет проверять аменабельность, проверяя наличие неподвижных точек для всех вышеописанных действий.*

• *Также стоит отметить, что условие теоремы очень редко выполняется для конечномерных X: хотя условие выпуклости довольно мягкое, но всю эту мягкость убивает требование аффинности действия: сами подумаете, к примеру, в том же $\mathbb{R}^2$ какие вы вообще можете придумать выпуклые множества, чтобы для него были биекции в себя аффинными преобразованиями? Думаю, таких окажется очень немного; и чем больше X будет допускать различных преобразований - тем симметричнее оно будет становиться, ослабляя тем самым мощь этой теоремы. Тем более, что в очень многих случаях аффинные биекции в себя вообще вынужденно оказываются какими-нибудь вращениями или симметриями, для которых 0 - очевидная неподвижная точка. В бесконечномерном случае примеры могут быть более содержательными: и если $G \curvearrowright X$ произвольное действие, то индуцированное действие $G \curvearrowright F(X)$ на пространстве некоторых функций (обычных функций, мер, и т.д.) будет типичным примером аффинного действия; особенно часто эта теорема используется для случая действия $G \curvearrowright \mathcal{P}(X)$ на пространстве борелевских вероятностных мер некоторого пространства X (по теореме Риса, к примеру, для компактного X верно $\mathcal{P}(X) \cong C(X)^*$). Если в качестве X взять само G и рассмотреть только конечно-аддитивные меры $M(G)$, то наличие неподвижной точки для действия $G \curvearrowright M(G)$ есть в точности определение аменабельности G. Замечу, что пространство $\mathcal{P}(X)$ со своей самой естественной топологией является компактным iff X компактен. Поэтому не должно быть удивительным, что из этой теоремы не вытекает существование счетно-аддитивной инвариантной меры для аменабельной G, так как пространство счетно-аддитивных мер:*

$$\mathcal{P}(G) = \{x \in \ell^1(G) : \sum_{g \in G} |x_g| = 1 \text{ и } x_g \geq 0\}$$

будет некомпактным для бесконечных счетных дискретных G в любой пригодной для этой теоремы топологии; и даже несмотря на то, что на нем аффинно действует G - неподвижной точки у действия $G \curvearrowright \mathcal{P}(G)$ не будет. Так что разница между $\mathcal{P}(G)$ и $M(G)$ принципиальная.

Третий сюжет: второй сюжет фактически строит мост между теорией групп и динамическими системами, проводя довольно интересную связь даже несмотря на то, что инвариантные меры довольно часто всплывают в теории динамических систем; следующий же сюжет проводит параллель между теорией групп и функциональным анализом и представляется мне еще более удивительным.

На самом деле аменабельные группы связаны с функциональным анализом намного более плотно в другом направлении: через операторные алгебры. К примеру аменабельность G эквивалентна ядерности редуцированной групповой алгебры $C_r^*(G)$, то есть возможности ее в некотором смысле хорошо аппроксимировать конечномерными алгебрами. Или же ядерность эквивалентна совпадению полной и редуцированной групповых алгебр $C^*(G) = C_r^*(G)$. И этот список можно продолжать и продолжать не менее фантастическими результатами, но здесь мы ограничимся одним не столь эффектным, но все же очень поучительным и ярким результатом, который в отличие более фундаментальных результатов проще доказать "с нуля" (все-таки это методичка по теории групп, а не функциональному анализу).

Немного подготовительной теории: пусть G - счетная дискретная группа, рассмотрим гильбертово пространство $\ell^2(G)$ и представление сдвигами группы G в нем, заданное формулой $\lambda : G \to B(\ell^2(G))$, $\lambda(g)\delta_h = \delta_{gh}$, где δ_h - базисный орт, т.е. вектор, у которого h-ая координата равна 1, а все остальные равны 0. Это представление очень часто возникает в функциональном анализе, играет огромное значение и называется *регулярным представлением*. Когда это не будет приводить к путанице, часто вместо $\lambda(g)$ мы будем писать просто g. Также отметим, что по построению все операторы $\lambda(g)$ будут унитарными.

Для представления $\pi : G \to B(H)$ группы G унитарными операторами *асимптотически инвариантным вектором* мы будем называть последовательность векторов ξ_n единичной длины, что для любого $g \in G$ выполнено: $\|\pi(g)\xi_n - \xi_n\| \to 0$. К примеру, если у представления существует законный инвариантный вектор ξ, то тогда $\xi_n = \frac{\xi}{\|\xi\|}$ будет и асимптотически инвариантным. Докажем следующее важное вспомогательное утверждение, представляющее независимые ценность и интерес:

Теорема

Счетная дискретная группа G аменабельна $\Leftrightarrow$ регулярное представление допускает асимптотически инвариантный вектор.

$\Rightarrow$ Пусть G - аменабельна, рассмотрим последовательность Фёльнера F_n и векторы $\xi_n = \frac{1}{\sqrt{|F_n|}}\chi_{F_n} \in \ell^2(G)$. Тогда нетрудно заметить, что:

$$\|g\xi_n - \xi_n\| = \frac{1}{\sqrt{|F_n|}}\|\chi_{gF_n} - \chi_{F_n}\| = \sqrt{\frac{|gF_n \triangle F_n|}{|F_n|}} \to 0$$

иными словами ξ_n является асимптотически инвариантным вектором.

$\Leftarrow$ Пусть теперь $\xi_n \in \ell^2(G)$ является асимптотически инвариантным вектором. Для доказательства аменабельности G построим на ней инвариантную меру. Рассмотрим вероятностную меру μ_n на G, заданную формулой:

$$\mu_n(M) = \sum_{h \in M} |\xi_n(h)|^2$$

Рассмотрим также полунорму $\|\xi\|_M = \sqrt{\sum_{h\in M} |\xi(h)|^2}$ для $\xi \in \ell^2(G)$ и $M \subset G$. Ясно, что $\|\xi\|_M \leq \|\xi\|$. Так как $\|\xi_n\| = 1$, и так как оператор $\lambda(g)$ - унитарен то $\|g^{-1}\xi_n + \xi_n\| \leq 2$, и введя для удобства обозначения $A = \xi_n = (\xi_n(h))_{h\in G}$ и $B = g^{-1}\xi_n = (\xi_n(gh))_{h\in G}$, а также вспоминая неравенство треугольника для полунорм $|\|\xi\| - \|\eta\|| \leq \|\xi - \eta\|$, мы получим:

$$|\mu_n(gM) - \mu_n(M)| = \left|\sum_{h\in gM} |\xi_n(h)|^2 - \sum_{h\in M} |\xi_n(h)|^2\right| = \left|\sum_{h\in M} |\xi_n(gh)|^2 - \sum_{h\in M} |\xi_n(h)|^2\right| =$$

$$= \left|\|B\|_M^2 - \|A\|_M^2\right| = \left|(\|B\|_M - \|A\|_M)(\|B\|_M + \|A\|_M)\right| \leq 2\left|\|B\|_M - \|A\|_M\right| \leq 2\|B-A\|_M \leq$$
$$\leq 2\|B - A\| = 2\|g^{-1}\xi_n - \xi_n\| \to 0$$

Теперь рассмотрев некоторый ультрафильтр $\mathcal{U}$, искомую меру можно получить как предел:

$$m(M) = \lim_{n\to\mathcal{U}} \mu_n(M)$$

Из-за того, что если классический предел существует, то он совпадает с пределом по ультрафильтру, мы получаем:

$$m(gM) - m(M) = \lim_{n\to\mathcal{U}}(\mu_n(gM) - \mu_n(M)) = \lim_{n\to\infty}(\mu_n(gM) - \mu_n(M)) = 0$$

таким образом мера m - инвариантна, а значит группа G - аменабельна.

Замечание

*Построение инвариантной меры m по μ_n можно было провести технически сложнее, но при этом чуть более "законно", если вдруг кто-то до сих пор идеологически не может принять взятие пределов по ультрафильтрам, хотя это часть современной математики и очень полезная техника, на которую я советую не закрывать глаза. Но если пока еще некоторые читатели не созрели до современных методов анализа - можно построить m по старинке: рассмотреть $\mu_n \in \ell^1(G) \subset \ell^\infty(G)^*$. Единичный шар в $\ell^\infty(G)^*$ является *-слабо компактным, а потому у последовательности $\{\mu_n\}_n$ должна быть предельная точка $m \in \ell^\infty(G)^*$, которую можно воспринимать, как мы помним, как меру на G. Убедимся в инвариантности m, проведя аккуратные выкладки со *-слабой топологией: напомню, что окрестности*

$$U_{\varepsilon,x}(f) = \{\tilde{f} : |(\tilde{f} - f)(x)| < \varepsilon\} \subset \ell^\infty(G)^*$$

*где $\varepsilon > 0$, $f \in \ell^\infty(G)^*$ и $x \in \ell^\infty(G)$ являются базой для *-слабой топологии. Тогда вспоминая, что конечно-аддитивные вероятностные меры на G находятся в естественном взаимно-однозначном соответствии с $S(\ell^\infty(G))$, мы будем использовать одни и те же обозначения для мер и соответствующих им состояний. Рассмотрим произвольный $g \in G$ и пусть $f = g^{-1} \cdot m - m$ и $f_n = g^{-1} \cdot \mu_n - \mu_n$. Тогда нетрудно заметить, что f будет предельной для $\{f_n\}_n$ (фактически из-за непрерывности операции вычитания). Тогда рассмотрим произвольное $\varepsilon > 0$ и произвольное $M \subset G$ и положим $x = \chi_M$; тогда в окрестности $U_{\varepsilon,x}(f)$ будет находиться бесконечное число f_n; и раз $|\mu_n(gM) - \mu_n(M)| \to 0$, то из этого бесконечного набора можно выбрать такое n, что:*

$$|f_n(x)| = |(g^{-1} \cdot \mu_n)(M) - \mu_n(M)| = |\mu_n(gM) - \mu_n(M)| < \varepsilon$$

Окончательно получаем:

$$|f(x)| \leq |f(x) - f_n(f)| + |f_n(x)| < 2\varepsilon$$

*И в силу произвольности ε получаем, что $f(x) = 0$, иными словами $m(gM) = m(M)$. Рассуждения получились такими тяжелыми из-за сложности и хитрости *-слабой топологии: в частности если f является предельной для $\{f_n\}$, то f не обязана быть равна пределу некоторой подпоследовательности $\{f_{n_k}\}$ (к примеру, рассмотрите $\delta_n \in \ell^\infty(\mathbb{N})^*$, где $\delta_n(f) = f(n)$; и у этой последовательности должна быть предельная точка, но ясно, что никакие подпоследовательности δ_{n_k} не имеют предела). Мне больше нравятся рассуждения с ультрафильтрами, но, возможно, кому-то ближе будет такой подход.*

Пусть S - симметричное множество порождающих для счетной дискретной группы G (это не очень существенное условие, так как если S не является симметричным, то можно добавить все обратные, превратив его в симметричное), пусть λ - регулярное представление G в $\ell^2(G)$. Ключевым персонажем последующего изложения станет оператор:

$$M = \frac{1}{|S|} \sum_{g \in S} \lambda(g)$$

С ним тесно связан оператор $\Delta = |S| - |S|M$, чрезвычайно важный для приложений и который носит очень много имен: иногда его называют оператором Маркова, потому что он является генератором Маркова для стандартного случайного блуждания на группе G, иногда его называют оператором Лапласа для группы, так как с одной стороны по свойствам он очень напоминает обычный оператор Лапласа для гладких функций, а с другой стороны служит заменой для классического оператора Лапласа в дискретных физических задачах (модель Изинга - хороший пример). Но нам удобнее будет работать с неоткалиброванной версией M. И оказывается, что через этот оператор можно записать критерий аменабельности G, а именно:

Теорема

Конечнопорожденная дискретная группа G с симметричным порождающим множеством S аменабельна $\Leftrightarrow \|M\| = 1$.

Совершенно ясно, что в любых ситуациях $\|M\| \leq \frac{1}{|S|} \sum\limits_{g \in S} \|\lambda(g)\| = 1$.

$\Rightarrow$ Пусть G аменабельна, рассмотрим существующий по предыдущей теореме асимптотически инвариантный вектор $\xi_n \in \ell^2(G)$ (в качестве которого можно взять $\frac{1}{\sqrt{|F_n|}}\chi_{F_n}$ для фёльнеровских множеств F_n), тогда ясно, что $M\xi_n - \xi_n \to 0$, а значит можем выписать цепочку неравенств:

$$1 = \lim_n \|M\xi_n\| \leq \sup_{\|\xi\|=1} \|M\xi\| = \|M\| \leq 1$$

Таким образом $\|M\| = 1$.

$\Leftarrow$ Здесь будет немного сложнее, пусть $\|M\| = 1$. В первую очередь из функционального анализа вспомним, что для самосопряженного оператора T верно $\|T\| = \sup\limits_{\|x\|=1} \big|\langle Tx, x\rangle\big|$ (это вытекает, например, из спектральной теоремы; на самом деле это равенство верно даже без модуля у скалярного произведения, но с модулем

нам будет работать удобнее). Также заметим, что M - самосопряженный оператор (так как S - симметричное, то для любой пары $\{g, g^{-1}\}$ из-за того, что $\lambda(g)^* = \lambda(g^{-1})$, мы получаем

$$(\lambda(g) + \lambda(g^{-1}))^* = \lambda(g) + \lambda(g^{-1})$$

Если же симметричная пара вырождена, т.е. $g = g^{-1}$, то и в этом случае из-за того, что $\lambda(g)^* = \lambda(g^{-1})$, вклад этой "пары" в итоговый оператор тоже будет самосопряженный). Таким образом для любого $\varepsilon > 0$ мы сможем найти такой вектор $\|\xi\| = 1$, что $\left|\langle M\xi, \xi\rangle\right| > 1 - \varepsilon$. Также рассмотрим вектор $|\xi|$, координаты которого являются модулями координат ξ, т.е. $|\xi|(h) = |\xi(h)|$; ясно что он тоже единичной длины. Дальше заметим, что:

$$1 - \varepsilon < \left|\langle M\xi, \xi\rangle\right| = \left|\frac{1}{|S|}\sum_{g\in S}\langle\lambda(g)\xi, \xi\rangle\right| = \left|\frac{1}{|S|}\sum_{g\in S}\sum_{h\in G}\xi(g^{-1}h)\overline{\xi(h)}\right| \leq$$

$$\leq \frac{1}{|S|}\sum_{g\in S}\sum_{h\in G}|\xi(g^{-1}h)||\xi(h)| = \frac{1}{|S|}\sum_{g\in S}\langle\lambda(g)|\xi|, |\xi|\rangle = \langle M|\xi|, |\xi|\rangle \leq 1$$

Отметим, что $\langle\lambda(g)|\xi|, |\xi|\rangle$ являются вещественными неотрицательными числами и $\langle\lambda(g)|\xi|, |\xi|\rangle \leq 1$. Так как их среднее арифметическое по только что доказанному лежит в $(1 - \varepsilon, 1]$, тогда для каждого из них верно:

$$1 - |S|\varepsilon < \langle\lambda(g)|\xi|, |\xi|\rangle \leq 1$$

ведь если вдруг кто-то из них $\leq 1 - |S|\varepsilon$, то даже если все остальные по максимуму равны 1 - их среднее арифметическое дотянет максимум до $1 - \varepsilon$. Так как $|S|$ - это зафиксированная для всей задачи постоянная, то для $\varepsilon = \frac{1}{n}$ мы можем построить векторы единичной длины ξ_n, равные подходящим $|\xi|$, что

$$\langle\lambda(g)\xi_n, \xi_n\rangle \to 1$$

И теперь из элементарного геометрического факта $\|a-b\|^2 = \|a\|^2+\|b\|^2-\langle a, b\rangle-\langle b, a\rangle$, а также из-за того, что $\langle a, b\rangle = \langle b, a\rangle$, когда $\langle a, b\rangle$ - вещественно, мы получаем:

$$\|\lambda(g)\xi_n - \xi_n\| \to 0$$

для любого $g \in S$. И если последовательность векторов является асимптотически инвариантной для порождающих - то она является таковой и для всех элементов группы: для доказательства для слов большей длины можно воспользоваться индукцией, доказав возможность редукции проверки асимптотической инвариантности к словам меньшей длины, а именно, если $g = ab$, то

$$\|\lambda(ab)\xi_n - \xi_n\| = \|\lambda(ab)\xi_n - \lambda(a)\xi_n + \lambda(a)\xi_n - \xi_n\| \leq \|\lambda(b)\xi_n - \xi_n\| + \|\lambda(a)\xi_n - \xi_n\| \to 0$$

Таким образом $\|\lambda(g)\xi_n - \xi_n\| \to 0$ для для всех $g \in G$, а наличие асимптотически инвариантного вектора по предыдущему утверждению влечет аменабельность нашей группы G.

Замечания:

• *На самом деле, вот эти вот хитрости с введением вектора $|\xi|$ нужны были лишь для того, чтобы освободить скалярное произведение от модуля: без этих векторов, лучшее, что мы могли получить - это $\left|\langle\lambda(g)\xi_n,\xi_n\rangle\right|\to 1$, и максимум, что можно извлечь отсюда: это либо хорошую ситуацию $\lambda(g)\xi_n\approx\xi_n$, либо крайне нежелательную $\lambda(g)\xi_n\approx-\xi_n$.*

• *Не знаю, какие впечатления оставил у вас этот факт, но мне этот результат представляется просто фантастическим: фактически это дает в корне другой аналитический подход к исследованию аменабельности: потому что "доказать, что что-то там существует" (меры или множества Фёльнера) - это одно, а вычислить норму оператора - это совершенно другое. Но при этом сразу отмечу, что вычисление нормы оператора - это сложная и далеко не алгоритмическая задача. Даже в n-мерном случае она не решаема и эквивалентна нахождению корней многочлена степени n; напомню, что $\|A\|^2$ равен максимальному корню характеристического многочлена матрицы A^*A. Что касается бесконечномерного случая, то напомню, что до сих неизвестно, является ли аменабельной группа Томпсона, хотя она имеет довольно простое копредставление, про нее известно множество фактов, и ее оператор Лапласа изучали многие ученые: выписывали оценки, доказывали свойства, можно выписать довольно явно его бесконечную матрицу - но все равно неясно, равна ли 1 его норма. Также отмечу, что автоматически это утверждение дает критерий и для проверки группы на неаменабельность, которая будет эквивалентна $\|M\|<1$.*

==========

Задачи для самостоятельной работы

• *Пусть $P=\{p_1,p_2,p_3,\ldots\}$ множество всех простых чисел в порядке возрастания. Доказать, что группа $G=\langle(p_n,p_{n+1},p_n+p_{n+1}+1)\rangle<S_\infty$, порожденная всеми такими тройными циклами, является аменабельной.*

• *Доказать аменабельность группы*

$$G=\langle a,b,c,d|\ \ [a,b]=[a,c]=[b,c]=1,d^{-1}ad=ab,d^{-1}bd=abc,d^{-1}cd=bc\rangle$$

• *Доказать, что для любой группы G существует аменабельный радикал $Rad(G)$, т.е. максимальная по включению аменабельная нормальная подгруппа G. Доказать, что в группе может не существовать максимальная аменабельная подгруппа (если отбросить условие нормальности). Чему равен $Rad(G)$ для аменабельных групп? Вычислить $Rad(\mathbb{F}_2)$.*

• *Вычислить класс эквивалентности функции роста группы Баумслага-Солитера $B(1,2)=\langle a,b|b^{-1}ab=a^2\rangle$.*

• *Вычислить норму $\|M\|$ оператора Маркова M для двух групп с множеством порождающих S:*

1) Лампочная группа $\mathbb{Z}_2\wr\mathbb{Z}$, где $S=\{a,b,b^{-1}\}$.

2) Свободная группа $\mathbb{F}_2$, где $S=\{a,a^{-1},b,b^{-1}\}$.

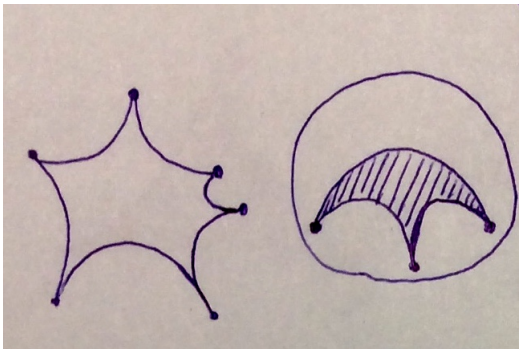
• *Вычислить класс эквивалентности функции роста группы Баумслага-Солитера $B(2,3)=\langle a,b|b^{-1}a^2b=a^3\rangle$ (Подсказка: группы субэкспоненциального роста являются аменабельными).*

Гиперболические группы

Гиперболические группы, подобно аменабельным, являются чрезвычайно важным классом групп совершенно удивительным способом связывающие самые разные математические области: и если аменабельные группы как мы выяснили среди прочего связывают функциональный анализ, теорию меры, динамические системы и аппроксимацию конечными группами; то гиперболические группы главным образом являются крепким связующим мостом между геометрией многообразий отрицательной кривизны, метрической геометрией и алгоритмическими проблемами в группах. Идеи этих связей долгое время витали в воздухе - но лишь в 1987 году М.Л. Громову удалось объединить их в единую субстанцию, которую он назвал *гиперболической геометрией*. Фактически ему удалось осмысленно определить понятие пространств отрицательной кривизны для произвольных метрических пространств, тогда как для кривизны в классическом понимании требуется гладкая структура многообразия: и приложения этих идей оказались фантастически продуктивными, за них даже М.Л. Громов был удостоен премии Абеля, считающейся самой престижной у математиков и служащей своеобразной математической версией премии Нобеля. Не нужно скептично относиться к тому, что фактически эта теория начала зарождаться лишь в 1987 году: сейчас она уже по праву считается классической, и как минимум общими представлениями о ней должен обладать любой профессиональный математик, деятельность которого хоть немного связана с теорией групп. На правах рекламы тем, кто хочет глубже разобраться с этой тематикой - порекомендую посмотреть лекции И.Г. Лысенка, которые легко можно найти в Интернете, и вес и значимость которым добавляет то, что он сам стоял у истоков многих классических результатов в этой области.

Самые глубокие корни этой теории ведут нас в 19-ый век, когда Н.И. Лобачевский открыл свою знаменитую геометрию, по свойствам так непохожую на обычную евклидову. У исследуемой им плоскости есть несколько моделей: это и дисковая модель, где плоскость - это внутренность круга, а прямые - это окружности, идущие перпендикулярно границе этого круга, называющейся абсолютом; это и модель, где плоскость - это верхняя полуплоскость обычной декартовой плоскости, а прямые - это окружности, перпендикулярные оси x; а также многие другие модели. Впоследствии появились и многомерные версии этой геометрии. Изначальная цель построения Н.И. Лобачевским своей плоскости были попытки построения непротиворечивой геометрии, в которой через одну точку могло проходить несколько прямых параллельных заданной (иными словами ее не пересекающих); но задним числом у этой плоскости оказалось множество свойств, которые кажутся невероятными и аномальными для привыкших к евклидову миру: к примеру, сумма углов треугольника всегда меньше 180 градусов, или то, что радиусы вписанных в треугольники окружностей равномерно ограничены: в евклидовом случае такого в принципе быть не может - если треугольник увеличить в два раза, то и окружность увеличится в два раза, а в гиперболической геометрии это так не работает, и очень часто в гиперболической геометрии возникают абсолютные длины, совершенно не зависящие от габаритов объектов, к которым они относятся. Интуитивно гиперболическую геометрию нужно себе представлять так, что все многоугольники

сильно сужаются у своих вершин; на рисунке мы схематично нарисовали в некотором роде типичный многоугольник гиперболической геометрии, а также треугольник в дисковой модели Пуанкаре:



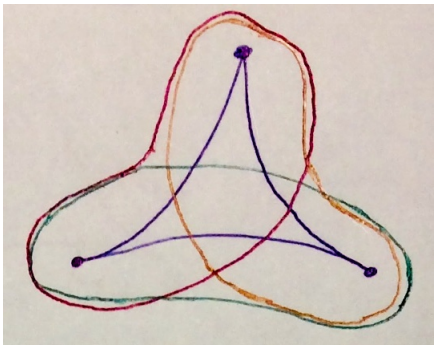
В дальнейшем люди поняли, что вся эта концепция переносится на многообразия отрицательной кривизны: есть даже такой специальный термин "многообразия отрицательной кривизны", по свойствам которые существенно выделяются из класса всех многообразий. Ну и венцом развития этой науки как раз стало введение М.Л. Громовом его гиперболических пространств. Отметим, что эта теория хорошо работает не для произвольных метрических пространств, а лишь для так называемых геодезических пространств. Метрическое пространство X называется *геодезическим*, если любые его две точки можно соединить геодезической (не обязательно единственной; геодезической мы называем отображение $p : \mathbb{R} \to X$, такое что $\ell(p|_{[s,t]}) = |s - t|$, где ℓ - длина кривой), и расстояние между любыми точками $x, y \in X$ равно длине геодезической их соединяющей, т.е. $\ell([x, y]) = d(x, y)$ (договоримся, что для произвольных точек a, b геодезического пространства некоторую соединяющую их геодезическую мы будем обозначать $[a, b]$). К примеру плоскость со стандартной метрикой является геодезическим пространством, а сфера с наследуемой из $\mathbb{R}^3$ метрикой таковой не является (путь по поверхности сферы оказывается длиннее расстояния между ними в $\mathbb{R}^3$), пространство рациональных чисел $\mathbb{Q}$ тоже не является геодезическим пространством, т.к. в него невозможно отобразить $\mathbb{R}$ нетривиальным образом. Также договоримся, что многоугольник с вершинами $a_0, a_1, \ldots, a_n$ и с геодезическими сторонами $[a_0, a_1], [a_1, a_2], \ldots [a_n, a_0]$ мы будем обозначать $[a_0, a_1, \ldots, a_n]$ и называть такой многоугольник геодезическим. Итак мы уже мотивационно подготовлены к первым определениям:

Определение

Геодезический треугольник $[a_0, a_1, a_2]$ мы будем называть δ-тонким (в английской литературе δ-slim), если каждая сторона лежит в δ-окрестности объединения двух других сторон, а именно для любого i mod 3 выполнено:

$$[a_i, a_{i+1}] \subset B_\delta([a_{i+1}, a_{i+2}] \cup [a_{i+2}, a_{i+3}])$$

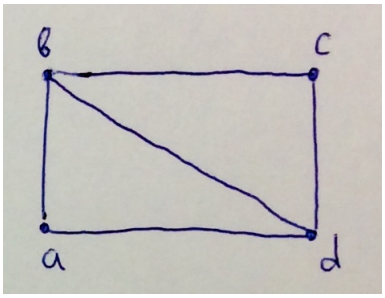
Договоримся, что окрестности во всей этой науке у нас будут замкнутыми, т.е. $B_\delta(X) = \{x : d(x, X) \leq \delta\}$. Вот так это выглядит на рисунке: каждая сторона оказывает полностью лежащей в объединении соответствующих оставшимся сторонам колбасок (совершенно очевидно, что $B_\delta(X \cup Y) = B_\delta(X) \cup B_\delta(Y)$):



Определение

Геодезическое пространство X называется δ-гиперболическим по Громову, если любой геодезический треугольник является δ-тонким.

Также сразу отмечу полезное следствие этого определения: что в любом геодезическом n-угольнике любая сторона лежит в $(n-2)\delta$-окрестности объединения других сторон: достаточно провести все диагонали, проходящие через одну из вершин исследуемого отрезка, и воспользоваться определением для каждого из полученных треугольников. Проиллюстрируем для четырехугольника $[a, b, c, d]$: имеем $[a, b] \subset B_\delta([a, d] \cup [b, d])$, но в свою очередь $[b, d] \subset B_\delta([b, c] \cup [c, d])$, а значит $B_\delta([b, d]) \subset B_{2\delta}([b, c] \cup [c, d])$. Таким образом $[a, b] \subset B_{2\delta}([a, d] \cup [b, c] \cup [c, d])$.

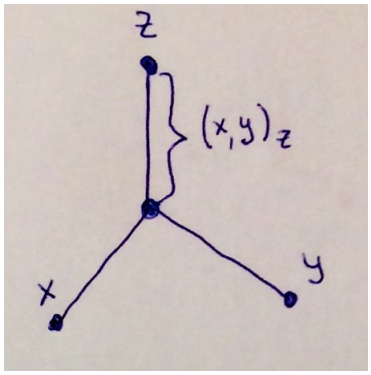


Также полезным является следующее наблюдение: если рассмотреть треугольник с одной вырожденной стороной, то реально получается двуугольник, для которого тоже выполнено условие определения. Формулируя это в немного других терминах мы получаем, что в δ гиперболических пространствах если p, q - любые две геодезические, соединяющие одну и ту же пару точек, то $p \subset B_\delta(q)$ (ну и разумеется $q \subset B_\delta(p)$ в силу симметричности ситуации относительно p и q).

Дадим еще два эквивалентных подхода к определению гиперболических пространств. Скалярным произведением Громова называется функция трех точке x, y, z:

$$(x, y)_z = \frac{1}{2}\left(d(x, z) + d(y, z) - d(x, y)\right)$$

Хотя оно и называется скалярным произведением - совершенно ясно, что в отличие от классического скалярного произведения в данном случае $(x, y)_z \geq 0$ всегда; и вообще алгебраически скалярное произведение Громова показывает, насколько неравенство треугольника для сопутствующих точек далеко от равенства. У него также есть геометрический смысл: главными модельными примерами гиперболических пространств в нашем случае будут деревья, так вот произвольный геодезический треугольник в дереве будет иметь следующий вид, и обычно называется *трезубцем*. И тогда $(x, y)_z$ будет в точности равно расстоянию от z до "центральной" точки:

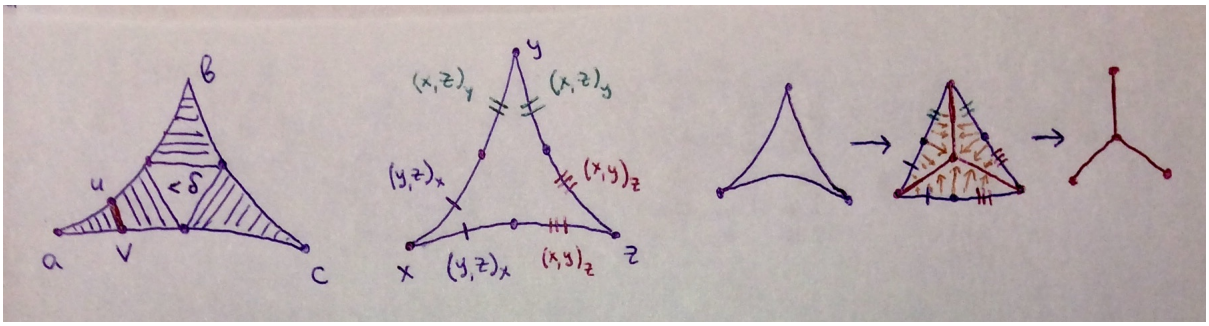


Формулу для $(x,y)_z$ довольно легко запомнить: вычитается расстояние между точками, от которых берется скалярное произведение, и прибавляется их расстояние до точки по которой берется это произведение.

Определение

Геодезический треугольник $[a,b,c]$ называется δ-узким (в английской литературе δ-thin), если для любых $u \in [a,b]$ и $v \in [a,c]$, таких, что $d(a,u) = d(a,v) \leq (b,c)_a$ выполнено $d(u,v) \leq \delta$.

Геометрически это означает, что концы всех "параллельных" отрезков на левой картинке находятся на расстоянии не больше δ. Важно отметить, что для пограничных точек соприкосновения этих "потоков" выполняются равенства длин соответствующих отрезков, что мы обозначили штрихами как в школьной геометрии. И если бы этот треугольник находился в обычно евклидовой $\mathbb{R}^2$ - то это были бы точки касания со вписанной окружностью; эти точки мы будем иногда называть *internal points*. В частности, расстояние между любой парой internal points не превосходит δ. Если написать соответствующую систему уравнений на длины этих сегментов - то она будет иметь единственное решение, причем решение это будет в точности скалярное произведение Громова в различных перестановках в зависимости от того, какие длины мы вычисляем.



Также отмечу, что в геодезических пространствах эти internal points всегда существуют: для их построения на геодезической нужно откладывать длины вида $(x,y)_z$, но так как геодезические - это изометрические отображения $\mathbb{R} \to X$ - то на отрезках можно откладывать совершенно любые длины. Второй подход к δ-узким треугольникам - это рассмотреть сквозное отображение: сначала нашего гиперболического треугольника в обычный евклидов с такими же длинами сторон, причем отображение на сторонах будет изометричным, а дальше евклидов треугольник отображаем в трезубец кусочно линейно на сторонах, причем все internal points его чтобы переходили в центральную точку трезубца (иными словами

придавливаем его стороны к трезубцу), а вершины остаются неподвижными; визуализация этого отображения - это картинка справа. И в этой терминологии δ-узкость означает, что диаметр прообраза произвольной точки при таком сквозном отображении не превосходит δ. Также уверен, что немногих должен удивить тот факт, что часто происходит терминологическая путаница между тонкими и узкими треугольниками (в английском языке термины slim и thin похожи даже больше чем в русском, и путаницы там еще больше).

Второй взгляд на δ-узкие треугольники хотя и выглядит немного навороченным и неестественным; зато он в полной мере раскрывается, если бы мы пытались построить теорию аппроксимации гиперболических многоугольников деревьями; и этот трезубец в образе сквозного отображения как раз является идеальным кандидатом на роль аппроксимирующего дерева в простейшем случае гиперболического треугольника.

Определение

Будем говорить, что пространство X удовлетворяет δ-условию Громова, если для любых точек $x, y, z, w \in X$ выполнено:

$$(x, z)_w \geq \min\{(x, y)_w, (y, z)_w\} - \delta$$

Оказывается, что все три подхода приводят к эквивалентным определениям гиперболических пространств,а именно верна:

Теорема

Пусть X - геодезическое пространство. Тогда следующие условия эквивалентны:

1) X является геодезическим для некоторого δ, т.е. любой геодезический треугольник является δ-тонким.

2) Для некоторого δ в пространстве X любой треугольник является δ-узким.

3) Для некоторого δ пространство X удовлетворяет δ-условию Громова

Первое условие иногда называют δ-гиперболичность по Рипсу, третье - δ-гиперболичностью по Громову. Сразу уточню, что эти условия не эквивалентны для конкретного δ; и переход от одного условия гиперболичности к другому сопровождается изменением константы гиперболичности. Например, верны следующие импликации (если первое условие обозначить через $R(\delta)$, второе $T(\delta)$ и третье $G(\delta)$):

$$G(\delta) \Rightarrow T(4\delta)$$

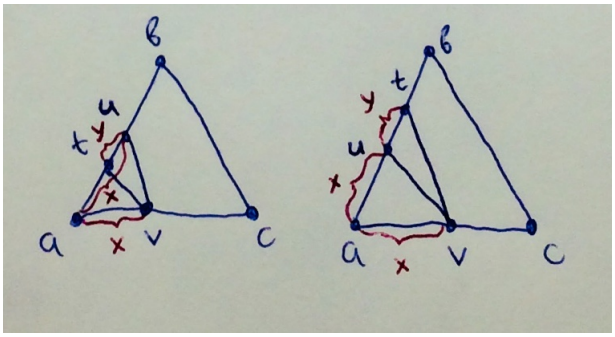
$$T(\delta) \Rightarrow R(\delta)$$

$$R(\delta) \Rightarrow G(3\delta)$$

При изучении гиперболичности пространств сами значения констант гиперболичности δ крайне редко бывают важны, важно лишь что такая константа существует. И у разных людей разные предпочтения в выборе базового определения гиперболичности из этих трех - и из-за этого иногда возникает путаница и сложности: особенно если вы хотите вникнуть в технические детали чьих-то выкладок - и за счет того, что неясно какое определение гиперболичности использовалось - оказывается сложно разобраться какое же там реально δ. Повторюсь, что говоря

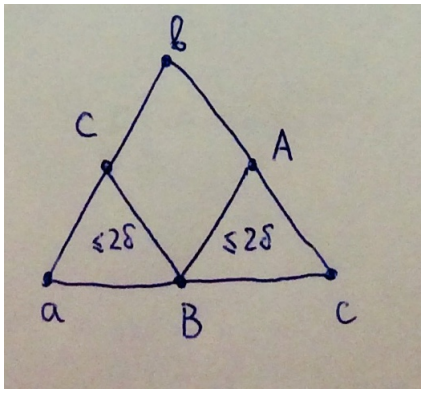
про δ-гиперболичность мы будем всегда иметь в виду первое условие. Кстати отмечу, что из-за упомянутых выше импликаций все три условия эквивалентны при $\delta = 0$ - и это единственный случай, когда константу менять не нужно. Эквивалентность доказывать мы не будем, лишь для иллюстрации техники работы с подобными оценками докажем $R(\delta) \Rightarrow T(6\delta)$ - так как доказательство очень идейно важное (кстати, получается более сильная импликация, чем если применять две из упомянутых выше, которые дают самое лучшее $R(\delta) \Rightarrow T(12\delta)$.

Для начала заметим, что если в геодезическом треугольнике $[a, b, c]$, для некоторых точек $u \in [a, b]$ и $v \in [a, c]$, таких что $d(a, v) = d(a, u)$, и для которых либо найдется точка $t \in [a, c]$, что $d(u, t) \leq \delta$, либо найдется $t \in [a, b]$, что $d(v, t) \leq \delta$ (иными словами если расстояние от одной из точек до стороны, где находится вторая точка, не больше δ) - тогда $d(u, v) \leq 2\delta$. Без ограничения общности считаем, что $t \in [a, b]$. Тогда возможны две ситуации расположения t относительно u:

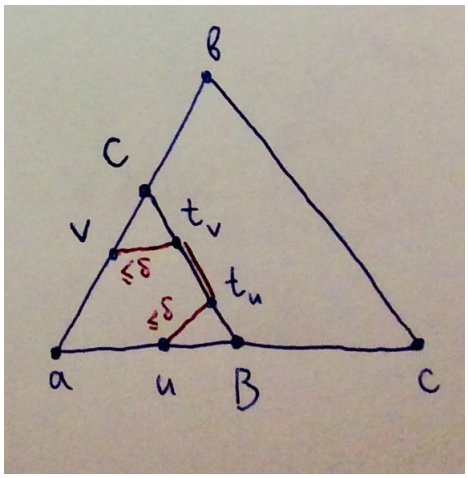


В левом случае из неравенства треугольника $[a, v, t]$ мы получаем $x \leq (x - y) + \delta$, т.е. $y \leq \delta$. А из неравенства треугольника $[t, u, v]$ получаем $d(u, v) \leq \delta + y \leq 2\delta$. Правый случай разбирается полностью аналогично: треугольник $[a, v, t]$ дает $x + y \leq x + \delta$, т.е. $y \leq \delta$, а дальше треугольник $[t, u, v]$ дает искомое $d(u, v) \leq y + \delta$.

Теперь пусть в пространстве X выполнено условие $R(\delta)$, и в произвольном треугольнике $[a, b, c]$ рассмотрим internal points $\{A, B, C\}$. Тогда расстояние между любыми двумя internal points будет $\leq 4\delta$. Действительно, рассмотрим к примеру точку B; так как треугольник $[a, b, c]$ является δ-тонким - тогда существует точка t на $[a, b] \cup [b, c]$, что $d(t, B) \leq \delta$. Пусть счастливчиком оказалось $[a, b]$ - тогда раз по определению internal points их расстояние до одной из вершин одинаковое: то в силу нашего замечания $d(B, C) \leq 2\delta$. И рассмотрим оставшуюся internal point (в нашем предположении это получается A) - из условия тонкости треугольника для нее тоже можно найти δ-близкую точку на одной из сторон и получить, что до одной из internal point (пусть это будет B) расстояние $d(A, B) \leq 2\delta$. Тогда по неравенству треугольника $d(A, C) \leq d(A, B) + d(B, C) \leq 4\delta$. Иными словами наши рассуждения дают, что расстояние от любой internal point до некоторой другой не больше 2δ - и отсюда при любых раскладах из неравенства треугольника вытекает, что между любыми internal points расстояние не больше 4δ



Теперь рассмотрим согласованные точки $u \in [a, c]$ и $v \in [a, b]$, то есть такие, что $d(a, u) = d(a, v)$. И рассмотрим геодезический треугольник $[a, B, C]$, который по предположению будет δ-тонким. Теперь: если либо существует точка $t_v \in [a, B]$ на расстоянии $\leq \delta$ от v, либо если существует точка $t_u \in [a, C]$ на расстоянии $\leq \delta$ от точки u - тогда наше замечание автоматически обеспечивает $d(u, v) \leq 2\delta$. И для рассмотрения остается один плохой случай, когда $t_v, t_u \in [B, C]$:



Но в таком случае из неравенства треугольника мы получаем

$$d(u, v) \leq d(u, t_u) + d(t_u, t_v) + d(t_v, v) \leq \delta + d(B, C) + \delta \leq 6\delta$$

То есть для всех случаев получается верна общая оценка $d(u, v) \leq 6\delta$. Иными словами мы доказали $R(\delta) \Rightarrow T(6\delta)$.

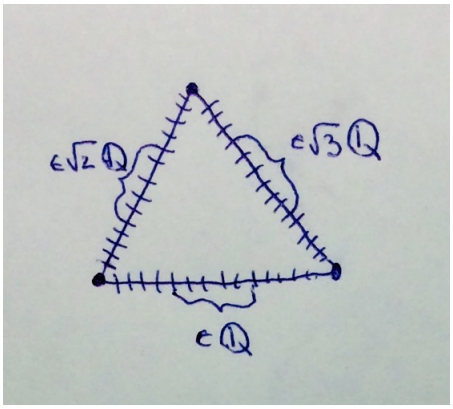
Некоторые из импликаций очевидны, к примеру $T(\delta) \Rightarrow R(\delta)$ очевидно выполняется в геодезических пространствах: рассмотрим треугольник $[a, b, c]$ и точку $v \in [a, c]$; а вместе с ней и согласованную с ней точку u на $[a, b]$ или $[b, c]$ в зависимости от того, с какой стороны от internal point B находится точка v. Из δ-узкости получаем, что $d(u, v) \leq \delta$, но это в частности означает, что $v \in B_\delta([a, b] \cup [b, c])$.

Замечание:

Обычно за первоначальное определение гиперболических пространств берут третье эквивалентное условие, так как оно единственное не требует геодезической структуры и для него нужна исключительно метрика, хотя, увы, оно самое непонятное и малоинтуитивное из этих трех; также отмечу, что для задач, где нужно работать с конкретными оценками, лучше всего подходит

второе эквивалентное условие. Первое условие самое понятное, и лучше всего подходит для задач с топологически-метрическим уклоном, то есть где много окрестностей. Основными объектами нашего исследования будут графы Кэли групп $C_A(G)$ - они являются геодезическими пространствами и для них все условия эквивалентны; хотя еще раз повторюсь, что эта эквивалентность работает только для геодезических пространств, т.е. где любые две точки соединяются геодезической и где метрика геодезическая (также отмечу, что иногда граф Кэли мы будем обозначать просто $C(G)$ когда ничего не сказано о порождающем множестве - и попрошу не путать это обозначение с централизатором: в этой главе он появится только один раз и мы отдельно уточним, что это именно он; то есть к путанице такое соглашение не должно привести). Однако в одном крайне важном для нас случае, когда пространство есть просто множество вершин графа Кэли $C_A(G)$ с такой же словесной метрикой (фактически граф с выброшенными ребрами) - можно определить понятие "дискретных" геодезических: путем мы будем называть просто последовательность точек, где две последовательные находятся на расстоянии 1 друг от друга в словесной метрике, а дискретной геодезической назовем кратчайшую из таких путей. Выбрасывание ребер - очень полезная операция, так как в таком случае любая точка пространства будет элементом группы. И вся теория гиперболических пространств во многом переносится на такие пространства, но возникают нюансы, и эта эквивалентность уже не полностью работает. К примеру, одним из отличий "дискретных" гиперболических пространств от классических является возможное отсутствие internal points - так как для их построения нужно делить отрезок в заданном отношении, но в дискретном случае геодезический треугольник вполне может состоять лишь из трех точек - и понятное дело в таком треугольнике никаких internal points не существует. Кстати иногда, хотя и не очень часто, в похожих ситуациях работает следующий прием: можно просто рассмотреть классическое гиперболическое "надпространство"(т.е. вспомнить про ребра), сделать все что нужно с существующими ребрами - а потом просто про эти ребра забыть - и иногда это работает.

Для некоторых стрелочек импликации переносятся почти дословно (возможно, нужно немного δ подправить): к примеру, стрелочка $R(?) \Rightarrow G(?)$ в "дискретном" случае доказывается точно так же как и в непрерывном (это одна из причин, почему условие Рипса мы выбрали в качестве отправного определения). Однако для некоторых стрелочек ситуация намного сложнее, и описанные выше условия уже не являются эквивалентными. Поучительным является следующий пример: рассмотрим в некотором гиперболическом пространстве равносторонний треугольник с очень большой константой тонкости δ. И построим новое пространство X, оставив лишь точки этого треугольника, и лишь те, расстояния от которых до вершин соизмеримы с $\mathbb{Q}$, $2\mathbb{Q}$ и $\sqrt{3}\mathbb{Q}$ соответственно для точек первой второй и третьей сторон:



Если эти изрешеченные стороны считать "дискретными" геодезическими - то этот треугольник будет 0-узким: потому что по построению этого пространства в этом треугольнике в принципе нет согласованных пар точек (т.е. точек, расстояние от которых до одной из вершин были бы одинаковыми) - поэтому и ничего проверять не нужно, и узкость выполняется с любой константой. С другой стороны относительно тонкости он ведет себя как нормальный треугольник, и в силу плотности $\mathbb{Q}$ в $\mathbb{R}$ его константа тонкости будет такой же, как и у первоначального треугольника. Таким образом в общем случае никакая разумная импликация $T(?) \Rightarrow G(?)$ не выполняется. Для желающих как следует разобраться с гиперболической геометрией мы советуем проделать творческое упражнение по выяснению, какие из импликаций остаются в силе при переходе к произвольным метрическим пространствам, где можно определить разумную версию "дискретных" геодезических.

Определение

Пусть дана группа $G = \langle A \rangle$, порожденная конечным множеством $A = \{a_1, \dots, a_n\}$. Рассмотрим ее граф Кэли $C_A(G)$, вершины которого есть элементы группы G, а направленными ребрами соединяются точки вида (g, ag) для некоторого $a \in A$. Группу G будем называть δ-гиперболической, если ее граф Кэли $C_A(G)$ со словесной метрикой является δ-гиперболическим пространством.

Напомню, что через $|g|$ обычно обозначается длина слова как элемента свободной группы $\mathbb{F}(A)$, т.е. сколько есть букв - такая и длина. В группе G разумнее рассматривать $|g|_G = \min\{|h| : h \underset{G}{=} g\}$, так как $|g|$ зависит от того, как именно мы выразили элемент $g \in G$ через порождающие, а значит не является функцией на группе G. И тогда *словесная метрика* на группе G определяется как $d(g,h) = |g^{-1}h|_G$. Словесная метрика является инвариантной относительно сдвига, а именно $d(gx, gy) = d(x, y)$. Также отмечу, что $d(x, gx) = |x^{-1}gx|_G \neq |g|_G$, то есть при сдвиге на g элементы не всегда сдвигаются на $|g|_G$ - в это ловушку можно попасть если слишком доверять интуиции, связывающей сдвиги на графах Кэли со сдвигами в обычных евклидовых пространствах.

Также отмечу, что в некотором смысле бессмысленно в этой теории рассматривать бесконечно-порожденные группы: потому что, если в качестве множества порождающих взять все G - тогда диаметр графа Кэли будет равен

1, иными словами пространство будет автоматически 1-гиперболическим. Любое ограниченное пространство является гиперболическим.

Важный пример гиперболических пространств - это деревья; они же являются единственным примером 0-гиперболических пространств. В случае деревьев любой гиперболический треугольник является трезубцем, (которые мы обсуждали, когда изучали понятие δ-узкости), для которых все геометрические характеристики лежат как на ладони. Но на самом деле, деревья являются не просто важным частным примером, а типичным примером, потому что в некотором смысле одномерные гиперболические пространства (а именно их мы и будем в основном рассматривать) выглядят "как деревья на бесконечности". Т.е. чем больше мы "удаляемся" от нашего пространства вверх, тем больше оно начинает быть похожим на дерево. Также деревья являются интуитивными светочами: и если некоторое утверждение верно на деревьях, то с большой вероятностью оно верно и для произвольных гиперболических пространств. Поэтому свои гиперболические идеи я советую в первую очередь проверять на деревьях. Также деревья помогают придумывать доказательства: если Вам нужно получить оценки на длины для произвольных гиперболических пространств - полезно их записать сначала для деревьев, чтобы понять нюансы (например, кто в данной ситуации длинный, а кто - нет), а также чтобы вообще разобраться, верны ли изучаемые оценки. Этот подход сильно помогает.

Также отмечу, что гиперболичность группы не зависит от выбора порождающего множества: на пальцах это очень непросто объяснить, и для строгого доказательства требуется весьма серьезная теория квазиизометрий: и в результате независимость вытекает из факта, что тождественное отображение $\mathrm{id} : (G, d_A) \to (G, d_B)$ является квазиизометрией, где d_M - словесная метрика, индуцированная порождающим множеством M.

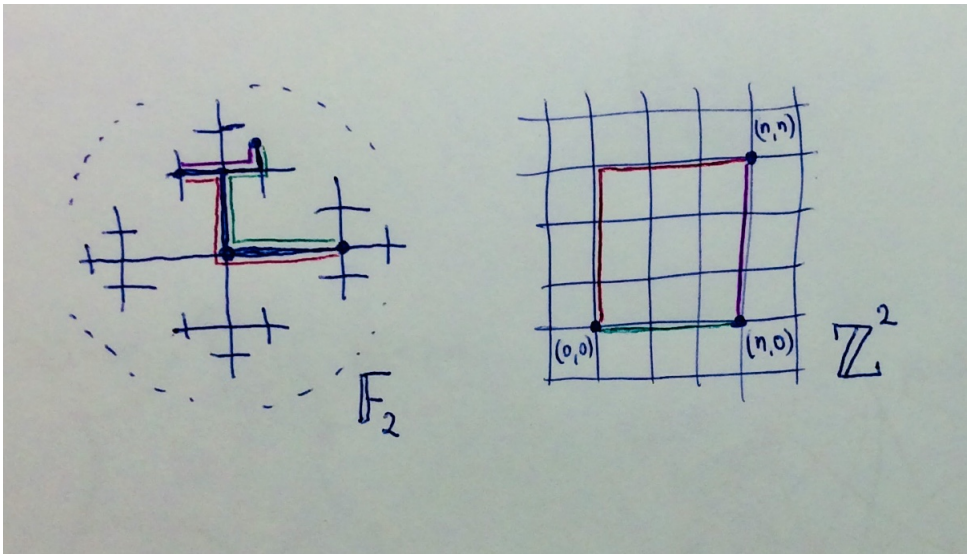
Важные примеры

- *Свободная группа $\mathbb{F}_n$ является гиперболической для любого n.*
- *Группа $\mathbb{Z}^2$ не является гиперболической.*
- *Любая конечная группа является гиперболической.*

---

1) Граф Кэли свободной группы является деревом, а потому является 0-гиперболическим пространством (так как дерево не имеет циклов, то единственная возможность для геодезического треугольника: это быть трезубцем, в таком случае каждая сторона содержится в объединении оставшихся двух сторон). На рисунке изображен типичный геодезический треугольник, и разные его стороны покрашены в разные цвета.

2) Рассмотрим изображенные на картинке геодезические треугольники $[(0,0),(n,0),(n,n)]$ (где опять разные стороны покрашены в разные цвета). Видно, что радиус окрестности объединения зеленой и фиолетовой сторон, которая содержит красную сторону, растет с ростом n и не ограничивается никакой константой.



3) Если G - конечная, то диаметр его графа Кэли ограничен числом $|G|$. Но в таком случае что угодно лежит в $|G|$-окрестности чего угодно, а значит любой геодезический треугольник является $|G|$-тонким.

Утверждение

Пусть G, H - гиперболические группы, тогда $G * H$ тоже является гиперболической.

Пусть M и N - порождающие множества для G и H соответственно, пусть $A = M \cup N$. И здесь как раз полезно перейти к дискретному случаю. Пусть X это вершины графа Кэли $C_A(G * H)$, геодезическими мы будем называть последовательности в X, где две последовательные точки находятся на расстоянии 1. Тогда если мы докажем для некоторого δ, что любая сторона треугольника в X содержится в некоторой δ-окрестности двух других; то (раз, как мы с вами уже обсуждали, стрелочка $R \Rightarrow G$ работает и в дискретном случае) - значит для любых четырех точек $x, y, z, w \in X$ будет выполнено условие Громова (правда уже с новой константой δ):

$$(x, z)_w \geq \min\{(x, y)_w, (y, z)_w\} - \delta$$

Тогда если рассмотреть произвольные четыре точки $x, y, z, w \in C_A(G * H)$, то на расстоянии не больше 1 от каждой можно найти точку из X. Если сдвинуть точки на расстояние не больше 1, то величина $d(x, y)$ изменится не больше чем на 2, а значит $(x, y)_z$ изменится не больше чем на 3. Таким образом выражение $(x, z)_w - \min\{(x, y)_w, (y, z)_w\}$ изменится самое больше на 9, а значит для $C_A(G * H)$ будет выполнено условие Громова с константой $\delta + 9$. Но это пространство уже геодезическое, а значит для некого верна эквивалентность определений, а значит группа $G * H$ будет гиперболической. Также отметим, что если для G (аналогично и для H) выполняется условие Рипса с константой δ, то будет выполнено "дискретное" условие Рипса с константой $\delta + 1$: так как для каждой точки x в δ-окрестности можно найти точку y на некоторой другой стороне, а в свою очередь уже от y на расстоянии не больше 1 найти элемент группы G; таким образом от x мы нашли в $\delta + 1$-окрестности точку на другой стороне, представленную элементом группы.

Если резюмировать сказанное выше: то можно ограничиться случаем, когда вершины геодезического треугольника - это элементы группы (т.е. не лежат внутри

ребер графа Кэли). Также мы помним, что $d(gx, gy) = d(x, y)$ - поэтому "сдвинув" треугольник на подходящий элемент группы всегда можно добиться, чтобы одна из вершин стала нейтральным элементом. Итак после сдвига у нас есть треугольник $[e, y, zy]$, и нужно показать, что $[e, zy]$ лежит в некоторой окрестности $[e, y]$ и $[y, zy]$, радиус которой не зависит от выбора треугольника. Пусть $y = x_n x_{n-1} \dots x_1$ и $z = \theta_m \theta_{m-1} \dots \theta_1$ - приведенные формы слов, где каждая буква - это нетривиальный элемент либо G либо H (то есть буква в данном случае - это целое слово в алфавите A), причем соседние буквы принадлежат разным сомножителям, а потому не получается никаких сокращений. Обозначим $y_i = x_i x_{i-1} \dots x_1$ и $z_i = \theta_i \theta_{i-1} \dots \theta_1$. Тогда ясно, что в силу единственности приведенной формы:

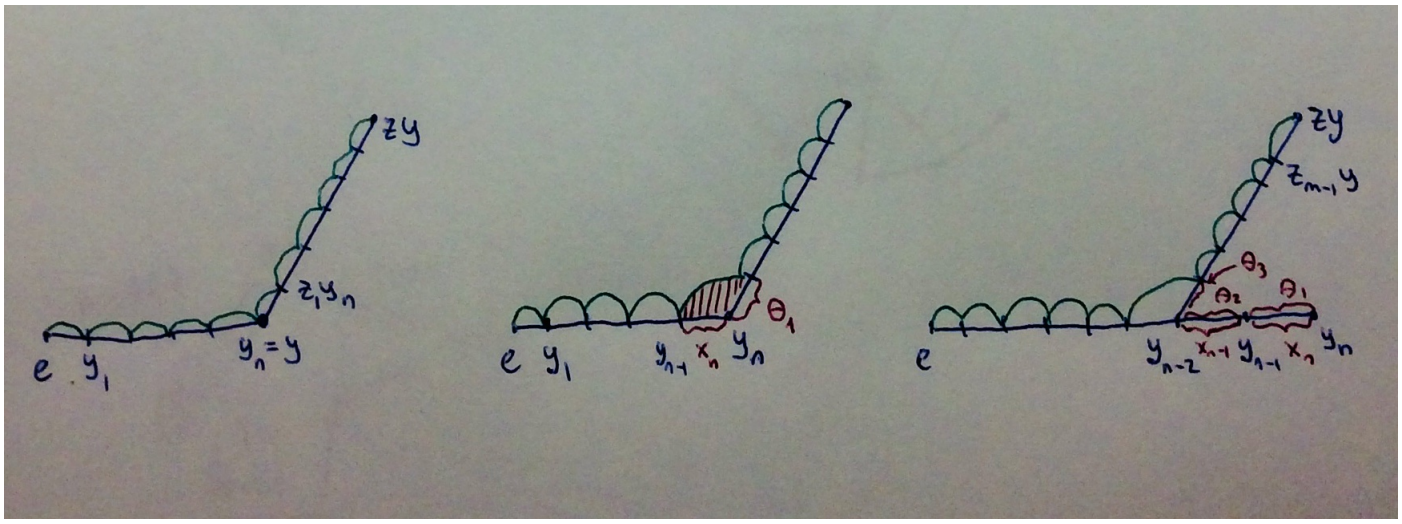
$$[e, y] = [e, y_1] \cup \dots [y_{n-1}, y_n]$$

$$[y, zy] = [y_n, z_1 y_n] \cup \dots \cup [z_{m-1} y_n, z_m y_n]$$

Также ясно, что геодезическая $[e, zy]$ получается из приведенной формы zy и допускает такое разложение опять-таки в силу единственности приведенной формы:

$$[e, zy] = [e, y_1]^* \cup [y_1, y_2]^* \cup \dots \cup [z_{m-1} y_n, z_m y_n]^*$$

здесь я поставил звездочки, чтобы подчеркнуть, что геодезические этого разложения не обязаны совпадать с геодезическими из разложения первых двух сторон: так как может существовать несколько геодезических, соединяющих заданные точки. Но так как мы уже знаем, что из определения непосредственно вытекает, что в δ-гиперболических пространствах для любых двух точек соединяющая их геодезическая лежит в δ-окрестности другой соединяющей их геодезической - то самое главное понять, как узловые точки $[e, zy]$ связаны с узловыми точками $[e, y]$ и $[y, zy]$. Узловые точки могут отличаться только если будут сокращения в словах, а так как изначальные слова были несократимыми, то единственное сокращение может появиться на стыке y и z, и возможны три ситуации (геодезическая $[e, zy]$ изображена зеленым цветом):



Левый случай - стыкующиеся буквы оказались из разных сомножителей, а потому никаких сокращений быть не может - и тогда узловые точки в точности

совпадают: но так как по замечанию каждый геодезический фрагмент содержится в δ-окрестности другого, то и вся сторона $[e, zy]$ окажется в δ-окрестности двух других сторон.

Центральная ситуация: стыкующиеся буквы x_n и θ_1 лежат в одном сомножителе (для определенности пусть это будет G), но не сокращаются до нейтрального элемента. Тогда в силу δ-тонкости красного треугольника, "длинная" его сторона, входящая в $[e, zy]$, будет лежать в δ-окрестности других сторон - и опять условие Рипса выполнено.

Правая ситуация: когда стыкующиеся буквы x_n и θ_1 мало того, что лежат в одном сомножителе, так еще и сокращаются полностью. Фактически это будет означать, что пройдя одним путем по $[e, y]$ уже в $[y, zy]$ мы пройдем по нему же только в обратном направлении (ну с точностью до неединственности геодезической). Если крайние буквы сократились - тогда смотрим на следующие: x_{n-1} и θ_2, если они тоже сократились - то так будем продолжать до тех пор, пока не окажемся либо в центральной, либо левой ситуации. Каждое полное сокращение будет увеличивать уходящий вправо штырь. Но в любом случае условие Рипса для этого треугольника будет выполнено с константой δ, такой что и G, и H являются δ-гиперболическими (то есть можно просто максимум из их собственных констант взять, и это все по модулю того, что переход к дискретному случаю стоил нам некоторых модификаций константы гиперболичности δ). Таким образом $G * H$ - гиперболическая группа.

Замечание:

Из этого утверждения получается упомянутый раньше результат, что $\mathbb{F}_n$ являются гиперболическими, а также и более нетривиальные примеры: например $\mathbb{Z}_2 * \mathbb{Z}_3$ или же бесконечная группа Диэдра $\mathbb{Z} * \mathbb{Z}_2 \cong \mathbb{Z} \rtimes \mathbb{Z}_2 \cong D_\infty$. Также отмечу, что этот результат не верен для бесконечного числа свободных сомножителей: так как гиперболическая группа обязана быть конечно-порожденной.

Определение

Пусть X, Y - метрические пространства. Функция $f : X \to Y$ называется квазиизометрией, если существуют $A, B, C > 0$, что выполнены два условия: для любых точек $x_1, x_2 \in X$ верно:

$$\frac{1}{A} d(x_1, x_2) - B \leq d(f(x_1), f(x_2)) \leq A \cdot d(x_1, x_2) + B$$

А также для любого $y \in Y$ существует $x \in X$, что

$$d(y, f(x)) \leq C$$

Также будем говорить о квазиизометрическом отображении, если выполнено только первое условие.

Метрические пространства X, Y будем называть квазиизометричными, если существует квазиизометрия $f : X \to Y$, в таком случае будем писать $X \underset{q.i.}{\sim} Y$.

Нетрудно заметить, что композиция двух квазиизометрий/квазиизометрических отображений будет квазиизометрией/квазиизометрическим отображением; таким образом квазиизометричность - это отношение эквивалентности. Условие с

неравенствами могут показаться навороченными (особенно константа $\frac{1}{A}$), но это всего лишь удобный способ записи того, что $d(f(x_1), f(x_2))$ оценивается с двух сторон некоторыми линейными функциями от $d(x_1, x_2)$, то есть первое условие эквивалентно существованию A, B, C, D, для которых выполнено:

$$C \cdot d(x_1, x_2) + D \leq d(f(x_1), f(x_2)) \leq A \cdot d(x_1, x_2) + B$$

Также отмечу, что для квазиизометрии $f : X \to Y$ всегда есть квазиизометрический обратный $g : Y \to X$, заданный формулой $g(y) = x$, где x - это один из тех x из второго условия. Левый обратный в данном случае понимается не совсем в классическом виде, а именно, что существует некоторая константа C, что для любого x выполнено: $d(x, g \circ f(x)) \leq C$; аналогично определяется и правый обратный. Иными словами обратный возвращает не совсем прообраз своего аргумента, а некоторую точку, которая находится близко от прообраза (конкретно: в окрестности прообраза фиксированного для всего пространства радиуса). И это отражение общей идеологии гиперболических пространств, где геометрические объекты рассматриваются с огромной долей гибкости. Кстати, гиперболичность в данном случае - не предел, и в математике есть раздел *грубая геометрия* (coarse geometry), где геометрические объекты рассматриваются с точностью до еще большей гибкости: и *грубым вложением* в данном случае называется отображением $f : X \to Y$, для которого существуют возрастающие функции $\rho, \theta : [0, +\infty) \to [0, +\infty)$ с условием $\lim\limits_{t \to +\infty} \rho(t) = \lim\limits_{t \to +\infty} \theta(t) = +\infty$, для которых выполнено:

$$\theta(d(x_1, x_2)) \leq d(f(x_1), f(x_2)) \leq \rho(d(x_1, x_2))$$

то есть линейные оценки из гиперболического подхода заменяются произвольными монотонными; условие же грубой эквивалентности дословно переписывается с аналогичного условия из квазиизометричного мира, а именно: грубое вложение $f : X \to Y$ называется *грубой эквивалентностью*, если существует константа C, что для любого $y \in Y$ существует $x \in X$, что $d(f(x), y) \leq C$, более лаконично это условие можно переписать как $B_C(f(X)) = Y$). Особое место в этой теории занимают группы G, допускающие $G \hookrightarrow \ell^2$ грубое вложение в гильбертово пространство, у таких групп огромное количество приложений (например, для таких групп верна гипотеза С.П. Новикова о высших сигнатурах, являющаяся на сегодняшний день одной из самых важных нерешенных топологических задач).

Фактически условие квазиизометричности означает, что из бесконечности пространства выглядят одинаково, а поведение на "конечных масштабах" непринципиально. Классический пример квазиизометричности - это $\mathbb{Z} \underset{q.i.}{\sim} \mathbb{R}$, и квазиизометрия задается тождественным вложением $\mathbb{Z} \hookrightarrow \mathbb{R}$ - оба условия проверить не составит труда. И хотя топологии пространств принципиально отличаются - если все больше увеличивать zoom, то $\mathbb{Z}$ будет все больше похоже на $\mathbb{R}$, и разрывы будут все меньше заметны. Другой классический пример квазиизометричных пространств - это $G \underset{q.i.}{\sim} C_A(G)$ для произвольного порождающего множества A, причем квазиизометрия опять задается тождественным вложением графа $G \hookrightarrow C_A(G)$ в вершины своего графа Кэли. Понятие квазиизометрии является исключительно важным для теории гиперболических пространств из-за следующего утверждения:

Теорема

Пусть X, Y - геодезические пространства. Пусть X - гиперболическое пространство и $X \underset{q.i.}{\sim} Y$. Тогда Y тоже гиперболическое.

Фактически, эта теорема показывает меру, с точностью до которой нужно рассматривать гиперболические пространства и чем нужно пренебрегать: интуитивно это означает, что поведение в ограниченных окрестностях не имеет особого значения для гиперболических пространств, и что их нужно рассматривать не под микроскопом, а в телескоп; а также это иллюстрация некоторой идеологии, что гиперболичность обычно гибка к тому, что допускает двухсторонние линейные оценки - дальше мы будем рассматривать квазигеодезические - и они будут еще одним аргументом в пользу этого).

Замечание:

Требование геодезически пространств принципиально, и в общем случае гиперболичность не является квазиизометрическим инвариантом, в чем легко убедиться, рассмотрев следующий классический контрпример: пусть пространство X - это график функции $f(x) = |x|$ с метрикой, унаследованной от плоскости $\mathbb{R}^2$, где он находится. Тогда если рассмотреть точки $x = (-2n, 2n)$, $y = (2n, 2n)$, $z = (n, n)$, $w = (0, 0)$, то

$$(x, z)_w - \min\{(x, y)_w, (y, z)_w\} = \left(\frac{3 - \sqrt{5}}{2} - (2 - \sqrt{2})\right) n \approx -0.2n$$

И это никак не может быть $\geq -\delta$ для некоторого δ - иными словами условие Громова не выполняется ни для каких δ, а значит X не является гиперболическим пространством (для не являющихся геодезическими пространств гиперболичность обычно определяется через условие Громова). Легко заметить, что $\mathbb{R} \underset{q.i.}{\sim} X$, и квазиизоморфизм задается формулой $x \mapsto (x, |x|)$, но при этом $\mathbb{R}$ является гиперболическим.

Из важных следствий этой теоремы хочется отметить следующее:

Следствие

• *Пусть $H < G$ и $|G : H| < \infty$. Тогда G - гиперболическая $\Leftrightarrow$ H - гиперболическая.*

• *Пусть $N \lhd G$ и $|N| < \infty$. Тогда G - гиперболическая $\Leftrightarrow$ G/N - гиперболическая.*

Иными словами гиперболичность и подгруппы конечного индекса являются друзьями. В первом случае вложение $H \hookrightarrow G$ а во втором случае эпиморфизм $G \to G/N$ индуцирует квазиизоморфизм между соответствующими группами; а значит и между их графами Кэли, так как для любой группы K верно $K \underset{q.i.}{\sim} C_A(K)$. То есть, к примеру, в первом случае мы получим:

$$C_B(H) \underset{q.i.}{\sim} H \underset{q.i.}{\sim} G \underset{q.i.}{\sim} C_A(G)$$

где B и A - порождающие множества для H и G соответственно. Так как графы Кэли - это геодезические пространства, то из нашей теоремы получаем эквивалентность гиперболичности в двух данных случаях. Читателю предлагается самостоятельно проверить квазиизометричность упомянутых выше гомоморфизмов. Это следствие помогает получить серии новых примеров гиперболических групп - к примеру, $\mathbb{Z} \times \mathbb{Z}_5$ будет гиперболической, также это следствие доказывает вторым способом

гиперболичность бесконечной группы Диэдра $D_\infty \cong \mathbb{Z} \rtimes \mathbb{Z}_2$, так как она содержит изоморфную $\mathbb{Z}$ подгруппу индекса 2 (первый способ - это использовать изоморфизм $D_\infty \cong \mathbb{Z}_2 * \mathbb{Z}_2$).

Также хочется отметить следующий теоретический факт, имеющий огромное историческое значение:

Теорема

Пусть M^n - n-мерное многообразие отрицательной кривизны, тогда:

$$\pi_1(M^n) \underset{q.i.}{\hookrightarrow} \mathbb{H}^n$$

здесь $\underset{q.i.}{\hookrightarrow}$ - это квазиизометрическое вложение - то есть квазиизометрия, только без второго условия, $\mathbb{H}^n$ - стандартное n-мерное гиперболическое пространство, т.е. n-мерный аналог плоскости Лобачевского; у него тоже есть много моделей, например модель гиперболоида: $\mathbb{H}^n = \{x_0^2 - x_1^2 - \ldots - x_n^2 = 1\} \subset \mathbb{R}^{n+1}$. Громов пришел к понятию гиперболических групп, пытаясь понять какие групповые свойства выделяют фундаментальные группы многообразий отрицательной кривизны среди всех групп - и пришел к гиперболическим группам, которые являются обобщением фундаментальных групп многообразий отрицательной кривизны. Позволяя себе словесные спекуляции - можно сказать, что гиперболическая теория - это способ определять понятие отрицательной кривизны на пространствах, где есть только метрика и нет гладкой структуры.

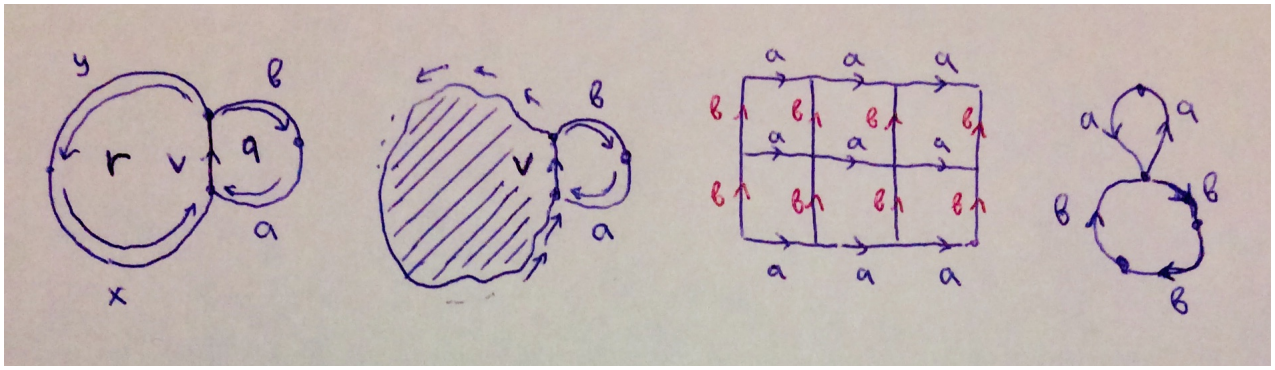
Но гиперболические группы связаны не только с геометрией: одно из их главных преимуществ, что они особенно гибки и податливы ко всякого рода вопросам алгоритмической разрешимости, многие из которых решаются в гиперболических группах: например проблема равенства слов, сопряженности и даже изоморфизма групп, хотя и не все: вопрос принадлежности элемента заданной подгруппе не всегда разрешим в гиперболических группах (такая задача называется *проблемой вхождения*). В принципе связь гиперболичности с алгоритмической разрешимостью вполне закономерна, так как обе эти теории имеют очень глубокую геометрическую природу: в геометричности гиперболичности мы уже убедились; связь алгоритмических вопросов с геометрией стала проявляться очень давно, где-то в первой половине 20-ого века. Давайте немного об этом расскажу:

Одним из основных понятий в этом направлении является диаграммы ван Кампена: пусть $G = \langle A|R\rangle$ - группа заданная копредставлением, также предположим, что если $r \in R$, то и $r^{-1} \in R$ (если это не так - мы всегда к R можем добавить все его обратные), также давайте называть слово $\omega \in \mathbb{F}(A)$ тривиальным, если $\omega =_G 1$. Чтобы понять, что такое диаграмма ван Кампена: пойдем путем "от частного к общему": соотношения мы будем визуализировать многоугольниками, у которых на ребрах последовательно будут написаны буквы, из которых состоит соответствующее соотношению слово. Заметим, что склейкой многоугольников можно визуализировать следующую операцию: пусть $r = xvy$ и $q = avb$ (или даже более общая ситуация, когда общее подслово является подсловом в циклическом смысле, если считать, что следующая после последней

буквы будет первая буква): тогда раз $r, q \in R$, то $r =_G q =_G 1$, а значит $v = a^{-1}b^{-1}$ и получаем, если подставить это выражение в формулу для r, что $xvy = xa^{-1}b^{-1}y =_G 1$: то есть на уровне алгебры мы получили новое тривиальное слово, заменив кусок слова r соотношением, получаемым из соотношения q. На уровне же геометрии это можно визуализировать приклейкой соответствующего q многоугольника к многоугольнику, соответствующему p по их общему подслову v: тогда у полученного сложного многоугольника вдоль границы как раз будет читаться полученное $xa^{-1}b^{-1}y$ (если стрелка направлена вдоль направления чтения - то берем обратный к соответствующему ей слову или букве). Фактически, эта операция - это микс умножения и сопряжения, так как:

$$xa^{-1}b^{-1}y = x(a^{-1}b^{-1}v^{-1}vyx)x^{-1} = x((vba)^{-1}(vyx))x^{-1}$$

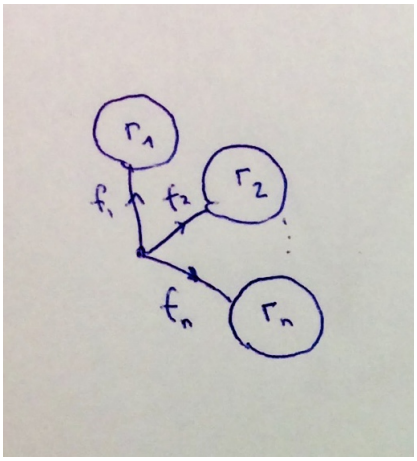
при этом любой циклический сдвиг - это сопряжение: $vba = a^{-1}(avb)a$ и $vyx = x^{-1}(xvy)x$ (здесь возник обратный к соотношению - и именно поэтому мы требуем, чтобы если $r \in R$, то и $r^{-1} \in R$). В более общей ситуации, когда многоугольник $q = avb$ мы приклеиваем к очень сложной конструкции, по границе которой читается тривиальное слово в G - после склейки читаемое вдоль границы все равно будет тривиально из тех же аргументов: потому что на алгебраическом языке результат этой склейки - это использование соотношения $v = a^{-1}b^{-1}$: Обычно этот процесс иллюстрируют примером группы $\mathbb{Z}^2 = \langle a, b | [a, b] = 1 \rangle$ и диаграммой для соотношения $[a^3, b^2]$. Также в склейке может не быть необходимости - нарисуем также диаграмму для a^2b^3 в группе $\langle a, b | a^2 = b^3 = 1 \rangle$:



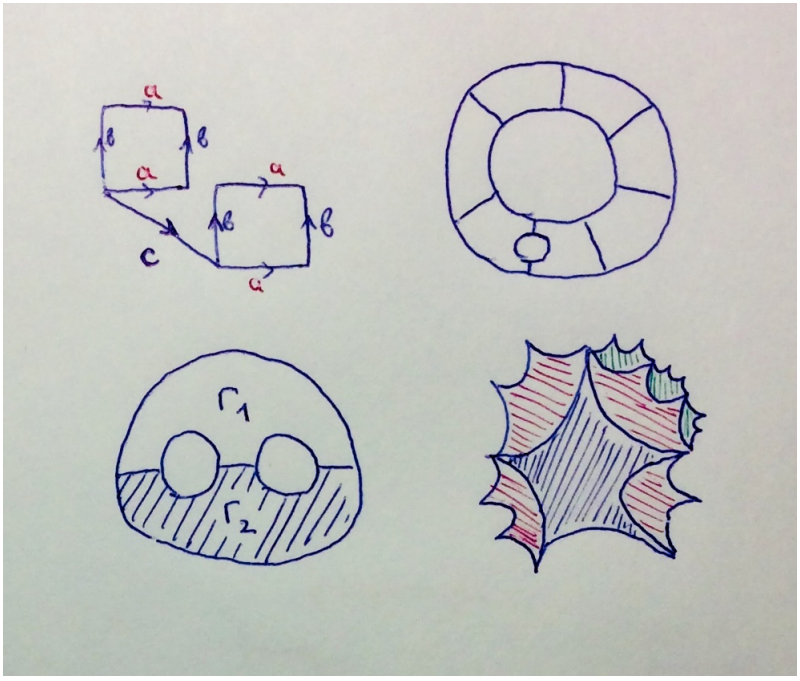
И зайдем теперь с другой стороны: так как $\omega =_G 1 \Leftrightarrow \omega \in \langle\langle R \rangle\rangle$, где $\omega \in \mathbb{F}(A)$ - то для произвольного нейтрального в G слова мы получаем разложение:

$$\omega = (f_1^{-1}r_1f_1)\dots(f_n^{-1}r_nf_n)$$

где $f_i \in \mathbb{F}(A)$ и $r_i \in R$. И тогда ω можно задать изображенной на рисунке *диаграммой ван Кампена*. Причем на практике так часто получается, что многие $f_i = 1$, а потому в блоки группируются несколько r_i, которые между собой могут частично сокращаться, образуя склейки; также некоторые сопряжения могут сводить лишь к циклическим сдвигам соотношений: к примеру если в некоторой группе $abcd =_G 1$, то и $bcda = a^{-1}(abcd)a =_G 1$, то есть сопряжение элемента задается тем же многоугольником (которые в этой науке называются клетками). Диаграмма ван Кампена не единственна, и в таком общем виде она обычно допускает массу дополнительных склеек и сокращений:



Но в реальности самая мякотка теории содержится не в этих веревочках, а в двумерных областях; на практике часто веревочки сокращаются; хотя и не всегда: что хорошо видно на примере группы $\langle a, b, c | [a, b] = 1 \rangle$ и тривиального элемента $\omega = [a, b]c^{-1}[a, b]c$ - и так как сопрягающий элемент c не имеет даже общих букв с соотношениями, то избавиться от него нельзя. Самое главное поле применение диаграмм ван Кампена - это работа с алгоритмической разрешимостью равенства слов: так как $g = h \Leftrightarrow gh^{-1} = e$ - то алгоритм часто удобно визуализировать на этих диаграммах, так как результат описанных выше подстановок воспринимается сложнее приклеивания клеток. Также отмечу на будущее, что на примере рассмотренных ранее диаграмм могло сложиться впечатление, что двумерные блоки имеют простую комбинаторную структуру: типа квадратиков в тетрадях в клеточку; в реальности их взаимные склеивания могут быть очень хитрыми: начиная от того, что клетка может вклеиться внутрь полосы, и заканчивая тем, что область склейки двух клеток не обязана быть связной. Некоторые аномалии я изобразил на рисунках: вспоминайте о них, если рассуждения с клетками у вас получаются очень простыми и с малым количеством вариантов взаимного расположения. Кстати, нижнее правое аномальное взаимное расположение как раз типично для гиперболических групп, где все вытянутое и острое:



Если определять диаграмму ван Кампена более формально - то это двумерный комплекс, у которого на ребрах стоят метки в виде букв алфавита, а каждая двумерная клетка соответствует некоторому порождающему соотношению R. Границей ∂D называется слово, которое получается, если стартовав из любой вершины выписывать подряд все буквы меток, стоящие на проходимых нами ребрах (буква, если проходим вдоль ребра, и ее обратная, если проходим в противоположном направлении). Ясно, что если строить граничное слово, начиная с двух разных точек, то результат будет отличаться только циклической перестановкой, а на уровне группового элемента - лишь сопряжением. Резюмируем все вышесказанное в виде леммы:

Лемма (ван Кампен)

Пусть $G = \langle A|R\rangle$ *и* $\omega \in \mathbb{F}(A)$. *Тогда* $\omega =_G 1 \Leftrightarrow \omega = \partial D$ *для некоторой диаграммы ван Кампена.*

$\Rightarrow$ Если $\omega =_G 1$ - то $\omega \in \langle\langle R\rangle\rangle$ - а значит ω представляется как произведение сопряженных к элементам из R, и по этому разложению можно построить диаграмму ван Кампена, как мы обсуждали выше.

$\Leftarrow$ Также мы обсуждали, что операция приклеивания клетки не меняет того, что граница является тривиальным элементом в группе. Также этого не меняет добавление веревочек: т.к. они соответствуют простому групповому сопряжению.

Пусть D - диаграмма ван Кампена, определим функции:

$$\mathrm{Area}(D) = \text{ количество клеток в } D$$

$$\mathrm{Area}(\omega) = \min_{\partial D = \omega} \mathrm{Area}(D)$$

$$D(n) = \max_{|\omega| \le n} \mathrm{Area}(\omega)$$

Функция $D(n)$ называется *функцией Дэна* группы G (иногда пишут $D_G(n)$ если важно подчеркнуть для какой группы мы функцию Дэна вычисляем), и на человеческом языке она равна минимальному числу сопряженных соотношений, которые нужно перемножить, чтобы получить любой тривиальный элемент ω группы G с $|\omega| \le n$. Или иными словами: такое минимальное число M, что если рассмотреть всевозможные M-кратные произведения всевозможных сопряжений к соотношениям - то получится множество, содержащее множество всех слов длины $\le n$, соответствующих тривиальному элементу. Другая интерпретация человеческими терминами - это сколько применений соотношений из R хватит, чтобы преобразовать любое тривиальное слово длины $\le n$ к единице. Разумеется, функция Дэна зависит от копредставления группы, но для двух различных копредставлений соответствующие функции Дэна зажимаются двухсторонними оценками (причем интересно, что если $f(n)$ и $g(n)$ являются функциями Дэна одной и той же группы, но построенные по разным копредставлениям, то для некоторых констант A, B, C выполнено $g(n) \le Af(Bn) + Cn$, ну и ясно, что из симметричности ситуаций аналогичная оценка может быть записана и для $f(n)$. Оценки очень похожи на оценки из квазиизометричности или оценки для функций роста, но бросается в глаза это странное слагаемое $+Cn$, природа которого кроется главным образом в возможности добавлять "пустышки" в копредставление: для двух копредставлений циклической группы $\langle a|\emptyset\rangle$ и $\langle a, b|b = 1\rangle$ функция Дэна для

первого конпредставления равна 0, так как в этом конпредставлении отсутствуют как соотношения, так и непустые несократимые тривиальные слова; тогда как для второго конпредставления функция Дэна равна n, т.к. нужно минимум n раз применять соотношение, чтобы слово $b^n = bb\dots b$ привести к единичному, иными словами добавление фиктивного b увеличило функцию Дэна на n). Если f и g зажимаются такими двухсторонними оценками, а именно для некоторых констант A, B, C выполнено $\frac{1}{A}f\left(\frac{n}{B}\right) - Cn \leq g(n) \leq Af(Bn) + Cn$, то будем говорить, что функции f и g *эквивалентны*. И хотя функция Дэна не является инвариантом группы, инвариантом является ее класс роста по этому отношению эквивалентности. Оказывается, верна следующая фундаментальная теорема:

Теорема (Громов)
G является гиперболической $\Leftrightarrow$ существует $C > 0$, такое что $D(n) \leq Cn$.

Иными словами: гиперболические группы - это в точности группы с линейной функцией Дэна. Так как $D(n)$ - это фактически площадь диаграммы ван Кампена (если считать площадь каждой клетки равной 1), а n - это длина $\omega = \partial D$, то есть фактически периметр диаграммы, то неформально на геометрическом языке это означает, что в гиперболических пространствах площадь линейным образом зависит от периметра (в математике неравенства, связывающие площадь и периметр, обычно называются *изопериметрическими неравенствами*). В какой-нибудь евклидовой геометрии это утверждение было бы абсурдным: площадь должна быть квадратичной от своих линейных габаритов. Но если проводить все-таки аналогию с евклидовой геометрией для выработки интуиции - то на плоскости обычно площадь линейным образом зависит от периметра для очень вытянутых и узких фигур (что типично для гиперболической геометрии с ее треугольниками, углы которых очень тоненькие). Также если вспомнить школьную евклидову формулу для площади треугольника через периметр p и радиус вписанной окружности $S = \frac{pr}{2}$, а дальше вспомнить, что в некотором смысле мы можем считать, что в гиперболической геометрии радиусы вписанных окружностей во всех треугольниках ограничены абсолютной константой - то становится чуть понятнее, почему такая оценка не нарушает законы мироздания.

Несколько примеров:

• $D_{\mathbb{F}_2}(n)$ в некотором смысле ее можно считать равной 0, так как множество тривиальных ω с условием $|\omega| \leq n$ состоит только из e - и для получения этого слова вообще не нужно перемножать соотношения, к слову которых вообще нет.

• $D_G(n)$ не более чем линейна для гиперболических G - в этом и состоит теорема Громова.

• $D_{\mathbb{Z}^2}(n)$ квадратична. Ключевой ингредиент доказательства - это то, что стандартная диаграмма ван Кампена для $[a^n, b^m]$ состоит из nm клеток. На самом деле квадратичными будут и функции $D_{\mathbb{Z}^k}(n)$.

Замечание:

Замечу, что для функции Дэна не существует никаких разумных оценок сверху (в отличие от экспоненциальной оценки для функции роста, туманные и отдаленные ассоциации с которой возможно возникают). И в качестве эффектного иллюстрирующего примера рассмотрим группы гидры (hydra group):

$$G_k = \langle a_1, a_2, \ldots, a_k, t | t^{-1}a_1 t = a_1, t^{-1}a_i t = a_i a_{i-1}, i > 1 \rangle$$

где a_i можно мыслить как головы гидры, а на процесс последовательного сопряжения на t смотреть как на процесс борьбы Геркулеса с чудовищем. А также рассмотрим ее HNN-расширение:

$$\Gamma_k = \langle a_1, a_2, \ldots, a_k, t, p | t^{-1}a_1 t = a_1, t^{-1}a_i t = a_i a_{i-1}, [p, a_i t] = 1, i \geq 1 \rangle$$

Тогда

$$D_{\Gamma_k}(n) \approx A_k(n)$$

где $A_k(n)$ - функция Аккермана, которая растет сказочно быстро, и определяется рекуррентным образом: $A_0(n) = n + 1$, $A_{m+1}(n) = A_m^{n+1}(1)$ - и здесь степень - это степень композиции. То есть:

$$A_1(n) = n + 2 \qquad A_2(n) = 2n + 3 \qquad A_3(n) \approx 2^n \qquad A_4(n) \approx \underbrace{2^{2^{2^{2}}}}_{n \text{ раз}}$$

функцией Аккермана иногда называют функцию $f(n) = A_n(n)$ и по внешнему виду A_4 видно, что это очень быстро-растущая функция. Часто функция Аккермана служит источником контрпримеров в самых разных сюжетах математической логики. Но вернемся к группам - вдумайтесь! У группы Γ_4 6 порождающих и 8 коротких соотношений, но при этом для приведения тривиального слова (т.е. равного 1 в группе) длины 5 может потребоваться применять соотношения квадриллионы-ундециллионы раз, чтобы привести его к тождественному. Поэтому разумные оценки на функцию Дэна записать невозможно.

Немного истории: группы G_k возникли как групповая версия так называемой "игры в гидру", которая сводится к следующему: есть конечный алфавит $\{a_1, \ldots, a_k\}$; и на словах в этом алфавите задано преобразование, которое стирает первую букву, а затем каждую букву оставшегося слова заменяет по правилу $a_1 \mapsto a_1$ и $a_i \mapsto a_i a_{i-1}$ где $i > 1$ (Геркулес отсекает одну голову у гидры, но вырастают новые). К примеру слово $a_1 a_2 a_3$ будет преобразовываться так:

$$a_1 a_2 a_3 \mapsto a_2 a_1 a_3 a_2 \mapsto a_1 a_3 a_2 a_2 a_1 \mapsto \ldots$$

И есть теорема, которая утверждает, что начиная с любого слова за конечное число шагов мы придем к пустому слову; а также, что слово $a_k^n = a_k a_k \ldots a_k$ приводится к пустому за $A_k(n)$ шагов. И чтобы понять откуда берутся эти квадриллионы-ундециллионы в соответствующей функции Дэна - попробуйте поиграть в эту игру с начальным словом $a_4 a_4 a_4 a_4$ - и прочувствуйте всю боль Геркулеса.

Поэтому с функцией Дэна $D(n)$ очень сложно работать: мы видели насколько плохая и непокорная функция Дэна у описанного выше HNN-расширения группы гидры, но даже для группы $\mathbb{Z}^2$ вычисление функции Дэна не является тривиальной задачей и сводится к солидным аналитическим выкладкам. Поэтому хочется чего-то идейно близкого, но при этом осязаемого. И самый лучший на это кандидат - это теория малых сокращений: начнем с базовых определений.

Копредставление группы $G = \langle A|R\rangle$ называется *симметричным*, если выполнены три условия: для любого $r \in R \Rightarrow r^{-1} \in R$, кроме того $uv \in R \Rightarrow vu \in R$, а также третье техническое условие: что все $r \in R$ являются циклически приведенными, т.е. не имеют вид $a^{-1}ua$ ни для какой $a \in A$. Второе условие означает, что любые циклические сдвиги соотношений из R остаются там же. Заметим, что если вдруг копредставление не является симметричным - его можно сделать таковым, добавив все обратные и все циклические сдвиги.

Определение

Симметричное конечное копредставление $G = \langle A|R\rangle$ называется копредставлением Дэна (Dehn presentation), если для любого приведенного $\omega \in \mathbb{F}(A)$, что $\omega =_G 1$, некоторый его циклический сдвиг содержит больше половины некоторого соотношения, иными словами некоторый циклический сдвиг ω содержит подслово u, которое также является подсловом некоторого $r \in R$ и $|u| > \frac{|r|}{2}$.

Лингвистически легко запутаться с терминологией, потому что копредставление по английски будет presentation, которое из-за первых букв может возникнуть желание перевести как представление; в свою очередь представление переводится как representation.

Обращаю внимание на то, что u является подсловом не самого ω, а некоторого его циклического сдвига. Связано это с тем, что у слова есть начало и конец, но основа всей этой теории - это диаграммы ван Кампена и их границы, которые можно читать с любого места; и все утверждения в этой теории доказываются по принципу "приклеим что-нибудь к границе" или "посмотрим, что у нас записано вдоль границы", поэтому нужно считать, что после последней буквы идет первая. Поэтому это немного странное условие нужно для ситуаций, когда наше "подслово" начинается ближе к концу ω, а затем продолжается с его начала. Другой способ избежать необходимости рассматривать циклические сдвиги - это ввести понятие *циклического слова*, то есть слова, которое читается не слева направо, а "по кругу"; фактически слово, записанное по окружности. Такой термин также упросит второе условие на копредставление, так как инвариантность относительно циклических сдвигов мы требовали из точно таких же соображений.

Также отмечу, что приведенность ω (т.е. его несократимость в $\mathbb{F}(A)$) требовалась для того, чтобы избежать возможности вставлять aa^{-1} где попало, нарушая тем самым естественную природу подслов. На уровне диаграмм ван Кампена вставить в некотором месте aa^{-1} означает выпустить штырь из того места, куда мы aa^{-1} вставили. Конечность копредставления нужна, потому что главным образом эта теория строится для решения алгоритмических задач, для большей части которых конечность копредставления групп более естественна, хотя и не строго обязательна.

Копредставление Дэна очень важно во всякого рода алгоритмических вопросах, в частности верна следующая теорема:

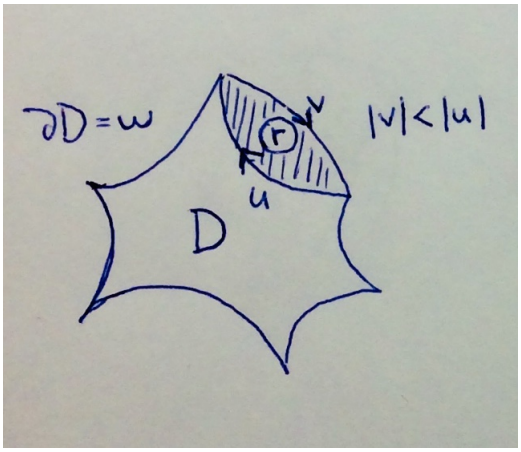
Теорема

В копредставлении Дэна $G = \langle A|R\rangle$ разрешима проблема равенства слов

Иными словами можно написать программу, которые по двум словам $g, h \in \mathbb{F}(A)$ выдаст равны или нет они как элементы группы G. Так как $g = h \Leftrightarrow gh^{-1} = e$, то проблема равенства слов эквивалентна проблеме равенства единице группы. Доказательство этой теоремы очень простое и поучительное: пусть $\omega =_G 1$. Можем считать, что ω циклически приведено, т.е. не имеет вид $\omega = a^{-1}\tilde{\omega}a$. Так как мы имеем дело с копредставлением Дэна, то существует некоторое соотношение $r \in R$, имеющее с циклическим словом ω общее подслово u с $|u| > \frac{|r|}{2}$. Так как в R есть все циклические сдвиги соотношений, то можно считать, что $r = uv$, учитывая, что мы рассматриваем циклическое слово, также можем считать, что $\omega = ux$. Тогда в группе G верно $u = v^{-1}$, и мы можем сделать в ω эту замену, т.е. $\omega = ux =_G v^{-1}x$, тем самым уменьшив его длину минимум на одну букву, т.к. $|u| > |v| = |v^{-1}|$.

Рассмотрим алгоритм, который на каждом шаге проверяет все циклические сдвиги ω на наличие общих подслов u со всевозможными $r \in R$, таких что $|u| > \frac{|r|}{2}$, делает описанную выше замену и дальше вновь повторяет эту процедуру. Если $\omega =_G 1$, то этот алгоритм (называемый алгоритмом Дэна) каждый раз будет уменьшать длину слова минимум на 1 - и в конечном счете приведет слово к единичному. Если же на каком-то шаге алгоритм не сможет найти общее длинное подслово с некоторым соотношением из R - то мы приходим к выводу, что $\omega \neq_G 1$ по определению копредставления Дэна. И уже за n шагов станет понятно, тривиально или нет наше слово, здесь $n = |\omega|$.

На уровне диаграмм ван Кампена этот алгоритм имеет следующую иллюстрацию: на место u мы вклеиваем клетку, и эта часть границы заменяется на v^{-1}, причем из условия копредставления Дэна больше половины периметра вклеиваемой клетки выпадает именно на u - и поэтому в результате склейки уменьшается периметр всей диаграммы ван Кампена минимум на 1.



И оказывается, что гиперболические группы имеют к этому всему самое непосредственное отношение, а именно верна следующая удивительная теорема:

Теорема

Пусть G - конечно-порожденная группа.

Тогда G - гиперболическая $\Leftrightarrow$ G допускает копредставление Дэна.

И из этой теоремы сразу получаем два очень важных следствия: что есть конечно-определенные группы, не допускающие копредставления Дэна (та же $\mathbb{Z}^2$), а также, что любая гиперболическая группа является конечно-определенной. Докажем эту теорему.

$\Leftarrow$ На языке функции Дэна то, что алгоритм Дэна для $|\omega| = n$ определяет тривиальность ω за самое большое n шагов, означает, что для этого копредставления $D(n) \leq n$. Из теоремы Громова вытекает, что группа G гиперболическая.

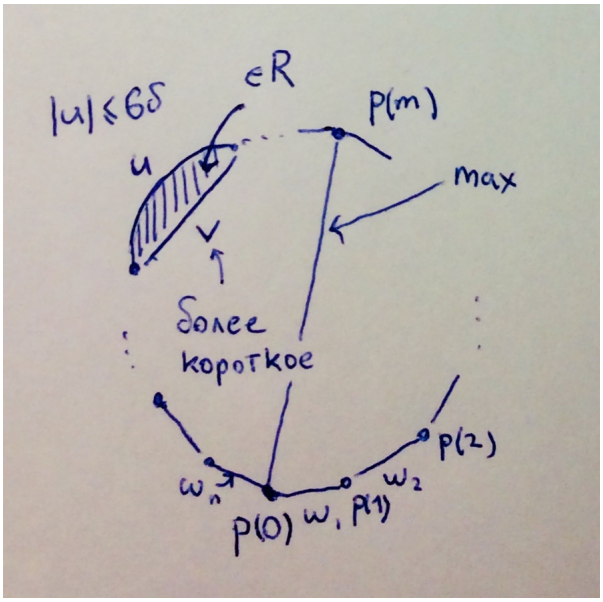
$\Rightarrow$ На самом деле мы даже сможем явно предъявить задающее G копредставление Дэна. Пусть $G = \langle A \rangle$ и δ - константа гиперболичности (причем из эквивалентного условия не на тонкость, а на узкость треугольников). Ясно, что G является гиперболической для любой большей константы (потому что соответствующие большей константе условия гиперболичности более слабые), а потому можем считать, что δ - натуральное. И оказывается, что в роли определяющих соотношений искомого копредставления Дэна можно взять:

$$R = \{\omega : \omega =_G 1 \text{ и } |\omega| \leq 12\delta\}$$

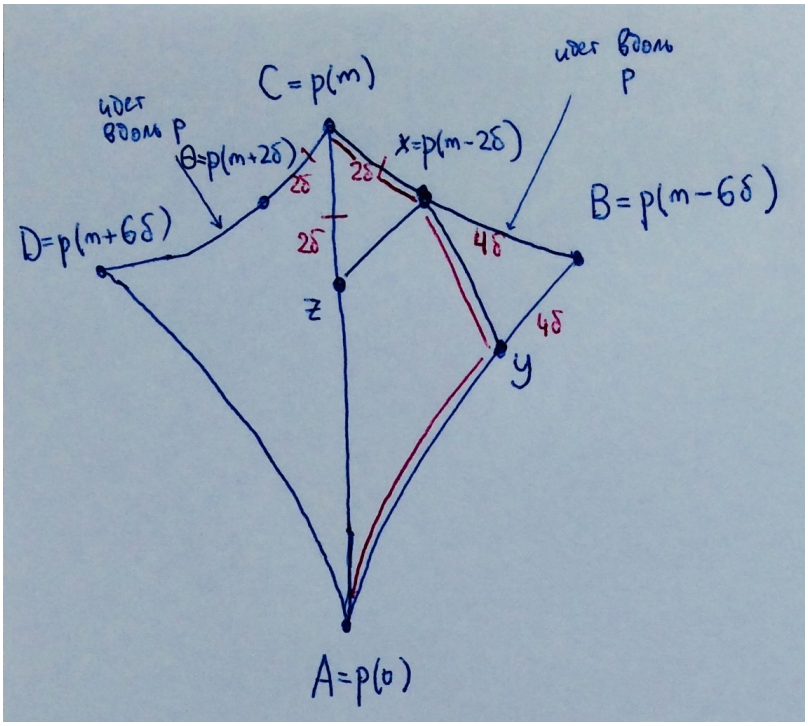
Ясно, что это конечное множество, так как в конечно-порожденной группе все шары конечны. Для доказательства того, что $G = \langle A|R\rangle$, достаточно проверить, что $\omega =_G 1 \ \Rightarrow \ \omega \in \langle\langle R \rangle\rangle$, для проверки чего в свою очередь достаточно показать, что если $\omega =_G 1$, то в *циклическом слове* ω содержится больше половины некоторого слова из R (так как в таком случае мы можем запустить описанный выше алгоритм Дэна, и для полученного соотношения $r = uv$ с общим подсловом u сделать сокращающую длину слова замену $u = v^{-1}$, и продолжать так до тех пор, пока не получим e). Доказывая это условие - мы убиваем сразу двух зайцев: доказываем и что $G = \langle A|R\rangle$, и что это - копредставление Дэна. Это условие очевидно выполнено при $|\omega| \leq 12\delta$ (потому что в таком случае по условию даже $\omega \in R$). Проверим его при $|\omega| > 12\delta$.

Предположим противное: пусть $\omega = \omega_n\omega_{n-1}\dots\omega_1 \in \mathbb{F}(A)$ несократимое как элемент свободной группы слово, где $\omega_i \in A$; и пусть как циклическое словно оно не содержит больше половины никакого соотношения из R. На графе Кэли последовательные точки $\omega_i\omega_{i-1}\dots\omega_1$ соединены ребром, и рассмотрим эти точки вместе с этими ребрами как изометрический путь $p : [0, n] \to C_A(G)$, такой, что $p(i) = \omega_i\omega_{i-1}\dots\omega_1$, а в нецелых точках путь будет проходить в точности по упомянутым выше ребрам. Также имеем $p(0) = e$ и $p(n) = \omega =_G e$, то есть это замкнутая петля. На это можно смотреть так, что p - это путь вдоль границы соответствующей ω диаграмме ван Кампена (пусть и не заполненной внутри клетками), тогда целочисленные подпути будут соответствовать подсловам ω. Ясно, что путь p не является геодезическим (так как геодезическая не может быть замкнутой), но оказывается, что он является локальной геодезической, а именно на любом целочисленном отрезке $[m, k]$ длины $\leq 6\delta$ путь p является геодезическим (который фактически соответствует подслову $u = \omega_k\dots\omega_{m+1}$ циклического слова ω если считать, что m, k рассматриваются по модулю n. На языке же теории групп это означает, что у несократимого в $\mathbb{F}(A)$ слова ω подслова длины $\leq 6\delta$ являются почти несократимыми в G в том смысле, что нельзя сократить, уменьшив при этом длину). Предположим, что такой путь не является геодезическим, тогда путь между $p(m)$ и $p(k)$ можно было бы пройти более коротким чем u словом v, а так как у них одинаковые концы в графе Кэли, то $uv^{-1} =_G 1$, но при этом $|v^{-1}| = |v| < |u| \leq 6\delta$, а значит $|uv^{-1}| \leq 12\delta$, и поэтому $uv^{-1} \in R$; и мы получаем, что ω имеет общий кусок

u со словом $uv^{-1} \in R$, причем такой, что $|u| > \frac{|uv^{-1}|}{2}$, что невозможно в силу нашего предположения.



Теперь рассмотрим такой m, на котором достигается максимум по i выражения $d(e, p(i))$, и рассмотрим два геодезических треугольника $[e, p(m-6\delta), p(m)]$, $[e, p(m), p(m+6\delta)]$. Так как подпути длины $\leq 6\delta$ в пути p являются геодезическими, то можем считать, что геодезические $[p(m-6\delta), p(m)]$ и $[p(m), p(m+6\delta)]$ идут вдоль p. Пусть $A = e$, $B = p(m-6\delta)$, $C = p(m)$, $D = p(m+6\delta)$; рассмотрим $x \in [B, C]$, такой что $d(x, C) = 2\delta$ (иными словами $x = p(m-2\delta)$), $\theta \in [C, D]$, что $d(C, \theta) = 2\delta$ (иными словами $\theta = p(m+2\delta)$), $z \in [A, C]$, что $D(z, C) = 2\delta$ и $y \in [A, B]$, что $d(y, B) = 4\delta$.



В силу выбора m имеем $d(A, B) \leq d(A, C)$.

Условие δ-узкости треугольника $[A, B, C]$ дает, что либо $d(x, y) \leq \delta$, либо $d(x, z) \leq \delta$ в зависимости от взаимного расположения x и internal point на отрезке $[B, C]$. Но где эта internal point находится мы не знаем, а поэтому предположим от противного, что $d(x, y) \leq \delta$. Тогда из неравенства треугольника получаем:

$$d(A, C) \leq d(A, y)+d(y, x)+d(x, C) = (d(A, B)-4\delta)+d(y, x)+2\delta \leq d(A, B)-\delta < d(A, B)$$

Что невозможно, значит $d(x, z) \leq \delta$. Так как треугольники $[A, B, C]$ и $[A, C, D]$ абсолютно равноправны, то аналогичными рассуждениями мы получаем $d(z, \theta) \leq \delta$. Таким образом $d(x, \theta) \leq d(x, z) + d(z, \theta) \leq 2\delta$. Но при этом идущий по сторонам треугольников (а также вдоль p) путь от $p(m - 2\delta)$ до $p(m + 2\delta)$ имеет длину $\leq 6\delta$, а потому является геодезическим, а значит $d(x, \theta) = d(p(m - 2\delta), p(m + 2\delta)) = 4\delta$, что невозможно, так как мы доказали $d(x, \theta) \leq 2\delta$. Полученное противоречие доказывает нашу теорему.

Теорема очень важная, и хотя доказательство может на первый взгляд показаться очень технически тяжелым - оно очень показательное и хорошо иллюстрирует, как узкость треугольников в определении гиперболичности транслируется на обычные групповые свойства элементов группы и возможность сократить некоторые слова. Плюс с теоретической точки зрения это доказательство помогает лучше прочувствовать важные ключевые понятия, в частности метрики на группе: к примеру, в нашей ситуации было $|\omega| = n$ и при этом $|\omega|_G = 0$ - это нужно хорошо понимать.

Копредставления Дэна намного полезнее абстрактной функции Дэна, потому что как минимум они несут с собой явный и прозрачный алгоритм проверки слова на тривиальность. И несомненным плюсом является то, что согласно только что доказанной теореме группы, допускающие копредставление Дэна, это в точности гиперболические; но минус в том, что это условие крайне сложно проверить. Поэтому полезно рассматривать осмысленный и очень важный класс групп, допускающих *копредставление с условием малого сокращения*, минус которых в том, что они являются лишь частным случаем гиперболических групп (хотя и довольно обширным), но с безусловным плюсом, что проверка этого условия простая и прозрачная - и делается в два шага, в отличие от проверки условия Дэна, которое проверить практически невозможно: ведь нужно искать общие подслова с подсловами соотношений для *всех* тривиальных элементов, а их бесконечное число. И хотя их можно алгоритмически перечислить (достаточно рассматривать всевозможные произведения всевозможных сопряжений наших соотношений) - все равно вручную этого сделать нельзя.

Определение

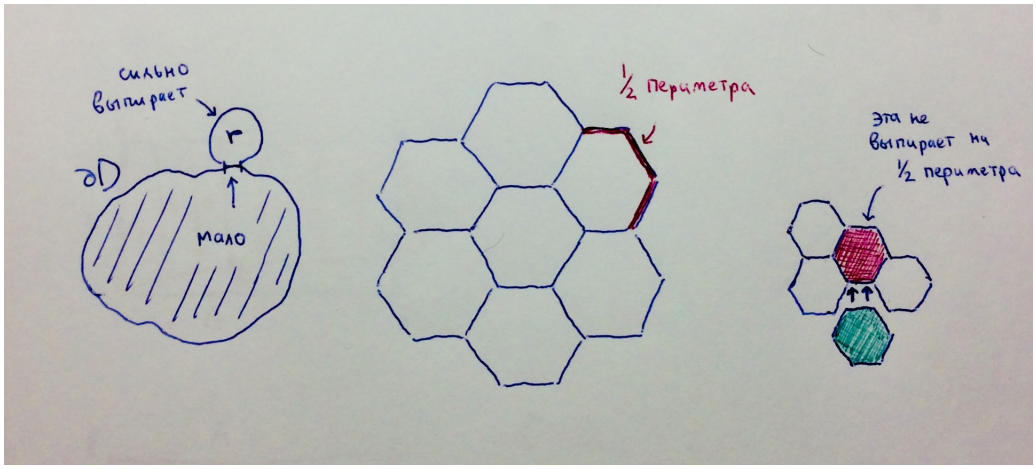
Симметричное конечное копредставление $G = \langle A|R\rangle$ называется копредставлением с условием малого сокращения $C'\left(\frac{1}{6}\right)$ (small cancellation property), если для любого общего подслова u слов r_1 и r_2, что $r_1, r_2 \in R$ и $r_1 \neq r_2$ (подслово и с такими условиями называется куском (piece)) выполнено $|u| < \frac{1}{6}|r_i|$ для обоих i.

Иными словами никакой общий фрагмент двух различных слов из R не может составлять больше $\frac{1}{6}$ части периметра каждой из этих двух клеток. Терминология пошла примерно из этих же соображений: что в таком случае клетки в диаграмме ван Кампена склеиваются менее чем по $\frac{1}{6}$ части периметра, т.е. сокращения при склеивании малые. Для краткости условие малого сокращения $C'\left(\frac{1}{6}\right)$ мы будем называть просто *условием* $C'\left(\frac{1}{6}\right)$.

Лемма (Гриндлингер)

Пусть $G = \langle A|R\rangle$ удовлетворяет условию $C'\left(\frac{1}{6}\right)$, тогда это копредставление удовлетворяет условию Дэна.

В частности из этой леммы получаем, что все группы с условием $C'\left(\frac{1}{6}\right)$ являются гиперболическими. Также рассматривают группы с условием $C'(\lambda)$ с $\lambda < 1$, где в определении последнее условие заменяется на $|u| < \lambda|r_i|$, при этом есть более общая версия леммы Гриндлингера, согласно которой если $\lambda \leq \frac{1}{6}$, то у групп с условием $C'(\lambda)$ граница диаграммы ван Кампена произвольного тривиального элемента содержит больше $(1 - 3\lambda)$ части некоторого соотношения; и $\lambda = \frac{1}{6}$ является пограничным случаем, когда мы можем гарантировать условие Дэна, т.е. больше половины соотношения. Если $\lambda > \frac{1}{6}$ - то лемма Гриндлингера не работает, и группа не обязана быть гиперболической, а если $\lambda < \frac{1}{6}$, то по свойствам такие группы не так чтобы сильно отличались от групп с $\lambda = \frac{1}{6}$, поэтому условие малого сокращения обычно рассматривают только в случае $C'\left(\frac{1}{6}\right)$. Лемму Гриндлингера доказывать мы не будем, но скажем, что интуитивно ее понять можно так: чем по более маленькому куску можно клетку приклеить к другой уже присутствующей в диаграмме ван Кампена клетке - тем более выпирающими будут клетки приклеиваемых соотношений, а значит будет больше возможностей на итоговой границе найти большую часть некоторого соотношения. То, что при $\lambda = \frac{1}{6}$ получается именно половина соотношения на границе, хорошо иллюстрирует пример склеивающихся правильных шестиугольников - склеиваются они в точности по $\frac{1}{6}$ своего периметра и всегда в такой картинке некоторая граничная клетка (не обязательно все) выпирает минимум на половину своего периметра. На самой правой картинке показано, как красная граничная клетка выпирает лишь на $\frac{1}{3}$ своего периметра, хотя и суммарно на границу выходит половина, но к этой половине ничего нельзя приклеить из-за несвязности выходящей на границу части периметра - поэтому это не то, чего мы хотим. Причем если подклеить снизу зеленую клетку, то и суммарно выпирать красная клетка будет уже лишь на $\frac{1}{3}$.



И повторюсь, что эта теория - способ задаром проверить гиперболичность, так как в отличие от условия Дэна для проверки условия $C'\left(\frac{1}{6}\right)$ нужно просто сделать конечный перебор в соотношениях на наличие общих подслов.

Пример

Доказать, что группа $G = \langle a, b, c, d | [a, b][c, d] = 1 \rangle$ является гиперболической.

Эта группа G является фундаментальной группой "бублика с двумя дырками". Докажем для этого копредставления свойство $C'\left(\frac{1}{6}\right)$, откуда сразу же вытечет гиперболичность группы G.

Кстати, прошу обратить ваше внимание, что правильный ответ на вопрос "сколько соотношений вы видите в этом копредставлении?" будет 16: потому что R во всей этой теории должно быть симметричным, а потому вместе с каждым соотношением r нужно добавить его обратный r^{-1} и все их циклические сдвиги, если таковых раньше не было в R. В результате эти операции наше одно соотношение длины 8 расплодят на 16 соотношений. Но при этом я говорил, что можно избежать необходимости включать циклические сдвиги, если соотношения рассматривать как *циклические слова*, которые можно читать по кругу начиная с любого места. Давайте воспользуемся этой концепцией - и таким образом у нас будет 2 циклических слова:

$$aba^{-1}b^{-1}cdc^{-1}d^{-1}$$

$$dcd^{-1}c^{-1}bab^{-1}a^{-1}$$

Заметим, что каждая буква (с учетом степени, то есть a и a^{-1} считаем разными буквами) встречается только 2 раза: один раз в верхнем слове и один раз в нижнем. Но простой перебор 8 вариантов говорит о том, что следующая за ней буква с учетом степени будет в верхнем и нижнем слове разной. На геометрическом языке это означает, что если мы склеим два циклических соотношения по одной букве, то уже по следующей букве склеить не получится, так как они будут различны. Таким образом такие соотношения склеиваются максимум по $\frac{1}{8}$ части периметра, а значит группа удовлетворяет свойству $C'\left(\frac{1}{6}\right)$.

Вдумайтесь, насколько свойство $C'\left(\frac{1}{6}\right)$ является мощным инструментом для проверки гиперболичности - так как если пытаться действовать в лоб через определение, то неясно даже как подступиться к графу Кэли этой группы, не говоря уже о проверке треугольников на тонкость/узкость.

Группы с условием $C'\left(\frac{1}{6}\right)$ являются важным подклассом гиперболических групп, но они все равно не дают всех гиперболических групп; и следующая теорема очень хорошо иллюстрирует происходящее в этом ключе:

Теорема (Ньюмана) *Пусть $G = \langle A | r^n = 1 \rangle$, где $r \in \mathbb{F}(A)$ - некоторое циклически-приведенное слово, A - конечно, $n \geq 2$. Тогда G является гиперболической и удовлетворяет условию $C'\left(\frac{1}{n}\right)$.*

Таким образом, если $n = 2$, то группа обладает лишь $C'\left(\frac{1}{2}\right)$ и не обязана обладать $C'\left(\frac{1}{6}\right)$, но при этом все равно является гиперболической, несмотря на то, что лемма Гриндлингера не работает. Грубо говоря, даже если клетки не склеиваются лишь по малым кусочкам - все равно может возникнуть ситуация, когда на границе некоторые клетки будут сильны выпирать, то есть выполняться условие Дэна. Также замечу, что при $n = 1$ такие группы G принято называть *группами с одним соотношением (one-relator groups)*, у них много замечательных свойств, и их гиперболичность является открытым вопросом: а именно Герстен сформулировал такую гипотезу, что $G = \langle A | r = 1 \rangle$ является гиперболической $\Leftrightarrow$ G не содержит подгрупп, изоморфных группам Баумслага-Солитера $B(n, m) = \langle a, b | b^{-1}a^n b = a^m \rangle$

(то есть гиперболическими являются все группы с одним соотношением кроме негиперболических по очевидным соображениям). Ранее мы с вами доказали, что $\mathbb{Z}^2 = \langle a, b | [a, b] = 1 \rangle$ не является гиперболической; но этот пример не является решением давнишнего открытого вопроса, т.к. $\mathbb{Z}^2 = B(1, 1)$ является группой Бауслага-Солитера. То, что группы, содержащие группу Баумслага-Солитера, не являются гиперболическими мы проверим позже.

Говоря о свойстве $C'\left(\frac{1}{6}\right)$ нельзя не упомянуть очень мощную и важную конструкцию Рипса: которая помогает и лучше понять природу гиперболических групп, иногда позволяет свести вопрос о произвольной конечно-определенной группы к гиперболическому случаю, а также является неиссякаемым источником самого разного рода контрпримеров в теории групп.

Теорема (И.А. Рипс)
Пусть Q - конечно-определенная группа. Тогда существует группа G с условием $C'\left(\frac{1}{6}\right)$ (в частности гиперболическая), некоторая 2-порожденная группа N, и следующая точная последовательность:

$$1 \to N \to G \to Q \to 1$$

Или что то же самое $Q \cong G/N$, иными словами любая конечно-определенная группа является фактором некоторой гиперболической группы. Копредставление G Рипс предъявил явно: пусть $Q = \langle s_1, \ldots, s_n | r_1 = 1, \ldots, r_m = 1 \rangle$, и пусть $\omega_i, u_i, v_i \in \mathbb{F}(a, b)$ некоторый набор слов с условием $C'(\lambda)$ для очень маленького λ, тогда непосредственно можно проверить, что правильно выбирая ω_i, u_i, v_i группа:

$$G = \langle s_1, \ldots, s_n, a, b | r_i \omega_i = 1, s_j^{-1} a s_j u_j = 1, s_j^{-1} b s_j v_j = 1, i \leq m, j \leq n \rangle$$

является группой с условием $C'\left(\frac{1}{6}\right)$, и тогда $N = \langle a, b \rangle \lhd G$, а эпиморфизм $G \to Q$ на порождающих строится как $s_i \mapsto s_i$, $a, b \mapsto 1$ (легко проверить, что так заданное отображение продолжается до гомоморфизма, то есть уважает соотношения). Основная идея построения - это перебросить бремя условий на общие подслова на плечи ω_i, u_j, v_j, в выборе которых мы имеем абсолютную свободу; и если они между собой мало пересекаются, и если их сделать достаточно длинными (для того, чтобы возможно плохая доля пересечений исходных соотношений r_i в новых соотношениях группы G давала малый вклад), то можно добиться, чтобы и соотношения построенной G тоже мало пересекались. Отмечу, что условие $C'\left(\frac{1}{6}\right)$ в формулировке теоремы не принципиально и может быть заменено на любое $C'(\lambda)$ с $\lambda \leq \frac{1}{6}$; но этим обобщением редко пользуются, так как обычно от этой конструкции мы хотим главным образом гиперболичность группы G, даже условие $C'\left(\frac{1}{6}\right)$ уходит на второй план. Проиллюстрируем мощь и красоту этой теоремы на двух сюжетах:

Первый сюжет:

Хотя в гиперболических группах алгоритмически разрешимы многие проблемы (например, проблемы равенства слов, сопряженности, что мы обсудим чуть позже; и даже изоморфности), но все равно в этом направлении гиперболические группы не совсем идеальны - и мы сейчас построим пример группы, где будет не разрешима *проблема вхождения*, которая формулируется так: пусть $G = \langle A|R\rangle$, $N = \langle g_1, \ldots, g_n\rangle$, $g_i \in \mathbb{F}(A)$, и требуется построить алгоритм, проверяющий $\omega \in N$, где $\omega \in \mathbb{F}(A)$ (в такой постановке можно работать только с конечнопорожденной N, так как в противном случае вы за конечное число шагов не сможете даже входные данные загрузить в машину Тьюринга: это так называемая равномерная задача вхождения. В неравномерном же случае на вход подается только ω, а N уже изначально уже считается известной компьютеру, и в таком случае N может быть и бесконечно-порожденной. Однако замечу, что все равно вся эта теория лучше и легче всего работает, когда все конечно, так как алфавит машины Тьюринга конечный и работу она должна завершить за конечное число шагов, а потому в бесконечно-порожденных случаях как минимум нужно задать себе вопрос, сможете ли вы начальные данные прогрузить за конечное число шагов). Для построения заявленного примера для начала стартуем с некоторой конечно-определенной группы Q, в которой неразрешима проблема слов. Даже простейшие примеры очень сложные, но мы постараемся на пальцах объяснить, откуда такие примеры могут взяться: в математической логике есть два класса подмножеств $\mathbb{N}$ - это *разрешимые (они же recursive = computable)* и *перечислимые (recursively enumerable = computably enumerable)*. Разрешимыми называются такие множества, принадлежность которому произвольного элемента является алгоритмически разрешимой, иными словами вы сможете написать программу, проверяющую, лежит ли данный элемент в этом множестве, причем программа должна выдать результат за конечное число шагов. Перечислимыми называют множества, все элементы которого можно выписать определенным алгоритмом. Свет на связь между этими понятиями проливает почти очевидна теорема Поста: что множество M разрешимо $\Leftrightarrow$ оба M и $\mathbb{N}\backslash M$ являются перечислимыми: $\Leftarrow$ мы можем запустить параллельно два алгоритма перечисления M и $\mathbb{N}\backslash M$, и для определения принадлежности элемента M нужно просто дождаться когда один из перечисляемых алгоритмов выдаст этот элемент. $\Rightarrow$ для перечисления скажем M просто перебираем все элементы $\mathbb{N}$ и для каждого n запускаем алгоритм для проверки $n \in M$, и в зависимости от результата решаем, стоит ли его перечислять. В частности если множество разрешимо - то оно и перечислимо. Но есть хитрые примеры перечислимых, но неразрешимых множеств. При этом есть примеры и неперечислимых множеств: понять это очень просто: потому что всего подмножеств $\mathbb{N}$ континуум, при этом программ на компьютере вы сможете написать лишь счетное число, а потому и множество перечисляемых алгоритмов (а значит и самих перечислимых множеств) только счетно. Возвращаясь к группам - верна фундаментальная классическая теорема:

Теорема (Хигман)
Пусть $G = \langle a_1 \ldots, a_n | r_1, r_2 \ldots \rangle$ - конечно-порожденная группа. Тогда существует конечно-определенная H, что $G \hookrightarrow H \Leftrightarrow$ группа G является перечислимо-определенной (recursively presented group).

Перечислимая определенность означает, что если все слова в $\mathbb{F}(A)$ алгоритмически пронумеровать и воспринимать как элементы $\mathbb{N}$, то множество соотношений $\{r_1, r_2, \ldots\}$ является перечислимым множеством, или говоря более простым языком: можно записать алгоритм, который выпишет вам все определяющие соотношения. Иными словами конечно-порожденную группу G можно вложить в конечно-определенную при условии, что в группе G множество определяющих соотношений хорошее. Замечу, что как и перечислимых множеств, таких групп только счетное число, так как всего существует счетное число алгоритмов. Из формулировки понятно, что доказательство теоремы сложное и погружается глубоко в дебри логики. На самом деле включая эту существует три классические теоремы о вложениях групп, поэтому не хочу их разлучать и сразу здесь оставшиеся две сформулирую:

Теорема (Кэли)
Пусть G - счетная группа. Тогда $G \hookrightarrow S(\mathbb{N})$.

Раньше мы с Вами обсуждали эту теорему: действие левым умножением группы на себе $G \curvearrowright G$ индуцирует вложение $G \hookrightarrow S(G) \cong S(\mathbb{N})$. Иными словами $S(\mathbb{N})$ является универсальной группой, содержащей все счетные группы. Небольшое неудобство заключается в том, что сама $S(\mathbb{N})$ не является счетной, но в математике типично, что универсальный объект имеет мощность больше чем у объектов, для которых он является универсальным.

Теорема
Пусть G - счетная. Тогда G вкладывается в некоторую 2-порожденную.

И если резюмировать все три теоремы, то получаем, что существует универсальная группа, содержащая все счетные группы (и это $S(\mathbb{N})$), а также, что любая счетная группа вкладывается в конечно-порожденную (и даже 2-порожденную), и каждая конечно-порожденная вкладывается в конечно-определенную если множество определяющих соотношений алгоритмически хорошее. То, что количество порождающих элементов у большей группы может быть меньше, очень хорошо иллюстрируется примером $\mathbb{F}_\infty \hookrightarrow \mathbb{F}_2$, причем в теории групп в естественных примерах это скорее типичная ситуация, нежели аномалия.

У этой теоремы существует два классических доказательства: в первом доказательстве явно предъявляется такое вложение: рассмотрим вложение по теореме Кэли $G \hookrightarrow S(\mathbb{N})$, также занумеруем нашу счетную группу нечетными числами $G = \{g_1, g_3, g_5, \ldots\}$ и рассмотрим две перестановки $a, b \in S(\mathbb{Z} \times \mathbb{Z} \times \mathbb{N})$:

$$a(m,n,p) = (m+1,n,p)$$

$$b(m,n,p) = \begin{cases} (m,n+1,p),\ m=0 \\ (m,n,g_m(p)),\quad m\text{-нечетное}, m>0, n\geq 0 \\ (m,n,p),\qquad \text{иначе} \end{cases}$$

Советую проверить, что b является перестановкой (для a это очевидно). И дальше приводится явная, но довольно хитрая формула вложения:

$$G \hookrightarrow \langle a,b\rangle < S(\mathbb{Z}\times\mathbb{Z}\times\mathbb{N})$$

Плюс этого доказательства в том, что строится явное вложение, хотя оно довольно сложное, и в конкретной формуле нет особой необходимости, так как она не помогает лучше понять природу G (хотя мы довольно хорошо знаем структуру $S(\mathbb{N})$, но при этом в теории счетных групп масса открытых вопросов, несмотря на то, что все такие группы вкладываются в $S(\mathbb{N})$ - так что такое вложение не может ответить на все вопросы), и на практике важен бывает обычно только факт вложения без конкретики. И хотя идея возможности моделировать соотношения в G внутри $S(\mathbb{N})$ с помощью добавления двух прямых $\mathbb{Z}$-сомножителей - очень красивая, остается осадочек из-за того, что общая структура доказательства словно ускользает: то есть неясно "А почему у нас получилось? А что будет в чуть другой ситуации"?

Второе доказательство (исторически появившееся раньше первого) - основывается на понятии HNN-расширения, которое впервые были использовано как раз для этой теоремы и получило свое название по первым буквам фамилий своих создателей: Хигман, Б. Нейман, Х.Нейман (последние два - это муж и жена, их дети, кстати, тоже сделали весомый вклад в теорию групп). Напомним, что если $A,B < G$ две изоморфные подгруппы G и $\varphi : A \to B$ - изоморфизм, то *HNN-расширением* называется группа:

$$HNN_\varphi(G) = \langle G,t |\ t^{-1}at = \varphi(a)\ \ \text{для любого } a\in A\rangle$$

где подразумевается, что к выписанным соотношениям также нужно добавить все исходные соотношения на элементы группы G: грубо говоря, если $G = \langle g_1,\dots,g_n | r_1,\dots r_m\rangle$, то $HNN_\varphi(G) = \langle g_1,\dots,g_n,t | r_1,\dots,r_m, t^{-1}at = \varphi(a)\rangle$. Обычно HNN-расширение обозначают $G*_\varphi$, но мне не нравится это обозначение, так как складывается такое впечатление, что G умножается на пустоту. В важном частном случае если $A=B=G$, то $HNN_\varphi(G) = G\rtimes\mathbb{Z}$ обыкновенное полупрямое произведение. Итак, пусть нам дана счетная группа $G = \{g_1,g_2,\dots\}$. Пусть $\mathbb{F}_2 = \langle a,b\rangle$ - свободная группа, а также рассмотрим две подгруппы $A,B < G * \mathbb{F}_2$, заданные как:

$$A = \langle a,\ b^{-1}ab,\ b^{-2}ab^2,\dots\rangle$$

$$B = \langle b,\ g_1a^{-1}ba,\ g_2a^{-2}ba^2,\dots\rangle$$

Можно проверить, что $A\cong B\cong \mathbb{F}_\infty = \langle x_1,x_2\dots\rangle$, причем продолженные до гомоморфизма заданные на порождающих отображения $x_i\mapsto b^{-i}ab^i$ и $x_i\mapsto g_ia^{-i}ba^i$ для первой и второй подгруппы соответственно являются изоморфизмами, а потому изоморфизм $\varphi : A\to B$ на порождающих можно задать формулой $\varphi(b^{-i}ab^i) = g_ia^{-i}ba^i$, и используя теоретический факт, что для любой группы K

тождественное отображение $K \to HNN(K)$ является инъективным (что очевидно вытекает из леммы Бриттона, ее мы сформулируем позже), получаем:

$$G < G*\mathbb{F}_2 < HNN_\varphi(G*\mathbb{F}_2) = \langle G, a, b, t | t^{-1}(b^{-i}ab^i)t = g_i a^{-i}ba^i \text{для любого } i\rangle = \langle a, t | \ldots\rangle$$

причем эта сложная группа справа порождается двумя элементами a и t: потому что из соотношений $t^{-1}(b^{-i}ab^i)t = g_i a^{-i}ba^i$ можно все элементы g_i группы G выразить через a, b и t, а при $i = 0$ (действие φ на первых порождающих A и B) мы получаем соотношение $t^{-1}at = b$, т.е. b выражается через a и t. Замечу, что это типичная ситуация, когда у группы сильно уменьшается количество порождающих при полупрямом умножении на другую группу (или в более общей ситуации HNN-расширений) - и это мы раньше видели на примере, когда после полупрямого умножения бесконечно-порожденной группы $\bigoplus \mathbb{Z}_2$ на $\mathbb{Z}$ мы получили 2-порожденную лампочную группу $\mathbb{Z}_2 \wr \mathbb{Z}$. Это происходит из-за того, что при полупрямом произведении добавляется много новых соотношений, из которых зачастую можно выразить многие порождающие исходной группы.

Итак вернемся к гиперболическим группам. Для построения примера гиперболической группы, в которой неразрешима проблема вхождения, рассмотрим произвольную конечно-определенную группу Q, в которой неразрешима проблема равенства слов. Простейший пример, как мы уже обсуждали очень сложный, но я примерно объясню как можно строить такие примеры. Рассмотрим группу

$$H_I = \langle t, x | \ [x, t^{-i}xt^i] = 1 \ \text{ для любого } i \in I\rangle$$

где I - произвольное перечислимое но неразрешимое множество. Для H_I неразрешима проблема слов, так как по определению неразрешимости мы даже не сможем выяснить, содержится ли заданное слово среди определяющих соотношений $\{[x, t^{-i}xt^i] = 1\}$. Группа эта не является конечно-определенной, но так как I - перечислимое, то по теореме Хигмана мы можем вложить $H_I \hookrightarrow Q_I$ в некоторую конечно-определенную группу Q_I, в которой тоже не будет разрешима проблема слов: доказывать этого мы не будем, но интуитивно в это легко верится. И теперь для группы Q_I применим конструкцию Рипса:

$$1 \to N \to G \xrightarrow{\pi} Q_I \to 1$$

где N - 2-порожденная, а G - гиперболическая. Из определения точной последовательности вытекает:

$$g \in N \quad \Longleftrightarrow \quad \pi(g) = 1$$

Таким образом, если нельзя написать алгоритм для определения $\pi(g) = 1$, то и нельзя написать алгоритм для определения $g \in N$.

Замечание:

Хотя самый внимательный читатель должен был заметить, что доказательство еще не является полным, так как остался еще маленький алгоритмический штрих: потому что по предположению в группе Q_I неразрешима "проблем слов", а не "слов, представленных в виде $\pi(g)$ для некоторого g". Конечно же, π является эпиморфизмом, и слова вида $\pi(g)$ пробегают все слова, но в данной теории мы видели важно не только множество, но и его в некотором смысле порядок: все счетные множества биективны $\mathbb{N}$, но при этом среди них есть как разрешимые, так и неразрешимые: и по большому счету важна алгоритмическая структура π. Чтобы лучше передать то, что я хочу рассказать - приведу пример, пусть и не очень хороший, потому что он бесконечно-порожденный: пусть I - неразрешимое множество, рассмотрим произвольную биекцию φ этого множества и множества четных чисел и продолжим ее до биекции на всем $\mathbb{N}$ (дополнения до упомянутых множеств тоже счетны). Теперь рассмотрим две группы (изоморфные $\mathbb{F}_\infty$):

$$G = \langle x_i | x_i = 1 \quad для\ i \in I \rangle$$

$$H = \langle y_i | y_{2i} = 1 \rangle$$

и рассмотрим изоморфизм, заданный на порождающих формулой $\pi(x_i) = y_{\varphi(i)}$. Тогда ясно, что так как π - изоморфизм, то для любого $g \in G$ выполнено:

$$g = 1 \quad \Longleftrightarrow \quad \pi(g) = 1$$

но при этом в H разрешима проблема равенства слов, а в G нет.

В нашем же случае можно поступить двумя путями: либо заметить, что в конструкции Рипса π был не абстрактным, а простым и конкретным эпиморфизмом: а именно для $Q_I = \langle g_1, \ldots, g_n | r_1, \ldots, r_m \rangle$ мы строили $G = \langle g_1, \ldots, g_n, a, b | \ldots \rangle$, а наш эпиморфизм задавался на порождающих простой формулой $\pi(g_i) = g_i$, иными словами в алфавите $\{g_1, \ldots, g_n\}$ эпиморфизм π просто тождественный и слова из Q_I мы можем трактовать как слова из G. С учетом этого замечания можно сформулировать следующую эквивалентность: что для любого слова $g \in \mathbb{F}(\{g_1, \ldots, g_n\})$ верно:

$$g \in N \quad \Longleftrightarrow \quad g =_{Q_I} 1$$

И тогда если для слов в Q_I не будет разрешима проблема равенства, то для этих же слов не будет разрешима проблема вхождения в N. Это замечание о возможности слова из Q рассматривать и как слова в G в контексте конструкции Рипса сильно помогает в самых разных задачах так как дает явную формулу для прообразов. Причем отмечу, что делать это можно только для слов, а не групповых элементов; потому что такая "операция" не уважает группового умножения, так как в определяющих соотношениях группы G перемешаны как g_i, так и a и b.

Второй подход более универсальный: просто показать, что в конечно-порожденном случае от выбора эпиморфизма π ничего не зависит, и описанная выше аномалии с $\mathbb{F}_\infty$ возникнуть просто не может. А именно: рассмотрим алгоритм, который по порождающим в Q выдает их некоторые прообразы в G: и тут нужно сказать, что алгоритмическая разрешимость в математической

логике - означает, что существует программа, которая выдаст вам правильный результат, и от нее совсем не требуется какой-то осмысленной работы. К примеру, вычисление сотого знака после запятой в числе Пифагора π является алгоритмически разрешимой задачей, потому что если написать 10 программ, каждая из которых выдает соответствующую цифру - то одна из них будет искомой, но неясно какая. И программа просто выдаст ответ, и не будет разбираться в структуре числа π. На языке математической логики это формулируется как то, что любое конечное множество разрешимо, и осмысленными являются задачи, где вам нужно выдавать результат с бесконечным множеством вариантов входных данных: в противном случае если входных данных конечное число - можно рассмотреть все программы, которые по всем комбинациям входных данных выдают всевозможные комбинации ответов - и среди них обязательно будет нужная нам. Таким образом, несмотря на то, что ни мы, ни программа не предъявляем явную формулу для прообраза порождающих - все равно такой алгоритм существует. Если есть алгоритм, который находит прообразы порождающих - то этот же алгоритм может найти прообраз любого слова (действуя побуквенно). Из этих рассуждений также вытекает, что все алгоритмические вопросы не зависят от копредставления группы (в конечно-порожденном случае); и эти рассуждения обеспечивают, что такой переход между копредставлениями не нарушает алгоритмической природы.

И тогда можно рассуждать так: пусть в N разрешима проблема вхождения, иными словами, есть алгоритм, который получает g - и говорит, верно ли, что $g \in N$, но в силу эквивалентности, это означает, что он говорит, верно ли, что $\pi(g) = 1$. Теперь по слову $\omega \in Q_I$ мы алгоритмически находим такое g, что $\pi(g) = \omega$, и для полученного этим алгоритмом g - запускаем алгоритм на проверку $\pi(g) = 1$; и такой алгоритм проверит $\omega = 1$. Таким образом приходим к противоречию с тем, что в Q_I неразрешима проблема равенства слов.

Второй сюжет:

Внимательный читатель, должно быть, обратил внимание, что мы до сих пор старательно обходили стороной очень важный вопрос о сохранении гиперболичности при переходе к подгруппе. Уже при рассмотрении простейших примеров станет понятно, что гомоморфизмы не уважают геодезические, и все условия рушатся: и проблемы начинаются с ситуации, когда при элементарном вложении $\mathbb{Z} \hookrightarrow G$, где порождающий 1 группы $\mathbb{Z}$ переходит в некоторый элемент $g \in G$ - при попытке построить даже индуцированное отображение $C_{\{1\}}(\mathbb{Z}) \to C_A(G)$ мы натыкаемся на трудности, так как неясно каким образом геодезический отрезок $[0, 1]$ отобразить в $C_A(G)$, и если отобразить его в $[e, g]$, то неясно в какую именно, так как может существовать несколько соединяющих заданные точки геодезических; и заканчивая тем, что для $H < G$ геодезическая в H не обязана быть геодезической в G (так как геодезические в H строятся посредством разложения $u = h_1 h_2 \dots h_n$ с минимальным числом сомножителей, и если в качестве сомножителей допустить элементы группы G, то может хватить и меньшего числа сомножителей). Но на самом деле вопрос этот очень сложный, и технически мы только сейчас стали готовы лишь приступить к его обсуждению.

В самой примитивной постановке, *верно ли, что если $H < G$ и G - гиперболическая, то и H гиперболическая* ответ, разумеется, отрицательный: и можно рассмотреть пример

$$\mathbb{F}_\infty \cong \langle \{b^{-i}ab^i\}_{i\in\mathbb{N}} \rangle < \mathbb{F}_2 = \langle a, b \rangle$$

где $\mathbb{F}_2$ - гиперболическая, так как ее граф Кэли это дерево, а $\mathbb{F}_\infty$ не является гиперболической, так как она не является конечно-порожденной. Вообще, пытаться построить в некотором роде теорию гиперболических групп для бесконечно-порожденного случая является бессмысленным занятием: так как для произвольной счетной группы G мы всегда в качестве порождающих можем взять множество всех ее элементов, а значит диаметр графа Кэли $C_G(G)$ будет равен 1 (в нетривиальном случае, и 0 если G тривиальна) - а ограниченное пространство является гиперболическим в любом разумном смысле.

Вопрос можно поставить и чуть более осмысленно: *верно ли, что если $H < G$, причем H - конечно-порожденная, а G - гиперболическая - тогда и H гиперболическая* - ответ снова отрицательный, и для построения контрпримера нужно вспомнить, что гиперболическая группа является конечно-определенной, а потому достаточно просто предъявить не являющуюся конечно-определенной конечно-порожденную подгруппу гиперболической группы. Но для начала давайте просто построим пример конечно-порожденной и не конечно-определенной группы, а лишь потом будем пытаться как-то его адаптировать и засунуть в некоторую гиперболическую группу.

Вспомогательная лемма

Лампочная группа $\mathbb{Z}_2 \wr \mathbb{Z}$ является конечно-порожденной, и не является конечно-определенной группой.

Напомним, что

$$G = \mathbb{Z}_2 \wr \mathbb{Z} = \left(\bigoplus \mathbb{Z}_2\right) \rtimes \mathbb{Z} = \langle a, b | a^2 = 1, [a, b^{-j}ab^j] = 1 \text{ для всех } j \in \mathbb{Z} \rangle$$

Пусть $G = \langle g_1, \dots, g_n | r_1, \dots r_m \rangle$, а также рассмотрим свободную группу $\mathbb{F}_2 = \langle a, b \rangle$. Так как любое соотношение (в частности r_i) есть произведение сопряжений определяющих соотношений $R = \{a^2\} \cup \{[a, b^{-j}ab^j]\}_j$, то существует такое N, что

$$r_i \in \langle\langle R_N \rangle\rangle$$

для любого i, где $R_N = \{a^2\} \cup \{[a, b^{-j}ab^j]\}_{|j|<N}$, элементы g_i некоторым образом представлены в алфавите $\{a, b\}$, а нормальное замыкание здесь и далее рассматривается, разумеется, в $\mathbb{F}_2$. При этом если наше конечное копредставление рассматривать как "базовое", тогда опять любое соотношение можно представить как произведение сопряжений определяющих соотношений; и в частности $[a, b^{-N}ab^N] \in \langle\langle r_1, \dots, r_m \rangle\rangle \lhd \langle\langle R_N \rangle\rangle$. И чтобы теперь прийти к противоречию: рассмотрим гомоморфизм:

$$\pi : \mathbb{F}_2 = \langle a, b \rangle \to S_{2N+1}$$

$$a \mapsto (1, 2)$$

$$b \mapsto (1, 2, \dots, 2N + 1)^{-2}$$

Простой непосредственной проверкой (вспомнив формулу для сопряжение перестановок) можно показать, что:

$$b^{-j}ab^j \mapsto (1+2j, 2+2j) \mod 2N+1$$

Таким образом:

$$[a, b^{-j}ab^j] \mapsto 1$$

при $|j| < N$, и при этом перестановка $b^{-N}ab^N \mapsto (1+2N, 1)$ имеет носитель, пересекающийся с $(1,2)$, а потому $[(1,2),(1+2N,1)] \neq 1$, таким образом $\pi(R_N) = 1$, но при этом $\pi([a, b^{-N}ab^N]) \neq 1$, а значит $[a, b^{-N}ab^N] \notin R_N$, что является противоречием.

Если кратко резюмировать ход доказательства, то произошло следующее: в предположении конечной определенности лампочной группы мы получили, что в таком случае хватило бы конечного числа исходных определяющих соотношений, и через них выражались бы остальные определяющие соотношения, и в частности мы бы получили, что $[a, b^{-N}ab^N] \in \langle\langle a^2 \cup \{[a, b^{-j}ab^j]\}_{|j|<N}\rangle\rangle$ для некоторого N, но это невозможно, так как мы построили гомоморфизм $\mathbb{F}_2 \to S_{2N+1}$, такой что он переводит в единицу всё R_N, но при этом переводит не в единицу элемент $[a, b^{-N}ab^N]$, который из-за этого не может лежать в $\langle\langle R_N\rangle\rangle$.

Имея в арсенале лампочную группу - мы готовы теперь построить полноценный контрпример: рассмотрим эту самую не являющуюся конечно-определенной конечно-порожденную лампочную группу, которую по теореме Хигамана можно вложить $\mathbb{Z}_2 \wr \mathbb{Z} \hookrightarrow Q$ в некоторую конечно-определенную группу $Q = \langle g_1, \dots g_n | r_1, \dots, r_m\rangle$: потому что определяющие соотношения лампочной группы $[a, b^{-i}ab^i]$ и a^2 выписываются алгоритмическим образом. Кстати, участвующее в формулировке теоремы Хигмана понятие перечислимой определенности можно интуитивно трактовать как возможность явно записать на бумаге описание всех определяющих соотношений на понятном для всех языке: грубо говоря через троеточие, и чтобы все поняли закономерность. Теперь применим для группы Q конструкцию Рипса:

$$1 \to N \to G \xrightarrow{\pi} Q \to 1$$

где $N = \langle x, y | \dots\rangle$. Тогда

$$H = \pi^{-1}(\mathbb{Z}_2 \wr \mathbb{Z})$$

Пусть порождающие a, b группы $\mathbb{Z}_2 \wr \mathbb{Z}$ представляются словами A, B в группе Q в алфавите $\{g_1, \dots, g_n\}$. Тогда H порождается A, B, x, y с учетом замечания, что слова в Q можно рассматривать и как слова из G. Таким образом H конечно-порожденная. Но она не может быть конечно-определенной, так как добавив два соотношения $x = 1$ и $y = 1$ мы бы не нарушили конечную определенность, но с другой стороны мы бы получили копредставление для лампочной группы $\mathbb{Z}_2 \wr \mathbb{Z}$, хотя мы уже доказали, что она не является конечно-определенной. Но у H есть существенный upgrade по сравнению с лампочной группой $\mathbb{Z}_2 \wr \mathbb{Z}$, заключающийся в том, что $H < G$ является подгруппой некоторой гиперболической группы G, но при этом сама не является гиперболической из-за того, что не является конечно-определенной. Мы закончили построение контрпримера. И за счет того, что основывался этот контрпример на нарушении одного из основных свойств гиперболических групп, естественно задать следующий вопрос: *верно ли, что если $H < G$, группа G гиперболическая, а H*

является конечно-определенной, то H - является гиперболической - и оказывается здесь тоже ответ отрицательный, но контрпример для этого случая совсем сложный.

Однако есть и хорошие новости: предыдущие контрпримеры показали, что в гиперболической теории подход к изучению подгрупп на основании свойств их копредставлений в некотором смысле являются тупиковым, и правильнее смотреть на это с более геометрической точки зрения и рассматривать так называемые *квазивыпуклые подгруппы*, теории которых мы коснемся позже, и при переходе к которым гиперболичность уже сохраняется, а именно: если G - гиперболическая, $H < G$ и H - квазивыпуклая, то H тоже гиперболическая. В этом ключе есть еще некоторые результаты, которых мы тоже позже коснемся, например, если $\mathbb{Z}^2 < G$, то G не является гиперболической: это очень удобный способ проверки на гиперболичность. Причем отмечу, что это очень нетривиальный результат, требующий сложной теории, даже несмотря на то, что группа $\mathbb{Z}^2$ является в некотором роде эталоном негиперболичности: но опять-таки главная проблема в том, что свойство гиперболичности очень плохо себя ведет при переходе к подгруппам.

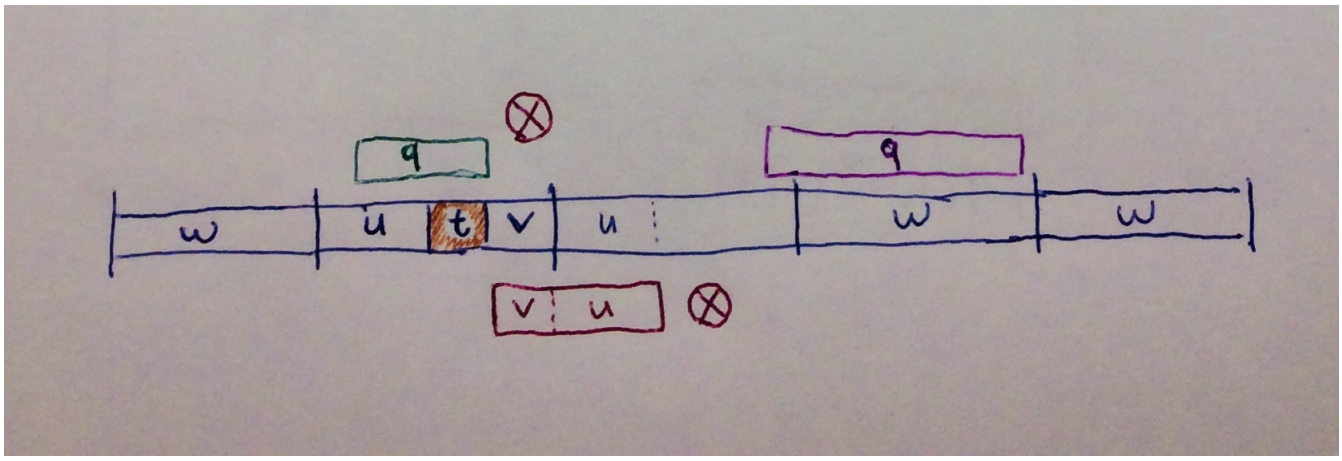
==========

Ключ к решению многих задач в теории гиперболических групп часто сводится к следующему: выписанные геометрические оценки можно трактовать как ограничение на длину элемента группы в словесной метрике: и из-за того, что в гиперболических пространствах очень часто можно встретить равномерные оценки, никак не зависящие от габаритов нашего геометрического объекта (мы помним, что радиус вписанной окружности для всех треугольников ограничен одним числом, к примеру) - то часто это выливается в то, что выбранный элемент можно представить произведением порождающих с равномерно ограниченным числом сомножителей, из чего вытекает, что множество элементов такого типа конечно. Полезно помнить про этот хитрый прием при решении задач на гиперболические группы. Проиллюстрируем этот метод на двух задачах:

Утверждение

Пусть G - гиперболическая группа. Доказать, что для любого n в ней существует лишь конечное число классов сопряженности элементов порядка n.

Иными словами, если в гиперболической группе есть много элементов порядка n, то многие из них сопряжены друг другу. Рассмотрим произвольное копредставление Дэна $G = \langle A|R\rangle$, и рассмотрим элемент $g \in G$, что $g^n = 1$ и n - его порядок (то есть минимальная такая степень). Также рассмотрим слово $\omega = x^{-1}gx$ минимальной длины как по всевозможным x, так и по всевозможным представлениям в виде слова в алфавите A; иными словами самое короткое слово в классе сопряженности g. Ясно, что минимальность длины в частности обеспечивает, что ω - циклически-приведенное. Из условия Дэна мы получаем, что циклическое слово ω^n содержит больше половины некоторого соотношения $r \in R$. В силу симметричности R мы можем считать, что $r = qs$ и q - подслово ω^n, причем $|q| > |s|$. Тогда возможны только три следующие ситуации вхождения q в ω^n:



Зеленая ситуация, когда q является частью ω, невозможна: так как в таком случае можно было бы, воспользовавшись соотношением $q = s^{-1}$, укоротить слово ω, что противоречит условию минимальности длины при выборе ω. Второй фиолетовый случай, когда q не содержится целиком в ω: длина q удовлетворяет оценке $|\omega| \leq |q| < \frac{|r|}{2}$ (то есть q длинная). И в оставшейся третьей красной ситуации, когда q не содержится целиком в некоторой ω (а значит цепляет границу стыка двух ω в циклическом слове ω^n) и при этом $|q| < |\omega|$ (то есть короткая), мы можем считать, что $q = vu$ и $\omega = utv$ (прослойка t как раз возникает из условия $|q| < |\omega|$, без этого условия могло случиться, что u "наложилось" бы на v); но в таком случае слово:

$$\tilde{\omega} = qt = vut$$

с одной стороны тоже лежит в классе сопряженности g, так как $\tilde{\omega}$ есть просто циклический сдвиг слова ω (в этом можно убедиться алгебраически: $vut = v(utv)v^{-1} = v\omega v^{-1}$), но с другой стороны $|\tilde{\omega}| = |\omega|$, и опять заменяя q на s^{-1} можно уменьшить его длину, не меняя при этом представляемый им элемент группы. Иными словами, единственная возможная непротиворечащая минимальности длины ω ситуация - фиолетовая, но в таком случае:

$$|\omega| < \frac{1}{2} \max_{r \in R} |r|$$

Иными словами каждый класс сопряженности элемента порядка n имеет своего представителя в шаре радиуса $\frac{1}{2} \max\limits_{r \in R} |r|$, но так как в конечно-порожденных группах в таких шарах лишь конечное число элементов - то и таких классов тоже лишь конечное число.

Замечания:

Отмечу, что кроме конечности числа таких классов мы также получили и довольно неплохую оценку на их число: и в теории гиперболических групп оценки через комбинаторные характеристики множества R встречаются очень часто. Также отмечу, что мы ничего не говорим о самих классах сопряженности; и они вполне могут быть бесконечными, как хорошо видно на примере группы

$$G = \mathbb{Z}_2 * \mathbb{Z} = \langle a, b | a^2 = 1 \rangle$$

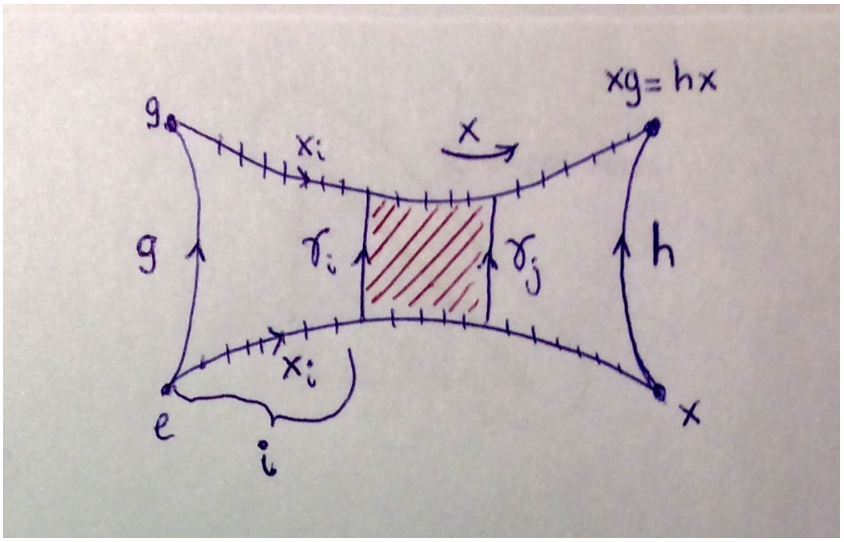
где $b^{-n}ab^n$ являются попарно различными элементами из класса сопряженности $[a]$. Также отмечу, что при $\max\limits_{r \in R} |r| = 1$ наша оценка даст

$|\omega| = 0$, но в этом нет никаких противоречий: так как в таком случае все соотношения имеют вид $x = 1$ для некоторых букв x, и в таком случае можно просто забыть про эти x, так как они представляют тривиальный элемент, а на оставшиеся буквы не будет никаких соотношений - иными словами группа будет свободная, а там нет нетривиальных элементов конечного порядка.

Утверждение

Пусть G является δ-гиперболической группой для некоторого копредставления (где δ - константа узкости), пусть $g, h \in G$ сопряжены. Тогда существует $x \in G$, такой что $xgx^{-1} = h$ и $|x| \leq K(|g|, |h|)$, где $K(|g|, |h|)$ - число элементов в шаре радиуса $2\delta + 3(|g| + |h|)$.

Иными словами мы можем жестко контролировать длину сопрягающего элемента. Пусть $G = \langle A|R\rangle$ - копредставление Дэна, представим g, h словами минимальной длины (которые будем для удобства обозначать теми же буквами g и h), и рассмотрим сопрягающий их x минимальной длины (то есть для него выполнено $xgx^{-1} = h$): мы докажем, что этот x будет искомым. Напомним, что для слов минимальной длины функции $|\cdot|_G$ и $|\cdot|$ совпадают. Пусть $x = y_n \dots y_2 y_1$, и рассмотрим также его суффиксы и префиксы $x_i = y_i \dots y_2 y_1$, $\bar{x}_i = y_n \dots y_{i+1}$. Рассмотрим гиперболический четырехугольник $[e, g, xg, x]$ в $C_A(G)$; мы можем считать, что верхняя и нижняя идущие вдоль x геодезические также идут вдоль всех суффиксов x_i, так как мы выбирали x минимальной длины (мы говорим, что геодезическая *идет вдоль* g, если геодезическая имеет вид $[a, b]$ и $ga = b$). Также из условия сопряженности $hx = xg$ вытекает, что правая сторона идет вдоль h; то, что g и h выбирались минимальной длины, означает, что длины левой и правой сторон равны $|g|$ и $|h|$ соответственно. Пусть $\gamma_i = x_i g x_i^{-1}$ групповые элементы, вдоль которых идут вертикальные сечения, параллельные боковым сторонам, в том смысле, что они соединяют точки, находящиеся на одинаковом расстоянии от соответствующих вершин. Изобразим все описанные выше на картинке:



Замечу, что точки соответствуют элементам группы, а "векторы" здесь просто означают на какой элемент группы нужно умножить, чтобы из одной точки попасть в другую. Из этого замечания получается, что "сумме векторов" в данном случае

соответствует произведение элементов группы, причем элемент, соответствующий новой стрелочке, нужно умножать *слева* (так как этого требует структура графа Кэли: ребром g соединяются точки вида a и ga); и что если по разным путям мы приходим в одну и ту же точку - то соответствующие произведения должны совпадать.

Факт номер 1

Все γ_i являются попарно различными. Действительно, если $\gamma_i = \gamma_j$ при $i < j$, тогда на рисунке можно "выбросить" красную часть, и склеить левый кусок с правым по совпадающим $\gamma_i = \gamma_j$, и новый $\tilde{x}$, который получится вдоль горизонтальных сторон - по прежнему будет сопрягающим элементом; но короче исходного x, что является противоречием с выбором x. Чуть более формально: проходя двумя разными способами по стрелочкам в образовавшихся слева и справа четырехугольниках мы получаем, что

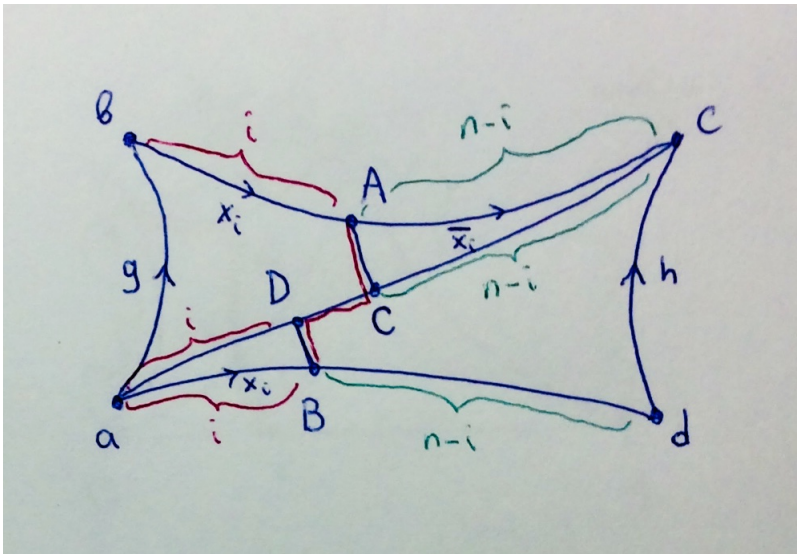
$$x_i g x_i^{-1} = \gamma_i = \gamma_j = \bar{x}_j^{-1} h \bar{x}_j$$

$$\bar{x}_j x_i g = h \bar{x}_j x_i$$

Таким образом получаем, что $\tilde{x} = \bar{x}_j x_i = y_n \dots y_{j+1} y_i \dots y_2 y_1$ годится в роли сопрягающего, а он короче x.

Факт номер 2

Можно записать оценку на $|\gamma_i|$ - вытекает это уже из особенностей гиперболической геометрии: прием, которым мы сейчас воспользуемся, очень часто используется для оценок сечений в гиперболических четырехугольниках - поэтому я очень советую его освоить. Пусть $|x| = n$, и рассмотрим такое i, что $|g| + \delta < i < n - |h| - \delta$. Введем следующие обозначения: $a = e$, $b = g$, $c = xg$, $d = x$, $A = x_i g$, $B = x_i$, точки C, D лежат на $[a, c]$ так, что $d(a, D) = i$, $d(C, c) = n - i$.



Так как треугольники в $C_A(G)$ являются δ-узкими, то в треугольнике $[a, b, c]$ расстояние от A до согласованной точки на другой стороне (зависящей от положения A относительно internal point) не больше δ. Но из-за того, что $i > |g| + \delta$ эта согласованная точка никак не может находиться на стороне $[a, b]$, так как сторона $[a, b]$ находится слишком далеко от A, и в таком случае нарушилось бы неравенство треугольника. Таким образом согласованная точка будет находиться на стороне $[a, c]$

и мы ее обозначили за C. Аналогично с B - из-за оценки $i < n - |h| - \delta$ согласованной точкой является D. Таким образом $d(A, C) \leq \delta$ и $d(B, D) \leq \delta$. Теперь из неравенства треугольника для $[a, b, c]$ мы получим $d(a, c) \leq d(a, b) + d(b, c) = |g| + n$, таким образом:

$$d(D, C) = d(a, c) - d(a, D) - d(C, c) = d(a, c) - n \leq |g|$$

И в результате применяя неравенство треугольника к ломанной $A - C - D - B$ (красной) мы получаем:

$$|\gamma_i| = d(A, B) \leq d(A, C) + d(C, D) + d(D, B) \leq 2\delta + |g|$$

И осталось разобрать 2 симметричных случая, когда i не удовлетворяет описанным выше неравенствам, то есть когда $[A, B]$ близок к левой или правой стороне. Рассмотрим случай левой стороны: пусть $i \leq |g| + \delta$, тогда из неравенства треугольника для ломанной $B - a - b - A$ (зеленой) мы получим:

$$|\gamma_i| = d(A, B) \leq d(B, a) + d(a, b) + d(b, A) \leq |g| + \delta + |g| + |g| + \delta = 2\delta + 3|g|$$

В случае $i \geq n - |h| - \delta$ получаем $|\gamma_i| \leq 2\delta + 3|h|$. Легко заметить, что функция $2\delta + 3(|g| + |h|)$ мажорирует все три случая; таким образом мы получаем общую оценку для произвольного i

$$|\gamma_i| \leq 2\delta + 3(|g| + |h|)$$

Иными словами, все γ_i лежат в шаре радиуса $2\delta + 3(|g| + |h|)$, а потому их количество не может превосходить количество элементов в этом шаре $K(|g|, |h|)$, так как в противном случае некоторые из γ_i совпадали бы, но согласно первому факту это невозможно. Таким образом $|x| = n \leq K(|g|, |h|)$; и мы полностью доказали это утверждение. Лично мне это доказательство и использовавшиеся идеи представляются головокружительно красивым: вдумайтесь! Фактически, нам удалось оценить горизонтальную сторону прямоугольника, имея оценки лишь на его вертикальные стороны!

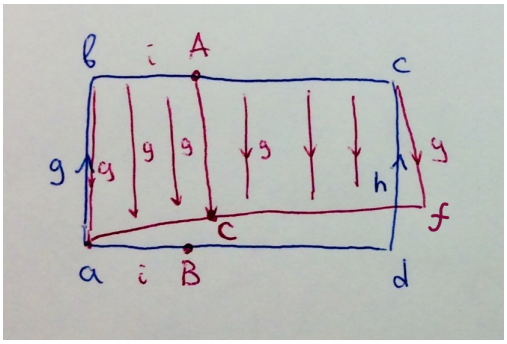
Замечания:

Только что доказанное утверждение очень важное; из него в частности вытекает, что в гиперболических группах разрешима **проблема сопряженности**, *что является усилением ранее обсуждаемого факта, что в гиперболических группах разрешима проблема равенства (напомню, что разрешимость проблемы равенства вытекает из факта, что гиперболические группы допускают копредставление Дэна; также проблема равенства является частным случаем проблемы сопряжения, так как $g = h \Leftrightarrow gh^{-1} \sim 1$): действительно, для проверки $g \sim h$ достаточно проверять равенства $x^{-1}gx = h$ для всех x, у которых длина удовлетворяет только что доказанной оценке, но таких x лишь конечное число - а потому проверяя лишь конечное число равенств вида $x^{-1}gx = h$ мы сможем выяснить, являются ли g и h сопряженными друг другу.*

Также хочется сказать, что этот важный пример является сильнейшим магнитом для ошибочных доказательств и очень легко, упустив крошечную деталь, попасть в ловушку. Приведем пример двух неправильных "доказательств", к которым очень легко прийти, если сильно не вникать в детали.

Первое "доказательство"

Повторим все дословно до выбора i с оценкой $|g| + \delta < i < n - |h| - \delta$. И теперь сдвинем геодезическую $[b, c]$ на элемент g^{-1} (иными словами, подействуем на каждую точку элементом g^{-1}, для вершин графа Кэли это будет просто левым умножением на g^{-1}). Эта операция сохраняет попарные расстояния, а значит геодезическая перейдет в геодезическую, причем $g^{-1}b = a$ (иными словами точка b вернется в точку a).



Пусть $f = g^{-1}c$, тогда в треугольнике $[a, f, d]$ точка $C = g^{-1}A$ будет согласованной для B (с учетом оценок на i), и таким образом из неравенства треугольника мы получим:

$$d(A, B) \leq d(A, C) + d(C, B) = |g^{-1}| + d(C, B) = |g| + d(C, B) \leq |g| + \delta$$

Ошибка в этом рассуждении заключается в том, что хотя визуально напрашивается, что при сдвиге на g точка сдвигается на расстояние $|g|$, то есть $d(x, gx) = |g|$; но это неправда. И можно рассмотреть ту же свободную группу $\mathbb{F}_2 = \langle a, b\rangle$ и $x = ab$ и $g = b$ и увидеть, что:

$$d(gx, x) = d(bab, ab) = |b^{-1}a^{-1}bab| = 5$$

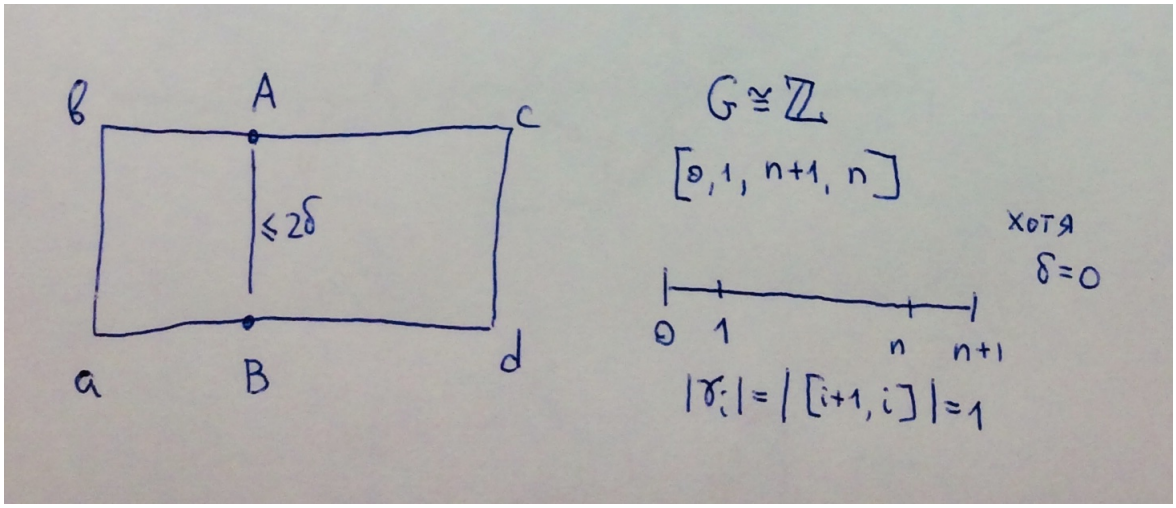
хотя при этом $|g| = |b| = 1$. Хотя несмотря на это небольшое разочарование, напомним, что такие сдвиги действуют изометрично:

$$d(ga, gb) = |b^{-1}g^{-1}ga| = |b^{-1}a| = d(a, b)$$

Со стыдом признаюсь, что я сам в свое время попался в эту ловушку и некоторое время эти "рассуждения" считал доказательством.

Второе "доказательство"

Будем гиперболичность понимать как δ-тонкость всех треугольников. В начале этой главы мы обсуждали, что любая сторона четырехугольника лежит в 2δ-окрестности остальных сторон: в предположении $|g| + 2\delta < i < n - |h| - 2\delta$ мы получим, что для точки A в ее 2δ-окрестности не может быть точек из вертикальных сторон - значит будет существовать точка B на $[a, d]$ такая что $d(A, B) \leq 2\delta$.



И таким образом мы получим, что

$$|\gamma_i| = d(A, B) \leq 2\delta$$

Здесь ошибка более заметная и заключается в том, что $[a, b, c, d]$ нужно мыслить не как прямоугольник, а скорее как параллелограмм: и полученная из 2δ-окрестности точка B совсем не обязана быть согласованной с точкой A, в том смысле, что $d(a, B) = d(b, A)$. Это очень хорошо видно на примере $G = \mathbb{Z}$ и $[0, 1, n+1, n]$ - вырожденный параллелограмм на прямой, и здесь $|\gamma_i| = d(i+1, i) = 1$, хотя при этом $\delta = 0$, потому что граф Кэли группы $\mathbb{Z}$ является прямой, а значит деревом. Но при этом даже при хороших i оценка $|\gamma_i| = 1 \leq 2\delta = 0$ оказывается неверной.

В общем случае нельзя сказать ничего хорошего про то, является ли подгруппа гиперболической группы сама гиперболической (мы это уже с вами обсуждали), однако есть важный класс *квазивыпуклых подгрупп*, при переходе к которым гиперболичность все же сохраняется - и мы сейчас немного погрузимся в их теорию:

Определение

Подгруппа $H < G$ группы G называется квазивыпуклой, если существует $K > 0$, что для любых $x, y \in H$ и для любой геодезической $[x, y]$ выполнено $[x, y] \subset B_K(H)$.

Иными словами любая геодезическая в G, соединяющая произвольные точки из H, должна быть равномерно близка к H. Напомним, что *квазиизометрическим вложением* называется отображение $f : X \to Y$, что существуют a, b, такие что

$$\frac{1}{a} d(x, y) - b \leq d(f(x), f(y)) \leq a \cdot d(x, y) + b$$

В таком случае пишут $X \underset{q.i.}{\hookrightarrow} Y$. Также нужно отметить, что в случае гиперболической группы G условие достаточно проверять *не для произвольной*, а лишь *некоторой* геодезической $[x, y]$, соединяющей выбранные две точки x, y; потому что, как мы уже обсуждали, непосредственно из определения гиперболического пространства, примененного к вырожденному треугольнику с одной нулевой стороной, вытекает, что любая геодезическая, содержится в δ-окрестности любой другой геодезической, если у них совпадают начало и конец. Поэтому если условие

квазивыпуклости выполняется для некоторой геодезической $[x, y]$, то для любой другой

$$[x, y]_* \subset B_\delta([x, y]) \subset B_{K+\delta}(H)$$

оно тоже будет выполнено. В случае же, если группа G не является гиперболической, "любая геодезическая" и "некоторая геодезическая" приводят к разным определениям; но это и не очень важно, так как понятие квазивыпуклости в целом почти бессмысленно за контуром гиперболических пространств. Также отмечу, что по духу определение близко к обычному понятию выпуклости в линейных пространствах, только отрезок оказывается лежащим не в самом множестве, а в некоторой его окрестности радиуса, зафиксированного для всего пространства.

Утверждение

Пусть G - конечно-порожденная группа. Тогда если $H < G$ квазивыпукла, то тождественное вложение $H \underset{q.i.}{\hookrightarrow} G$ является квазиизометрическим вложением.

Без порождающего множества группы нет метрики - а значит и нет геодезических. Пусть $G = \langle A| \dots \rangle$, а d_A - словесная метрика; пусть также K - участвующая в определении квазивыпуклости константа, и рассмотрим конечное множество:

$$B = \{h \in H : d_A(1, h) \leq 2K + 1\}$$

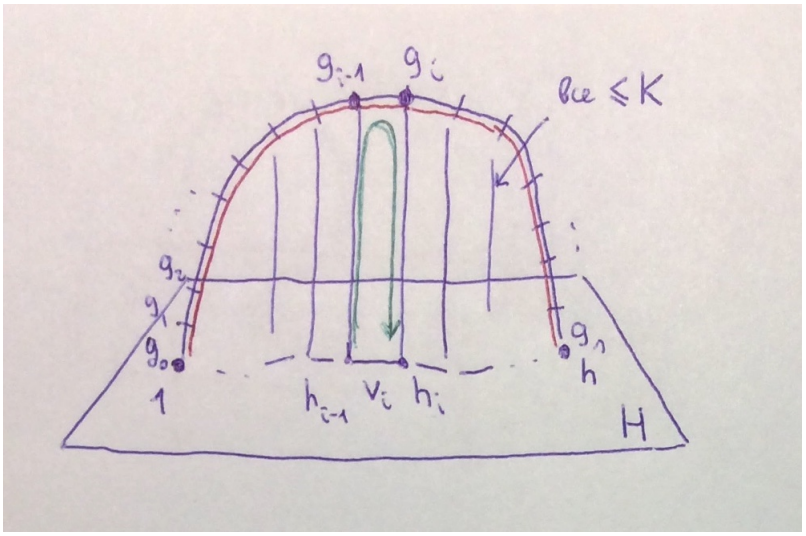
Давайте докажем, что $H = \langle B \rangle$. Рассмотрим произвольное $h \in H$, и рассмотрим геодезическую $[1, h]$ (красную на рисунке) в графе Кэли $C_A(G)$. Последовательные вершины графа, через которые проходит эта геодезическая, мы обозначим через $g_i \in G$ (где $0 \leq i \leq n$), и по условию, для каждой из них существует $h_i \in H$, что $d_A(g_i, h_i) \leq K$ (для удобства будем считать, что $h_0 = 1$ и $h_n = h$). И если $v_i \in H$ - это элемент, соединяющий h_{i-1} и h_i (то есть такой, что $v_i h_{i-1} = h_i$, или что эквивалентно $v_i = h_i h_{i-1}^{-1}$), то:

$$h = h_n = (h_n h_{n-1}^{-1})(h_{n-1} h_{n-2}^{-1}) \dots (h_1 h_0^{-1}) h_0 = v_n v_{n-1} \dots v_1$$

Но легко понять, что

$$|v_i|_G = |h_i h_{i-1}^{-1}|_G = |(h_i h_{i-1}^{-1})^{-1}|_G = d_A(h_{i-1}, h_i) \leq d_A(h_{i-1}, g_{i-1}) + d_A(g_{i-1}, g_i) + d_A(g_i, h_i) \leq 2K+1$$

где $d_A(g_{i-1}, g_i) = 1$, так как это последовательные элементы группы на геодезической. Все может показаться страшным и сложным, но в реальности ситуация очень прозрачная и понятная, если пристально взглянуть на картинку: здесь v_i - это "отрезочки" ломанной, которые связывают 1 и h в H, и так как они реализуют путь до h, то их произведение равно h. Более того их длину можно оценить с помощью неравенства треугольника вдоль ломанной, обход по которой обозначен зеленой стрелочкой.



Таким образом мы получили, что $H = \langle B \rangle$. Обозначим через d_B словесную метрику в H относительно этого набора порождающих. Тогда с одной стороны ясно, что $d_B(1, h) \leq d_A(1, h)$, так как на картинке $d_A(1, h) = n$, и мы смогли представить h как произведение n элементов из B, но теоретически может существовать и более короткое разложение. С другой стороны если представить $h = v_n v_{n-1} \dots v_1$, где $v_i \in B$, но при этом по условию каждый v_i можно представить произведением не более чем $2K + 1$ сомножителей из A, то h заведомо представляется в виде произведения не более чем $(2K + 1)n$ сомножителей из A, иными словами $d_A(1, h) \leq (2K + 1)d_B(1, h)$, таким образом:

$$\frac{d_A(1, h)}{2K + 1} \leq d_B(1, h) \leq d_A(1, h)$$

иными словами тождественное вложение является квазиизометрическим относительно словесных метрик, построенных по исходному порождающему множеству A в G и по построенному при решении задачи порождающему множеству B для H.

Замечание:

Забегая немного вперед скажу, что верно и обратное утверждение, таким образом в гиперболических группах G подгруппа $H < G$ квазивыпукла $\Leftrightarrow$ она вкладывается квазиизометрично. Для доказательства обратной стрелочки $\Leftarrow$ нужно заметить, что если $[x, y]_H$ геодезическая в H, соединяющая x и y; и раз вложение квазиизометрично, то $[x, y]_H$ будет квазигеодезической в G. По лемме Морса, которую мы обсудим далее, квазигеодезическая $[x, y]_H$ равномерно близка к некоторой геодезической $[x, y]$, в частности для любой точки $[x, y]$ можно найти близкую к ней в H. Для произвольных групп G эквивалентность уже не верна: пример очень простой и будет в задачах для самостоятельной работы.

Определение

Пусть (X, d) *- геодезическое метрическое пространство. Кривую* $p : [a, b] \to X$ *мы будем называть* (α, C)*-квазигеодезической (при* $\alpha, C > 0$*), если*

$$\frac{1}{\alpha}|t - s| - C \leq d(p(t), p(s)) \leq \alpha|t - s| + C$$

Если внимательно присмотреться к определению, то легко заметить, что (α, C)-квазигеодезические это в точности (α, C)-квазиизометрические отображения $\mathbb{R} \to X$. Вся эта теория крутится вокруг того, что понятия *квазигеодезичности*, *квазивыпуклости* и *квазиизометричности* очень тесно связаны, в некотором смысле это даже одно и то же.

• Напомню, что в геодезическом пространстве $d(x, y) = \ell([x, y])$ геодезическая определяется как кривая $p : [a, b] \to X$, что $v|t - s| = \ell([p(t), p(s)]) = d(p(t), p(s))$, где v скорость движения вдоль геодезической. Таким образом геодезические являются $(v + \frac{1}{v}, 0)$-квазигеодезическими (хотя обратное неверно), и они являются некоторым идеальным частным случаем, который квазигеодезические пытаются обобщить. Если $v = 1$, то необходимости в этом алгебраическом финте с $v + \frac{1}{v}$ нет, и геодезическая является $(1, 0)$-квазигеодезической.

• Также отмечу, что *непрерывная* кривая p автоматически является квазигеодезической: так как непрерывная функция на компакте (в данном случае на отрезке $[a, b]$) ограничена некоторым M (то есть для некоторой точки x_0 выполнено $d(x_0, p(s)) \leq M$). Тогда из неравенства треугольника мы получим, что

$$-2M \leq d(p(t), p(s) \leq 2M$$

$$\frac{1}{\alpha}|t - s| - \frac{1}{\alpha}|t - s| - 2M \leq d(p(t), p(s) \leq \alpha|t - s| + 2M$$

а потому p является $(\alpha, 2M + \frac{1}{\alpha}(b - a))$-квазигеодезической при любом α. При этом замечу, что типичной квазигеодезической в нашем случае будет геодезическая ломанная, соединяющая по ребрам графа Кэли некоторую последовательность групповых элементов, и она является непрерывной; но при этом наша теория не теряет осмысленности, так как в большинстве задач ситуация так закручивается, что важен не только факт квазигеодезичности, но и параметры квазигеодезичности (α, C).

• Также отмечу, что образ геодезической при (α, C)-квазиизометрии является (α, C)-квазигеодезической - это утверждение фактически тавтологическое. И с учетом последнего доказанного утверждение о квазиизометричности вложения квазивыпуклой подгруппы; мы получаем, что *если* $H < G$ *квазивыпукла, то геодезические в* H *являются квазигеодезическими в* G.

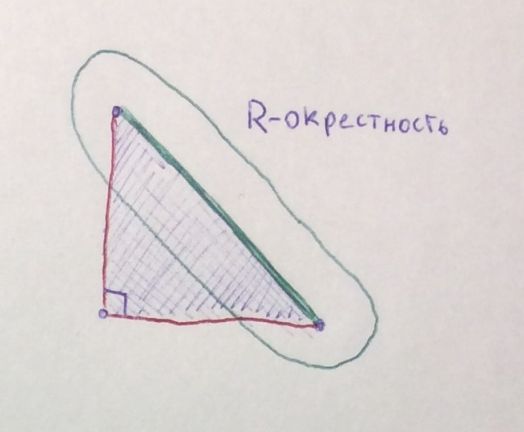
Мощь и сила теории квазигеодезических проявляется в *Лемме Морса*, являющейся одним из центральных утверждений в теории гиперболических групп, причем находящей практическое применение даже в нематематических областях: например, ее используют для анализа взаимодействия пользователей с интерфейсом некоторых приложений, например, Google maps.

Лемма (Морс)
Пусть X это δ-гиперболическое пространство. Тогда существует константа $R = R(\delta, \alpha, C)$, что для любых $p, q \in X$ и для любой (α, C)-квазигеодезической γ', соединяющей p и q, верно:

$$\gamma' \subset B_R([p,q]) \text{ и } [p,q] \subset B_R(\gamma')$$

(в таком случае обычно пишут $d_H([p,q], \gamma') \leq R$ и говорят, что расстояние Хаусдорфа между этими двумя множествами не превосходит R).

Иными словами каждая квазигеодезическая равномерно близка к некоторой геодезической. Ясно, что в евклидовых пространствах такое свойство совершенно абсурдно: к примеру, если рассмотреть равнобедренный прямоугольный треугольник - тогда красный путь, идущий со скоростью 1 вдоль двух сторон, будет $(\sqrt{2}, 0)$-квазигеодезической. Но ясно, что не будет существовать единого R, что такие красные линии лежат в R-окрестности зеленой геодезической, так как габариты треугольника можно увеличивать не меняя параметров квазигеодезичности.



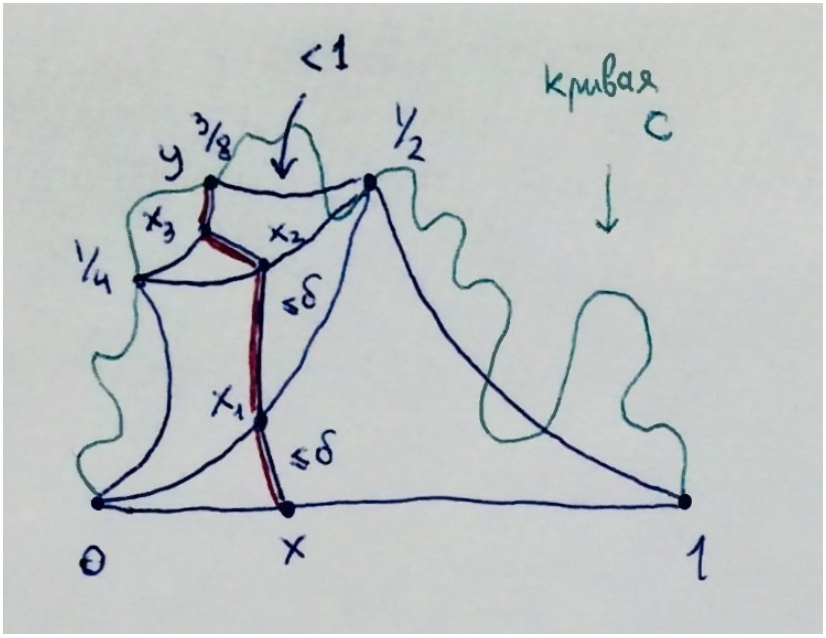
И эта лемма является еще одной отличной иллюстрацией равномерной природы гиперболических пространств, где часто возникают геометрические параметры, вообще не зависящие от габаритов связанных с ними геометрических объектов. В формулировке для квазигеодезической я использовал необычное обозначение γ' для удобства, так как больше всего в доказательстве нам придется работать работать с ее аппроксимацией γ, и хотелось бы штрихов писать поменьше. Я приведу доказательство, потому что оно основывается на нескольких красивых геометрических идеях, представляющих самостоятельную ценность. Отмечу, что расстояние Хаусдорфа удовлетворяет всем аксиомам метрики.

Вспомогательная лемма
Пусть X - это δ-гиперболическое пространство, $c : [0,1] \to X$ некоторая непрерывная кривая ограниченной длины $\ell(c) = \ell$ (не обязательно являющаяся квазигеодезической), и пусть $c(0) = p$ и $c(1) = q$. Тогда для любой $x \in [p,q]$ выполнено

$$d(x, c) \leq \delta(|\log_2 \ell| + 1) + 1$$

То есть расстояние от любой точки геодезической $[p,q]$ до кривой c имеет порядок $|\log_2 \ell|$, что опять-таки невозможно в евклидовом случае, где подобная

оценка может иметь только линейный по ℓ порядок. Лемму мы докажем принципом дихотомии: так как c непрерывна - изменим параметризацию так, чтобы двигаться по кривой с постоянной скоростью. Рассмотрим произвольную точку $x \in [p,q] = [c(0), c(1)]$ и в этой новой параметризации рассмотрим треугольник $[c(0), c(1/2), c(1)]$. Из гиперболичности мы получим, что $d(x, x_1) \leq \delta$ для некоторой точки $x_1 \in [c(0), c(1/2)] \cup [c(1/2), c(1)]$. Пусть для определенности это будет $[c(0), c(1/2)]$. Тогда поделим пополам тот временной промежуток, который нам выпал (в данном случае это $[0, 1/2]$) - и рассмотрим треугольник $[c(0), c(1/4), c(1/2)]$ - из гиперболичности опять найдется точка x_2, что $d(x_1, x_2) \leq \delta$, и точка x_2 лежит на одной из двух новых сторон, пусть для определенности это будет $[c(1/4), c(1/2)]$. Потом рассмотрим соответствующий делению пополам полученного временно́го интервала треугольник $[c(1/4), c(3/8), c(1/2)]$ и так далее. И делить пополам мы будем до тех пор, пока обе боковые стороны этого треугольника не станут меньше 1, а именно повторим эту операцию N раз, пока не будет выполняться $\frac{\ell}{2^N} < 1 \leq \frac{\ell}{2^{N-1}}$ (треугольники геодезические, а потому длина его сторон не превосходит длины соответствующего сегмента кривой c, которая в точности равна $\frac{\ell}{2^N}$).



Пусть $\ell \geq 1$. Тогда после N итераций рассмотрим $y = c\left(\frac{M}{2^N}\right)$, где $\frac{M}{2^N}$ точка временно́го отрезка, соответствующая добавленной вершине треугольника, полученного на последней итерации нашей дихотомии, и в силу выбора N мы имеем $d(y, x_N) < 1$. Таким образом если расписать неравенство треугольника вдоль ломанной, проходящей через все построенные точка x_i (красная ломанная, в этом иллюстративном примере $N = 3$), то получим:

$$d(x,y) \leq d(x,x_1) + d(x_1,x_2) + \ldots + d(x_{N-1},x_N) + d(x_N,y) < \delta N + 1 \leq \delta(\log_2 \ell + 1) + 1$$

где последнее неравенство получено из неравенства $1 \leq \frac{\ell}{2^{N-1}}$.

Во второй ситуации, когда $\ell < 1$, нельзя провести ни одной итерации, но можно заметить, что так как геодезическая - это кратчайший путь, то $\ell([p,q]) \leq \ell < 1$. И тогда для произвольной $x \in [p,q]$ мы имеем $d(x,p) < 1$, но так как $p \in c$, то и $d(x,c) < 1$. Ну и методом пристального взгляда получаем, что оценка:

$$d(x,c) \leq \delta(|\log_2(\ell)| + 1) + 1$$

годится для обеих ситуаций.

Далее нужно доказать техническую лемму, с очень пугающей формулировкой:

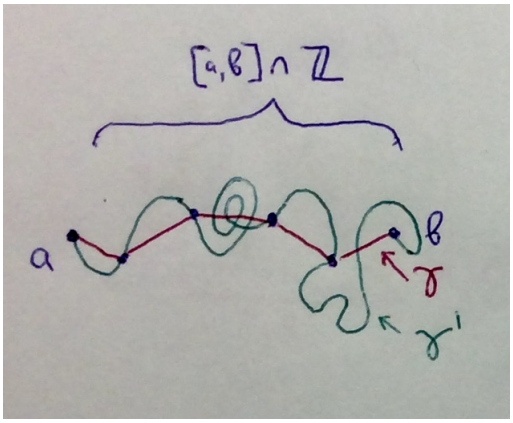
Лемма (об укрощении квазигеодезических)

Пусть X - геодезическое пространство и $\gamma' : [a,b] \to X$ является (α, C)-квазигеодезической (пусть также $\alpha \geq 1$). Тогда существует непрерывная (α, C_*)-квазигеодезическая $\gamma : [a,b] \to X$ с условиями:

- $\gamma(a) = \gamma'(a)$ *и* $\gamma(b) = \gamma'(b)$
- $C_* = 3(\alpha + C)$
- $\gamma' \subset B_{\alpha+C}(\gamma)$ *и* $\gamma \subset B_{\alpha+C}(\gamma')$, *или иными словами* $d_H(\gamma, \gamma') \leq \alpha + C$
- $\ell(\gamma|_{[s,t]}) \leq A \cdot d(\gamma(s), \gamma(t)) + B$ *для любых* $s, t \in [a,b]$, *и где* $A = \alpha(\alpha + C)$ *и* $B = 3(\alpha + C)(\alpha(\alpha + C) + 1)$.

Требование $\alpha \geq 1$ совершенно несущественно и нужно лишь чтобы в доказательстве в одном месте сделать оценку чуть более красивой. Если вдруг это условие не выполнено, то легко заметить, что если $\alpha \leq \alpha_0$ и $C \leq C_0$ и p является (α, C)-квазигеодезической, то она является и (α_0, C_0)-квазигеодезической, так что параметры можно увеличивать без существенного вреда качественной природы. Фактически эта лемма утверждает, что любую квазигеодезическую по расстоянию Хаусдорфа можно приблизить непрерывной квазигеодезической с хорошей оценкой на длины ее сегментов.

Пусть $\Sigma = \mathbb{Z} \cap [a,b]$, и для $t \in \mathbb{R}$ определим $[t]$ как ближайшую к t точку из Σ (для точек вида $\mathbb{Z} + \frac{1}{2}$ возьмем одну из них). Ясно, что $|[t] - t| \leq \frac{1}{2}$ для любого t, а значит $|t - s| - 1 \leq \big|[t] - [s]\big| \leq |t - s| + 1$ для любых t, s (чтобы не возиться с дробями я буду в первой оценке оценивать $|[t] - t|$ тоже 1 а не $\frac{1}{2}$). Определим $\gamma(t) = \gamma'(t)$ для точек $t \in \Sigma \cup \{a, b\}$, а на остальных определим γ идущей с постоянной скоростью вдоль геодезических сегментов, соединяющих последовательные образы Σ. Иными словами доопределим на остальных точках ее кусочно-линейным образом, если геодезические считать за линии. Мы докажем, что данная γ будет искомой.



Также легко заметить, что для любого t из квазигеодезичности мы получаем $d(\gamma'(t), \gamma'([t])) \leq \alpha|t - [t]| + C \leq \alpha + C$. Также имеем:

$$d(\gamma(i), \gamma(i+1)) = d(\gamma'(i), \gamma'(i+1)) \leq \alpha + C$$

для $i \in \Sigma$. Таким образом длина каждого описанного выше геодезического сегмента ломанной не превосходит $\alpha + C$ (для "целочисленных" это вытекает из этой оценки, а

для двух ситуаций с выходом на границу вытекает из аналогичных оценок, с заменой i и $i+1$ на a и i в случае левой границы, где i ближайшая к a точка из Σ; аналогично для правой границы), а значит $d(\gamma(t), \gamma([t])) \leq \alpha + C$. Таким образом:

$$\gamma(\Sigma) \subset \gamma \subset B_{\alpha+C}(\gamma(\Sigma))$$

$$\gamma(\Sigma) \subset \gamma' \subset B_{\alpha+C}(\gamma(\Sigma))$$

А значит получаем:

$$\gamma \subset B_{\alpha+C}(\gamma(\Sigma)) \subset B_{\alpha+C}(\gamma')$$

И совершенно аналогично проверяется $\gamma' \subset B_{\alpha+C}(\gamma)$, что доказывает пункт про условие на расстояние Хаусдорфа.

Используя квазигеодезичность γ' мы получаем следующие простые оценки:

$$d(\gamma(s), \gamma(t)) \leq d(\gamma([s]), \gamma([t])) + 2(\alpha + C) = d(\gamma'([s]), \gamma'([t])) + 2(\alpha + C) \leq$$
$$\leq \alpha\big|[s] - [t]\big| + 2\alpha + 3C \leq \alpha(|s - t| + 1) + 2\alpha + 3C = \alpha|s - t| + 3(\alpha + C)$$

$$\frac{1}{\alpha}|s - t| - 3(\alpha + C) \leq \frac{1}{\alpha}\left(\big|[s] - [t]\big| + 1\right) - (3\alpha + 3C) \underset{\alpha \geq 1}{\leq} \frac{1}{\alpha}\big|[s] - [t]\big| - (2\alpha + 3C) \leq$$
$$\leq d(\gamma'([s]), \gamma'([t])) - 2(\alpha + C) = d(\gamma([s]), \gamma([t])) - 2(\alpha + C) \leq d(\gamma(s), \gamma(t))$$

которые доказывают $(\alpha, 3(\alpha+C))$-квазигеодезичность γ. Для доказательства условия на длины заметим, что для $n, m \in \mathbb{Z}$

$$\ell(\gamma|_{[n,m]}) = \sum_{i=n}^{m-1} d(\gamma(i), \gamma(i+1)) = \sum_{i=n}^{m-1} d(\gamma'(i), \gamma'(i+1)) \leq (\alpha + C)|m - n|$$

В общем случае мы получим:

$$\ell(\gamma|_{[s,t]}) \leq (\alpha+C)+\ell(\gamma|_{[[s],[t]]})+(\alpha+C) \leq (\alpha+C)\big|[s]-[t]\big|+2(\alpha+C) \leq (\alpha+C)|s-t|+3(\alpha+C)$$

Но при этом в нашем арсенале уже есть оценка:

$$d(\gamma(s), \gamma(t)) \geq \frac{1}{\alpha}|s - t| - 3(\alpha + C)$$

из которой можем оценить $|s - t|$, и таким образом:

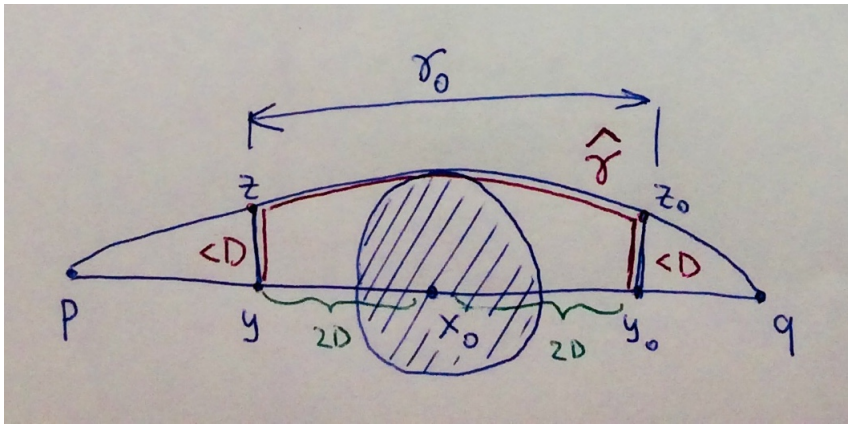
$$\ell(\gamma|_{[s,t]}) \leq \alpha(\alpha + C)d(\gamma(s), \gamma(t)) + 3\alpha(\alpha + C)(\alpha + C) + 3(\alpha + C)$$

что окончательно доказывает эту техническую лемму.

Далее рассмотрим эту построенную в лемме непрерывную квазигеодезическую $\gamma : [0, 1] \to X$ (без ограничения общности можно считать, что временной интервал стандартный). Пусть $\gamma(0) = p$ и $\gamma(1) = q$, и рассмотрим x_0, на котором достигается

$$D = \sup_{x \in [p,q]} d(x, \gamma)$$

достигается он за счет непрерывности c (но достижимость здесь не очень важна, и можно взять точку, расстояние от которой до γ чуть меньше D). Рассмотрим $y, y_0 \in [p, q]$, такие что $d(x_0, y) = d(x_0, y_0) = 2D$ - отступим вдоль геодезической с двух сторон от x_0 на $2D$, а если такой отступ выйдет за край отрезка - то просто возьмем его соответствующий конец. Так как на x_0 достигался супремум, то существуют $z, z_0 \in \gamma$, что $d(y, z) < D$ и $d(y_0, z_0) < D$ (причем положим $z = y$ и $z_0 = y_0$ в тех ситуациях, когда выступ выходил за границы отрезка). И рассмотрим красную кривую $\hat{\gamma}$, соединяющую y и y_0 и идущую сначала по геодезической $[y, z]$, затем от z до z_0 вдоль γ и потом по $[z_0, z]$. Довольно легко заметить, что по построению такая кривая не пересекает открытый шар с центром в x_0 и радиусом D:



Выписывая неравенство треугольника вдоль ломанной $z - y - y_0 - z_0$ мы получим, что $d(z, z_0) < D + 4D + D = 6D$. Пусть γ_0 - часть кривой γ, зажатая между z и z_0. Из технической леммы об укрощении вытекает $\ell(\gamma_0) \leq 6AD + B$, а значит:

$$\ell(\hat{\gamma}) \leq 2D + \ell(\gamma_0) \leq (6A + 2)D + B$$

Но с учетом первой леммы мы получаем (при условии, что $\ell(\hat{\gamma}) > 1$ для монотонности модуля логарифма):

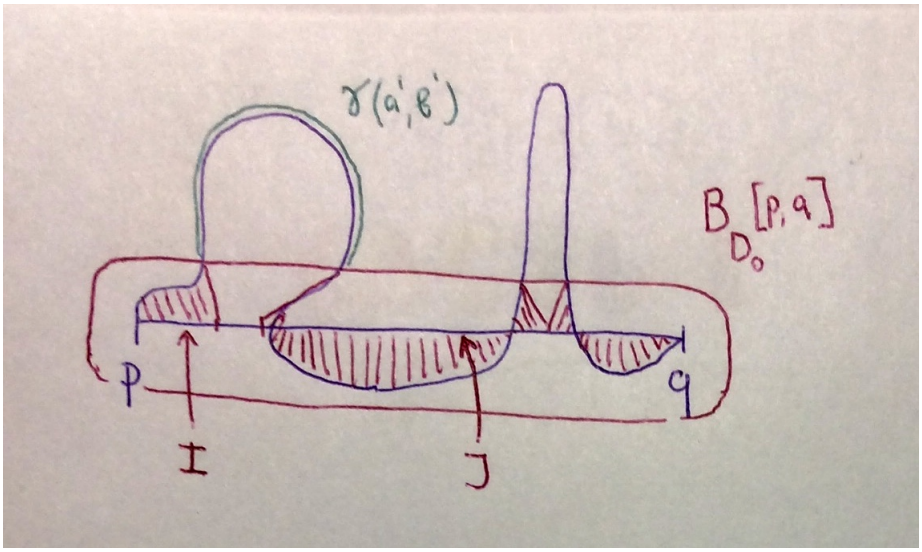
$$D \leq \delta(|\log_2((6A + 2)D + B)| + 1) + 1$$

Так как логарифмическая функция растет медленнее линейной, то решением этого неравенства не может быть неограниченное вправо множество - а значит существует некоторое максимальное D_0, заведомо мажорирующее все решения - оно и будет искомым. Если же $\ell(\hat{\gamma}) \leq 1$, то тогда $d(y, y_0) = \ell([y, y_0]) \leq 1$, а значит

$$d(x_0, t) \leq d(x_0, y) + d(y, t) \leq d(y, y_0) + \ell(\hat{\gamma}) \leq 2$$

для любой $t \in \hat{\gamma}$, тогда в роли мажоранты для D подойдет $D_0 = 2$. Таким образом в обоих случаях мы получаем $[p, q] \subset B_{D_0}(\gamma)$.

Для доказательства $\gamma \subset B_R([p,q])$ рассмотрим некоторый максимальный (то есть такой, который невозможно расширить) интервал $(a',b') \subset [a,b]$, что $\gamma|_{(a',b')}$ не пересекается с $B_{D_0}([p,q])$ (интервал нужно брать открытый, так как мы определяли $B_R(X)$ как замкнутые окрестности X), их может быть несколько, но возьмем один их них).



Из ранее доказанного $[p,q] \subset B_{D_0}(\gamma)$ вытекает, что для любой $x \in [p,q]$ для некоторой $t \in [a,b]$ будет выполнено $d(x,\gamma(t)) \leq D_0$, рассмотрим $I \subset [p,q]$ (соответственно $J \subset [p,q]$) множество таких $x \in [p,q]$, для которых вышеупомянутое t можно взять лежащим в $[a,a']$ (соответственно в $[b',b]$). Так как $\gamma|_{(a',b')}$ и $B_{D_0}([p,q])$ не пересекаются, то $I \cup J = [p,q]$. Также довольно несложно понять, что в силу компактности множеств $\gamma|_{[a,a']}$ и $\gamma|_{[b',b]}$, множества I и J будут замкнутыми. А потому в силу связности $[p,q]$ мы получаем, что $I \cap J \neq \emptyset$; пусть $\omega \in I \cap J$, тогда существуют $t_a \in [a,a']$ и $t_b \in [b',b]$, что $d(\omega,\gamma(t_a)) \leq D_0$ и $d(\omega,\gamma(t_b)) \leq D_0$, а значит $d(\gamma(t_a),\gamma(t_b)) \leq 2D_0$. Таким образом для любого $s \in (a',b')$ выполнено:

$$d(\gamma(a'),\gamma(s)) \leq \alpha|a'-s| + C_* \leq \alpha|t_a - t_b| + C_* \leq$$

$$\leq \alpha\left(\alpha d(\gamma(t_a),\gamma(t_b)) + \alpha C_*\right) + C_* \leq \alpha(2\alpha D_0 + \alpha C_*) + C_* =: R_0$$

напомним, что (α, C_*) - это параметры квазигеодезичности для γ, которые мы вычисляли в лемме об укрощении. В середине этой цепочки неравенств мы использовали получающееся элементарными выкладками из определения квазигеодезичности неравенство $|t-s| \leq \alpha d(\gamma(t),\gamma(s)) + \alpha C_*$. Иными словами, многие точки γ находятся на расстоянии D_0 от $[p,q]$, а если точка и попала в большой выходящий из $B_{D_0}([p,q])$ всплеск, то она все равно находится на расстоянии R_0 от $B_{D_0}([p,q])$, иными словами $\gamma \subset B_{D_0+R_0}([p,q])$. Таким образом мы получаем, что $d_H(\gamma,[p,q]) \leq D_0 + R_0$, а с учетом того, что согласно лемме об укрощении $d_H(\gamma,\gamma') \leq 2(\alpha + C)$, мы можем применить неравенство треугольника $d_H(\gamma',[p,q]) \leq d_H(\gamma',\gamma) + d_H(\gamma,[p,q])$, что завершает доказательство леммы Морса.

Мы сразу же можем доказать крайне важные следствия этой леммы, главным образом ради которых она и нужна:

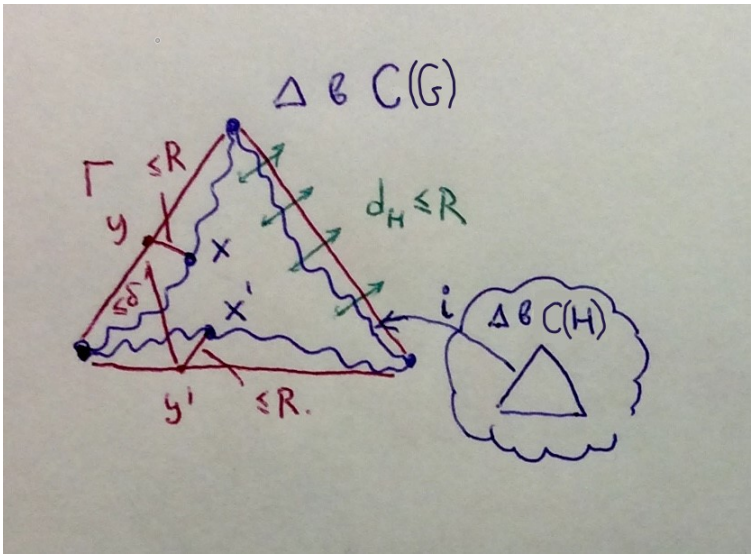
Следствие

Пусть $H < G$ является квазивыпуклой подгруппой и G - гиперболическая, тогда H тоже является гиперболической.

Если H - квазивыпукла, то мы уже доказывали, что $H \underset{q.i.}{\hookrightarrow} G$, но так как тождественное отображение индуцирует $N \underset{q.i.}{\sim} C(N)$ квазиизометрический изоморфизм любой группы и ее графа Кэли, то $i : C(H) \underset{q.i.}{\hookrightarrow} C(G)$ для некоторых порождающих множеств с параметрами квазиизометричности (α, C). Пусть Δ это геодезический треугольник в $C(H)$, и если считать, что по геодезическим мы движемся со скоростью 1 - то $i(\Delta)$ это (α, C)-квазигеодезический треугольник в $C(G)$. Применяя для каждой из его квазигеодезических сторон лемму Морса мы получаем геодезический треугольник Γ в $C(G)$, который является δ-тонким. Обозначим через d_* метрику $C(G)$ и через d метрику $C(H)$. Теперь рассмотрим произвольную точку $x \in \Delta$ (мы будем отождествлять x и $i(x)$), она лежит на какой-то стороне треугольника - и тогда на соответствующей стороне треугольника Γ по лемме Морса мы можем найти y, что $d_*(y, x) \leq R$. Так как Γ - тонкий - то на оставшихся сторонах Γ можно найти точку y', что $d_*(y, y') \leq \delta$, ну и опять по лемме Морса на соответствующей паре сторон треугольника Δ можно найти x', что $d_*(y', x') \leq R$. Таким образом для любой точки $x \in \Delta$ на других сторонах мы нашли x', что $d_*(x, x') \leq \delta + 2R$, из определения квазиизометричности мы получаем $\frac{1}{\alpha} d(x, x') - C \leq d_*(x, x')$, а потому:

$$d(x, x') \leq \alpha(\delta + 2R) + \alpha C$$

таким образом H является гиперболической группой с параметром тонкости $\alpha(\delta + 2R + C)$.



Следствие

Пусть $X \underset{q.i.}{\sim} Y$, X - гиперболическое и Y - геодезическое. Тогда Y - гиперболическое.

Доказательство почти дословно повторяет доказательство предыдущего следствия: строим геодезический треугольник в Y, его образ в X - это квазигеодезический треугольник в X, по лемме Морса его можно приблизить геодезическим треугольником в X и т.д. Напомню, что по нашему определению гиперболические пространства автоматически геодезические.

Замечания:

Эти следствия фактически ведут к следующему полуфилософскому посылу: что квазиизометричность - это мера, с точностью до которой нужно смотреть на гиперболические пространства в целом, и даже на то, что происходит внутри них в частности.

Иногда лемму Морса формулируют в облегченном варианте: что просто $\gamma' \subset B_R([p,q])$ вместо усиленной и доказанной нами формулировки с расстоянием Хаусдорфа, то есть одновременным выполнением и $[p,q] \subset B_R(\gamma')$. Вообще говоря одно вложение еще не влечет близость по Хаусдорфу, как можно было понять по одной из недавних картинок, когда одно множества может делать сильные всплески, уходящие очень далеко от другого множества. И стоит отметить, что для доказательства этих следствий недостаточно упрощенной формулировки: так в доказательстве нам приходилось не только по точке x на квазигеодезической найти близкое y на геодезической, но и наоборот: по точке на геодезической y' найти близкую точку на квазигеодезической x'.

Очень важное замечание:

Теперь немного шокирующая новость: в теории групп нет консенсуса по поводу того, что называть квазигеодезическими (я уже молчу про математику в целом, так как есть понятие квазигеодезических в теории выпуклых поверхностей, введенное А.Д. Александровым - и это прямо в корне совсем про другое). Так вот некоторые определяют квазигеодезические в теории гиперболических пространств как имеющие длину кривые $\gamma : [a,b] \to X$, что для некоторых констант $\alpha, C > 0$ выполнено:

$$\frac{1}{\alpha}\ell(\gamma|_{[t,s]}) - C \leq d(\gamma(t),\gamma(s)) \leq \alpha\ell(\gamma|_{[t,s]}) + C$$

иными словами то же самое, только с заменой нашего $|t-s|$ на длину соответствующего сегмента квазигеодезической $\ell(\gamma_{[t,s]})$. Вы, наверное, ждете, что я скажу, что эти определения эквивалентны... но это не так: к примеру в этом определении кривая имеет ограниченную длину, тогда как в определении, которое мы дали, длина не обязаны быть конечной - и можно рассмотреть что-то вроде ограниченной бесконечно-накручивающейся на себя спирали $[0,1] \to \mathbb{R}^2$ с бесконечной длиной, но при этом квазигеодезической из-за своей ограниченности: α не важно, просто нужно подобрать достаточно большое C.

Однако не нужно сильно паниковать из-за неэквивалентности, так как в этой теории практически ничего не меняется, если вместо кривой взять близкую к ней по метрике Хаусдорфа - и по ходу доказательства леммы об укрощении становится понятно, что хотя $|t-s|$ и $\ell(\gamma_{[t,s]})$ и близко не должны быть связаны друг с другом, однако можно найти для γ близкую кривую, для которой на $|t-s|$ и $\ell(\gamma_{[t,s]})$ можно записать двухсторонние оценки (и это означает, что лемма об укрощении оказывается намного более глубокой, чем может изначально показаться): так что существуют лазеечки для перехода от одного определения к другому. Более того ясно, что если в определении квазигеодезической через длины вдоль кривой двигаться с постоянной скоростью - то такие определения будут эквивалентными.

Что касается плюсов и минусов каждого из подходов - то плюсы нашего подхода заключаются в том, что с этим определением проще работать (вычесть одно число из другого проще, чем вычислить длину кривой в абстрактном метрическом пространстве). Многие утверждения при нашем подходе становятся очевидными или даже тавтологическими, как например то, что образ геодезической при квазиизометрии является квазигеодезической: при подходе к определению квазигеодезических через длины это содержательная теорема. К минусом я бы отнес, что хотя некоторые утверждения с таким подходом доказываются проще - доказательство некоторых утверждений усложняется (особенно тех, где что-то утверждается про длину кривой). К примеру, доказательство леммы об укрощении при нашем подходе сложнее, тогда как при подходе через длины в этой лемме не пришлось бы доказывать пункт про длины. Еще один минус нашего подхода заключается в меньшей геометричности: если подход через длины означает, что длина любого сегмента кривой допускает двусторонние линейные оценки по длине соответствующего геодезического сегмента, то в нашем определении все сильно зависит от параметризации, а $|t-s|$ вообще лежит в пространстве параметров и в X вообще не имеет никакого геометрического смысла.

Следующее идейное продолжение леммы Морса является очень важным, потому что на него зацикливаются несколько важных структурных результатов о гиперболических группах:

Утверждение

Пусть G - гиперболическая группа, $g \in G$ с $\mathrm{ord}(g) = \infty$. Тогда $\langle g \rangle \cong \mathbb{Z} \hookrightarrow G$ является квазиизометрией, иными словами существуют константы $A, C > 0$, что

$$\frac{n}{A} - C \leq |g^n|_G \leq An + C$$

Для удобства давайте в этой задаче обозначим словесную метрику $|g|_G$ через $|g|$ без индекса, так как мы не будем работать со словами, а будем работать только с групповыми элементами. Замечу, что правое неравенство очевидно, так как из свойств словесной метрики вытекает $|g^n| \leq n|g|$. Отмечу, что в данной задаче на $\langle g \rangle$ рассматривается именно метрика, индуцированная стандартной метрикой на $\mathbb{Z}$, так как если метрику наследовать из G, то утверждение будет просто тривиальным, а вложение не просто квазиизометричным, а даже изометрией. Также верна "непрерывная" версия этого утверждения, что $\gamma \underset{q.i.}{\hookrightarrow} C(G)$, где γ - кривая, геодезическими сегментами соединяющая все последовательные g^n и g^{n+1} (иными словами $\gamma = \bigcup\limits_n [g^n, g^{n+1}]$), и метрика на которой опять-таки индуцирована стандартной метрикой в $\mathbb{Z}$ (и вытекает это из того факта, что $G \underset{q.i.}{\sim} C(G)$ и $\langle g \rangle \underset{q.i.}{\sim} \gamma$). Пусть константа гиперболичности δ является константой для узкости треугольников, а также является натуральным числом (в противном случае ее можно увеличить, не нарушив свойства гиперболичности). И рассмотрим произвольное натуральное R. Так как $\mathrm{ord}(g) = \infty$ и в каждом шаре у нас конечное число элементов группы, то существует k, такое что:

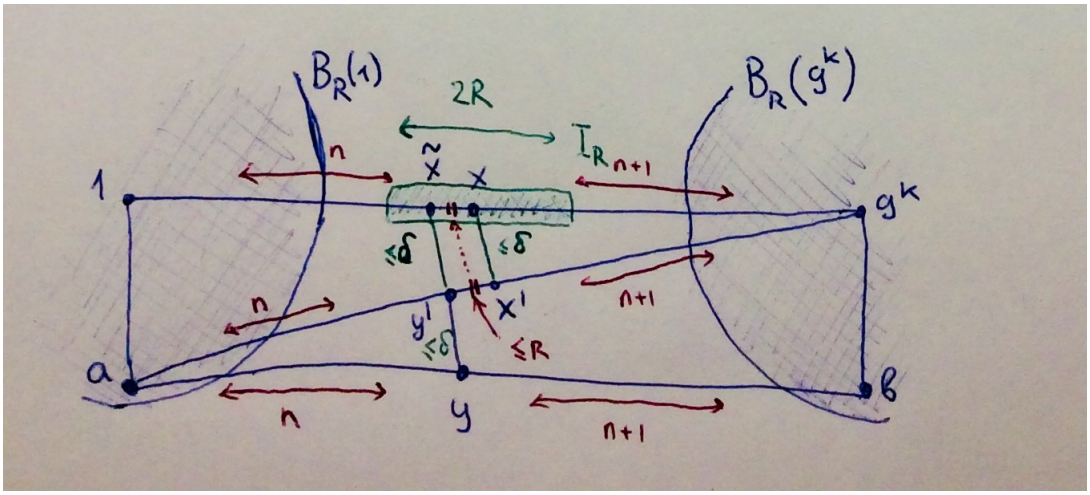
$$|g^k| \geq 4R + 2\delta + 2$$

Легко заметить, что длина отрезка $[a, b] \subset C(G)$ с вершинами $a, b \in G$ является целочисленной (и равна количеству входящих в нее ребер графа Кэли). Будем называть *"серединой"* такого отрезка элемент $c \in [a, b]$, что $c \in G$ и $d(a, c) = n$ где $d(a, b) = 2n$ или $d(a, b) = 2n + 1$ в зависимости от четности $d(a, b)$; иными словами в случае четной длины c - это классическая середина, а в случае нечетной - ближайший слева к середине элемент G на $[a, b]$. Также ясно, что расстояние от середины до "середины" не превосходит $\frac{1}{2}$ вне зависимости от четности.

Факт I

Рассмотрим произвольный $a \in B_R(1)$ и $b \in B_R(g^k)$, где $a, b \in G$. Пусть $d(1, g^k) = d(a, b)$. Рассмотрим геодезический четырехугольник $[1, g^k, b, a]$. Пусть x и y являются "серединами" отрезков $[1, g^k]$ и $[a, b]$ соответственно. Рассмотрим геодезический отрезок $I_R \subset [1, g^k]$ длины $2R$ и с центром в x. Тогда $y \in B_{2\delta}(I_R)$.

Для доказательства мы воспользуемся теми же идеями, что использовали в задаче на оценку длины сопрягающего элемента. Рассмотрим более сложный случай нечетной длины $d(1, g^k) = 2n + 1$ (доказательство в четном случае практически один в один такое же).



Рассмотрим $y' \in [a, g^k]$ согласованный с y в $[a, b, g^k]$, то есть такой, что $d(a, y) = d(a, y')$, и согласованный $x' \in [a, g^k]$ для x в $[1, a, g^k]$. Тогда с учетом того, что $d(1, g^k) = d(a, b) = 2n + 1$, из неравенства треугольника мы получаем, что

$$2n + 1 - R \leq d(a, g^k) \leq 2n + 1 + R$$

а значит $d(y', x') = |d(a, g^k) - (2n+1)| \leq R$ (замечу, что априори возможна ситуация, когда x' лежит левее y' - поэтому нужен модуль). В таком случае рассмотрим точку $\tilde{x} \in [1, g^k]$, согласованную с y' в $[1, a, g^k]$. И с учетом того, что $d(x', y') \leq R$ мы получаем $d(\tilde{x}, x) \leq R$ (то есть для построения $\tilde{x}$ нужно просто в правильную сторону отложить $d(y', x')$). По определению мы получаем, что $\tilde{x} \in I_R$. Также отмечу, что все введенные выше точки лежат в G: так как в G лежат вершины четырехугольника, а при построении остальных мы откладывали целочисленные расстояния вдоль геодезических отрезков, соединяющих элементы G.

И теперь станет ясно, откуда взялось $4R + 2\delta + 2$: это необходимая оценка, чтобы к построенным парам согласованных точек можно было применить условие узкости. В случае y: так как $d(b, g^k) \leq R$ и

$$d(y, b) = n + 1 = \frac{2n+1}{2} + \frac{1}{2} \geq \frac{4R + 2\delta + 2}{2} + \frac{1}{2} = 2R + \delta + \frac{3}{2} > R + \delta$$

таким образом на отрезке $[b, g^k]$ не может быть точек на расстоянии $\leq \delta$ от y - значит именно до согласованной точки на $[a, g^k]$ расстояние будет $\leq \delta$ из-за δ-узкости треугольника, иными словами $d(y, y') \leq \delta$. Аналогично и с верхним отрезком: нужно убедиться, что зеленый I_R не пересекается с $B_{R+\delta}(1)$, состоящим из точек, которые потенциально могут быть на расстоянии $\leq \delta$ от $[1, a]$. Для этого сделаем оценку:

$$d(1, \tilde{x}) \geq d(1, x) - d(x, \tilde{x}) \geq n - R = \frac{2n+1}{2} - \frac{1}{2} - R \geq \frac{4R + 2\delta + 2}{2} - \frac{1}{2} - R > R + \delta$$

Таким образом $d(\tilde{x}, [1, a]) > \delta$, а значит $d(\tilde{x}, y') \leq \delta$. И из неравенства треугольника получаем, что $d(y, \tilde{x}) \leq 2\delta$, но так как $\tilde{x} \in I_R$, то $y \in B_{2\delta}(I_R)$.

Пусть теперь $N = 3|B_{2\delta}(1)|$. Так как в I_R всего $2R + 1 \leq 3R$ элементов группы G ("целочисленные" элементы I_R это x и по R штук слева и справа), то

$$|B_{2\delta}(I_R)| \leq 3R|B_{2\delta}(1)| = NR$$

так как $B_{2\delta}(I_R)$ состоит из 2δ-окрестностей вокруг всех своих "целочисленных" точек, которых $\leq 3R$, а количество точек в 2δ-окрестности не зависит от того, вокруг какой точки мы строим окрестность. Теперь рассмотрим $\alpha = [1, g^k]$ и его сдвиги:

$$\alpha, g\alpha, \ldots, g^{NR}\alpha$$

"Серединами" этих отрезков являются элементы вида $g^i x$ (где x это "середина" α), и они не могут совпадать для двух различных отрезков, так как в таком случае было бы $g^i x = g^j x$, но так как $x \in G$ то $g^{i-j} = 1$, что невозможно из-за $\mathrm{ord}(g) = \infty$. Если предположить, что $g^i \in B_R(1)$ для всех $0 \leq i \leq NR$, то тогда можно применить доказанный *Факт I* к каждому из отрезков и получить $g^i x \in B_{2\delta}(I_R)$, причем $|B_{2\delta}(I_R)| \leq NR$. Таким образом в множестве с мощностью $\leq NK$ умещается $1+NR$ "середин", а значит по принципу Дирихле (Pigeonhole principle) как минимум две "середины" должны совпадать, что невозможно. Таким образом, некоторое g^i должно выкинуть из $B_{2\delta}(1)$, иными словами для некоторого $p(R) \leq NR$ будет выполнено

$$|g^{p(R)}| > R$$

Также очевидно, что $p(R) > \frac{R}{|g|}$, так как $R < |g^{p(R)}| \leq p(R)|g|$ (без этого условия мы физически не сможем набрать R букв в $p(R)$-степени).

Факт II

Выполнено $\left|g^{NR}\right| \geq R$ *для любого натурального* R.

Идея здесь такая: если для некоторого R_0 выполнено $\left|g^{NR_0}\right| < R_0$, то и $\left|g^{nNR_0}\right| \leq n\left|g^{NR_0}\right| < nR_0$. Если бы в природе все числа делились на NR_0, то поделим $p(R) = nNR_0$ и с учетом $p(R) \leq NR$ получим $\left|g^{p(R)}\right| < nR_0 = \frac{p(R)}{N} \leq R$, что невозможно. Но в реальности не все делится на nR_0, а потому можно просто разделить $p(R)$ на NR_0 с остатком и заметить, что при достаточно больших R достаточно большим будет и $p(R)$, и остатком можно пренебречь. Технически мы это реализуем вот так:

Пусть для некоторого R_0 и некоторого $\varepsilon > 0$ выполнено $\left|g^{NR_0}\right| < R_0 - \varepsilon$. Поделив произвольный натуральный s на NR_0 с остатком $s = nNR_0 + R_1$, где $0 \leq R_1 < NR_0$ мы получим для него:

$$\left|g^s\right| \leq n\left|g^{NR_0}\right| + \left|g^{R_1}\right| < n(R_0 - \varepsilon) + \left|g^{R_1}\right| < nR_0$$

при условии, что $n\varepsilon > \left|g^{R_1}\right|$; так как $\left|g^{R_1}\right| \leq NR_0|g|$, то это условие заведомо выполняется, если $n > \frac{NR_0|g|}{\varepsilon}$, что с учетом $n = \frac{s-R_1}{NR_0} \geq \frac{s}{NR_0} - 1$ заведомо выполняется при $\frac{s}{NR_0} - 1 > \frac{NR_0|g|}{\varepsilon}$, иными словами для достаточно большого s.

Так как $p(R) > \frac{R}{|g|}$, то при достаточно большом R можно сделать $p(R)$ сколь угодно большим, и поделив его с остатком $p(R) = nNR_0 + R_1$ (из этого разложения в частности вытекает, что $\frac{p(R)}{N} \geq nR_0$, также помним, что по построению $p(R) \leq NR$) мы получим:

$$\left|g^{p(R)}\right| < nR_0 \leq \frac{p(R)}{N} \leq R$$

Но при этом по определению $\left|g^{p(R)}\right| > R$, что приводит к противоречию. Значит для произвольного R имеем $\left|g^{NR}\right| \geq R - \varepsilon$, и в силу произвольности ε получаем заявленное $\left|g^{NR}\right| \geq R$.

Таким образом мы доказали:

$$Ca \geq \left|g^{aN}\right| \geq a$$

для любого $a \in \mathbb{N}$, где в роли C можно взять например $C = N|g|$ (здесь непривычно a - переменная, а N - константа); иными словами квазиизометричность на подгруппе $\langle g^N \rangle$. Для перехода к исходной подгруппе можно воспользоваться стандартным для квазиизометричности приемчиком: пусть $n \in \mathbb{N}$, рассмотрим такое a, что $aN \leq n < (a+1)N$, тогда $(n - aN) < N$ и $\left|g^{n-aN}\right| \leq (n - aN)|g| \leq N|g| = C = \text{Const}$, а значит:

$$|g^n| = \left|g^{aN+(n-aN)}\right| \leq \left|g^{aN}\right| + \left|g^{n-aN}\right| \leq Ca + C \leq \frac{C}{N}n + C$$

$$|g^n| = \left|g^{aN+(n-aN)}\right| \geq \left|g^{aN}\right| - \left|g^{n-aN}\right| \geq a - C = (a+1) - (C+1) \geq \frac{1}{N}n - (C+1)$$

Мы получили такую оценку сверху, чтобы она идейно сочеталась с нашим квазиизометрическим подходом к переходу от $\langle g^N \rangle$ к $\langle g \rangle$, хотя она и элементарно выписывается на основании базовых свойств словесной метрики: $|g^n| \leq n|g|$, оценку же снизу так просто получить не получится. И все это окончательно доказывает квазиизометричность вложения уже всей подгруппы $\langle g \rangle < G$.

Утверждение

Пусть G гиперболическая группа, $g \in G$ причем $\text{ord}(g) = \infty$. Тогда

$$|C(g)/\langle g \rangle| < \infty$$

И в этой задаче $C(g)$ уже не граф Кэли, а централизатор элемента; граф же Кэли в этой задаче мы обозначим через $Cay(G)$. Пусть γ - это кривая, заданная формулой:

$$\gamma(t) = g^n$$

где $t \in [n, n+1)$, иными словами кривая скачками перескакивает от степеней g^i к последующим. Нетрудно заметить с учетом предыдущего утверждения, что (пусть $t \in [n, n+1)$ и $s \in [m, m+1)$, в таком случае $|s-t| - 2 \leq |n-m| \leq |s-t| + 2$):

$$d(\gamma(t), \gamma(s)) = |g^{n-m}| \leq A|n-m| + B \leq A|t-s| + (2A + B)$$

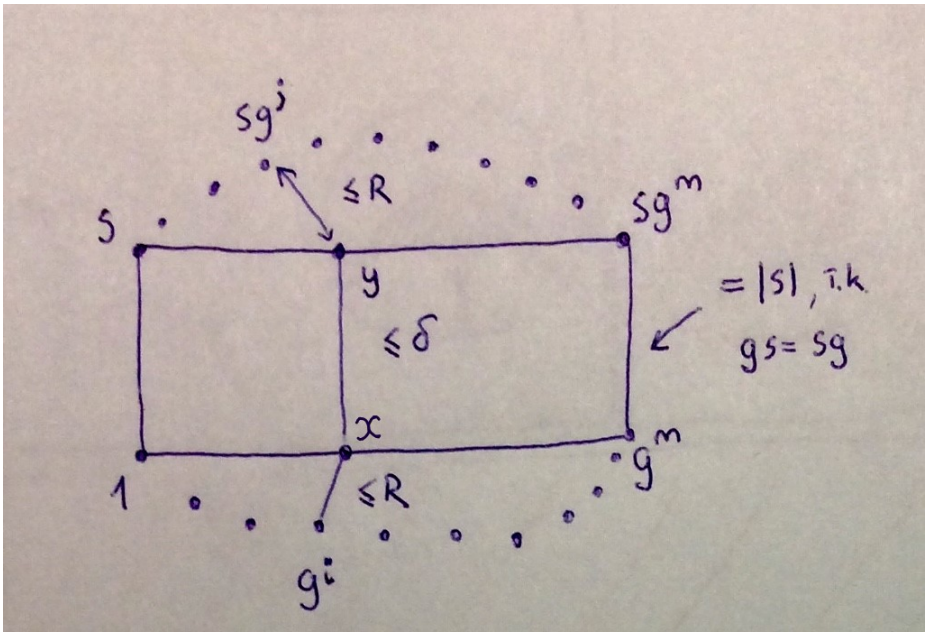
$$d(\gamma(t), \gamma(s)) = |g^{n-m}| \geq \frac{1}{A}|n-m| - B \geq \frac{1}{A}|t-s| - \left(\frac{2}{A} + B\right)$$

Таким образом эта кривая будет (α, C)-квазигеодезической (например для $\alpha = A$ и $C = \max\left\{2A + B, \frac{2}{A} + B\right\}$), а потому для любого n кривая $\gamma_n = \gamma|_{[0,n]}$ тоже будет (α, C)-квазигеодезической (как сегмент (α, C)-квазигеодезической). Тогда по лемме Морса существует некоторое R, что $d_H(\gamma_n, [1, g^n]) \leq R$, а так как фактически $\gamma_n = \{1, g, g^2, \ldots, g^n\}$, то для любого n мы получаем:

$$[1, g^n] \subset B_R(\{1, g, g^2, \ldots, g^n\})$$

Конечно же для каждого n можно найти такую окрестность, но пафос в том, что R не зависит от n из-за того, что у всех этих кривых общий параметр квазигеодезичности, а значит можно примерить лемму Морса.

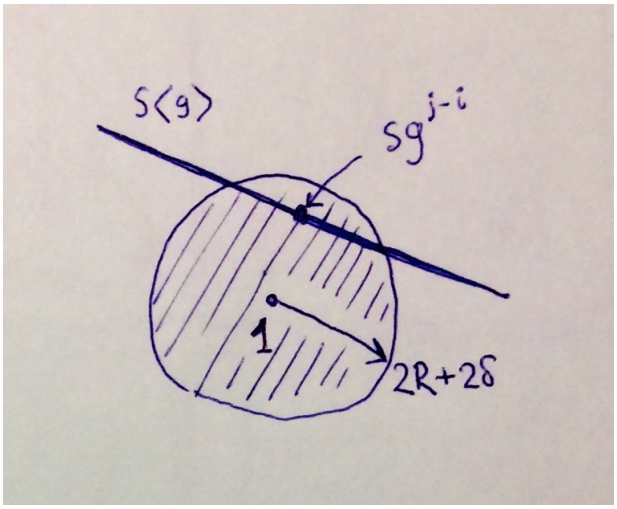
Рассмотрим произвольный элемент централизатора $s \in C(g)$, рассмотрим граф Кэли $Cay(G)$, и условие бесконечного порядка g обеспечит такое m, что $d(1, g^m) > 4\delta + 2|s|$, где δ - это константа тонкости. Рассмотрим в $Cay(G)$ геодезический четырехугольник $[1, g^m, sg^m, s]$, где сторона $[s, sg^m]$ является сдвигом на s стороны $[1, g^m]$:



Рассмотрим середину x отрезка $[1, g^m]$. Мы с вами обсуждали, что условие тонкости обобщается с треугольников на произвольные многоугольники: и каждая сторона n-угольника лежит в $(n-2)\delta$-окрестности остальных сторон, поэтому будет существовать y на оставшихся трех сторонах, что $d(x, y) \leq 2\delta$. Так как $d(1, s) = |s|$ и по условию $d(1, x) > |s|+2\delta$, то y по неравенству треугольника никак не может лежать на $[1, s]$. Условие $s \in C(g)$ обеспечивает, что $d(g^m, sg^m) = |g^{-m}sg^m| = |s|$, а потому из тех же соображений y не может лежать на $[g^m, sg^m]$. Таким образом $y \in [s, sg^m]$. Используя $[1, g^n] \subset B_R(\{1, g, g^2, \ldots, g^n\})$ для любого n мы получаем, что найдется i, что $d(x, g^i) \leq R$. Также, так как сдвиг на s сохраняет попарные расстояния, то $[s, sg^n] \subset B_R(\{s, sg, sg^2, \ldots, sg^n\})$, а значит найдется j, что $d(y, sg^j) \leq R$. Таким образом:

$$|sg^{j-i}| = |g^{-i}sg^j| = d(sg^j, g^i) \leq d(sg^j, y) + d(y, x) + d(x, g^i) \leq 2R + 2\delta$$

На человеческом языке это означает, что в классе $s\langle g\rangle$ всегда найдется элемент в шаре $B_{2R+2\delta}(1)$, а так как элементов этого шара конечное число - то и смежных классов может быть только конечное число (ведь если классы пересекаются, то они обязаны совпадать).



Мы с вами помним, что с сохранением гиперболичности при переходе к подгруппе есть большие проблемы, и только сейчас после продолжительных подготовительных мучений с доказательством леммы Морса и квазигеодезичности $\langle g \rangle$ мы готовы доказать следующее важное структурное свойство гиперболических групп:

Следствие
Пусть $\mathbb{Z}^2 < G$, тогда G не является гиперболической.

Пусть G является гиперболической и пусть a, b являются порождающими $\mathbb{Z}^2$. Тогда $\langle b \rangle < C(a)$, и $b^j\langle a \rangle$ являются различными смежными классами, что противоречит предыдущему утверждению, о том, что их должно быть лишь конечное число.

Идейно близким к этому следствию является следующее утверждение:

Утверждение
Пусть $B(2,3) < G$, где $B(2,3) = \langle a, b | b^{-1}a^2b = a^3 \rangle$ наша любимая группа Баумслага-Солитера. Тогда G не является гиперболической.

Из соотношения $b^{-1}a^2b = a^3$ по индукции легко выводится соотношение $b^{-n}a^{2^n}b^n = b^{3^n}$, потому что:

$$b^{-1}(b^{-n}a^{2^{n+1}}b^n)b = b^{-1}((b^{-n}a^{2^n}b^n)(b^{-n}a^{2^n}b^n)b = b^{-1}a^{3^n}a^{3^n}b = b^{-1}\left((a^2)^{3^n}\right)b = (a^3)^{3^n} = a^{3^{n+1}}$$

Пусть G является гиперболической, по доказанному ранее утверждению $\langle a \rangle$ является квазигеодезической, а значит для некоторых констант $A, B > 0$ выполнено:

$$\frac{n}{A} - B \leq |a^n| \leq An + B$$

Таким образом мы получим, что:

$$\frac{3^n}{A} - B \leq \left|a^{3^n}\right| = \left|b^{-n}a^{2^n}b^n\right| \leq |b^{-n}| + \left|a^{2^n}\right| + |b^n| \leq 2n|b| + 2^nA + B$$

Но функция слева имеет скорость роста как у 3^n, в то время как функция справа растет как 2^n, что приводит к противоречию.

Замечание:

На самом деле последние два утверждения являются частным случаем одного более общего утверждения, что гиперболическая группа не может содержать в качестве подгруппы любые группы Баумслага-Солитера $B(n,m) = \langle a, b | b^{-1}a^n b = a^m \rangle$ *(отмечу, что* $B(1,1) \cong \mathbb{Z}^2$*), что я оставлю вам в качестве упражнения, дав подсказку, что для его решения для произвольных* n *и* m *хватит двух идей, которыми мы воспользовались в последних двух примерах: оценки на словесные длины для высокостепенных следствий из определяющего соотношения, а также оценки индекса централизатора. Будем говорить, что группа обладает BS-свойством, если в нее нельзя вложить никакую группу Баумслага-Солитера* $B(n,m)$*. В этих терминах сказанное выше означает, что гиперболичность* $\Rightarrow$ *BS-свойство.*

Вопрос, является ли отсутствие BS-свойства единственным препятствием к гиперболичности для конечно-определенных групп (иными словами верно ли, что BS-свойство $\Rightarrow$ *гиперболичность), в общем случае довольно многогранный (осмысленно его задавать для конечно-определенных групп, так как в противном случае группа не является гиперболической автоматически). В общем случае ответ отрицательный, так как можно рассмотреть тот упомянутый нами очень сложный пример конечно-определенной негиперболической подгруппы* $H < G$ *гиперболической группы* G *(построение этой группы читатель сможет найти в статье Noel Brady, "Branched coverings of cubical complexes and subgroups of hyperbolic groups"). Группа* H *не является гиперболической, но при этом* $B(n,m) < H$ *невозможно, так как в таком случае* $B(n,m) < H < G$ *группа Баумслага-Солитера содержалась бы и в гиперболической группе* G*. Таким образом мы построили негиперболическую конечно-определенную группу* H *с BS-свойством. Однако по сей день открытыми остаются два вопроса про более специальные случаи:*

- *Пусть* $G = \langle a_1, \ldots, a_n | r = 1 \rangle$ *- группа с одним соотношением. Верно ли, что если* G *обладает BS-свойством, то* G *является гиперболической?*
- *Пусть* G *является конечно-определенной, и все ее рациональный гомологии* $H_k(G, \mathbb{Q})$ *конечномерны, а также равны нулю при достаточно больших* k*. Верно ли, что если* G *обладает BS-свойством, то* G *является гиперболической?*

И то, что математики до сих пор не смогли ответить на эти вопросы, хорошо говорит о том, что хотя вложимость группы Баумслага-Солитера является и не единственным препятствием к гиперболичности, но все же очень важным и принципиальным: то есть для очень широкого класса групп их негиперболичность проверяется отсутствием $B(n,m)$ *в качестве подгруппы, а примеры, где этого не хватает, очень специфические и сложные; это нужно себе концептуально мыслить как утверждение из прошлой главы, что если в группу вкладывается* $\mathbb{F}_2$*, то она неаменабельна; иными словами это можно неформально сформулировать так: для* $99,9\%$ *конечно-определенных групп, которые вы встретите в жизни, их гиперболичность эквивалентна BS-свойству.*

Следующий сюжет невозможно обойти стороной, рассказывая о гиперболических группах. Частично его мы касались, когда обсуждали аменабельные группы и на $\mathbb{Z}$ построили две различные инвариантные меры, каждая из которых отвечала за поведение группы на бесконечности со своей стороны (слева или справа). Оказывается, этот хитрый прием можно развить до красивой и очень содержательной теории, где каждое такое "бесконечное направление" является точкой некоторого вполне конкретного компактного пространства, называемого *границей Громова* (понятие границы Громова определяется и осмысленно исключительно для гиперболических групп, в других разделах теории групп встречаются другие границы, в общем случае имеющие с границей Громова почти ничего общего кроме общей идеологии изучения поведения группы "на бесконечности"). Тема довольно сложная, а потому мы приводим ее лишь для поверхностного ознакомления, и много технических деталей будет обходиться стороной. Итак, определение:

Определение

Пусть $G = \langle A|R\rangle$ является гиперболической группой, рассмотрим на ней заданную копредставлением словесную метрику. Определим ее границу ∂G как пространство

$$\partial G = \{(x_n) : \quad x_n \in G \quad и \quad x_n \to \infty\}/_\sim$$

где $x_n \to \infty$ непривычным образом определяется как $\lim\limits_{n,m\to\infty}(x_n, x_m)_\omega = \infty$, здесь $\lim\limits_{n,m\to\infty}$ обычный двойной предел, $(x_n, x_m)_\omega$ произведение Громова, и ω произвольная точка. Отношение эквивалентности определяется так:

$$(x_n) \sim (y_n) \qquad \Longleftrightarrow \qquad \lim_{n\to\infty}(x_n, y_n)_\omega = \infty$$

Топология же на множестве классов эквивалентностей задается базой окрестностей, параметризованных $r \geq 0$ и $p \in \partial G$:

$$U(p, r) = \{q \in \partial G : \text{существуют представители } p = [(x_n)], q = [(y_n)] \text{ что } \liminf_{n,m\to\infty}(x_n, y_m)_\omega \geq r\}$$

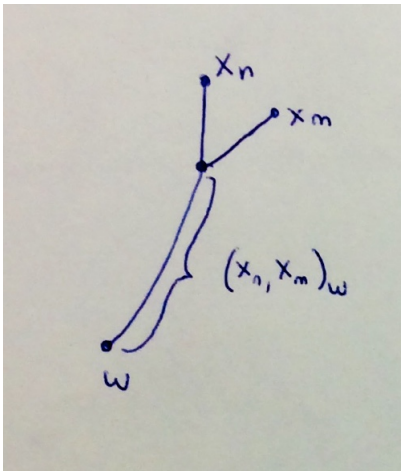
Сразу отмечу, что групповая структура здесь совершенно не нужна - и такое определение можно дать для произвольных метрических пространств, в которых выполняется условие Громова

$$(x,z)_\omega \geq \min\{(x,y)_\omega,(y,z)_\omega\} - \delta$$

для произвольных x,y,z,ω. Напомню, что это условие эквивалентно гиперболичности для геодезических пространств. Хотя в нашем случае пространство G не является гиперболическим, но это не является проблемой, так как $G \subset C_A(G)$, и так как $C_A(G)$ геодезическое, то в нем выполнено условие Громова, а значит оно выполнено и для любого подмножества, в частности и для G. Без условия Громова определение границы будет некорректным: в общем случае это отношение не обязано быть отношением эквивалентности, так как оно может быть нетранзитивным; однако в случае пространств с условием Громова при $(x_n) \sim (y_n)$ и $(y_n) \sim (z_n)$ мы имеем:

$$(x_n,z_n)_\omega \geq \min\{(x_n,y_n)_\omega,(y_n,z_n)_\omega\} - \delta \to \infty$$

а значит и $(x_n) \sim (z_n)$. Требование $\lim\limits_{n,m\to\infty}(x_n,x_m)_\omega = \infty$ в определении $x_n \to \infty$ нужно для того, чтобы (x_n) стремилось к бесконечности не хаотично, а "вдоль некоторого направления". Для того чтобы это понять - полезно поразмышлять о примере деревьев, где, как мы помним, геометрический смысл $(x_n,x_m)_\omega$ был как следующее расстояние в трезубце:



А потому, чем это расстояние больше, тем больше кажется, что (x_n) и (x_m) "идут" в одном направлении. С учетом этого комментария можно на человеческом языке объяснить структуру базы окрестностей топологии: так как в некотором смысле выражение $(x_n,y_m)_\omega \geq r$ означает, что у идущих в бесконечность по своим путям (x_n) и (y_m) общие первые r шагов пути, иными словами долгое время они идут вместе и после некоторого момента начинают расходиться. А всякие $\liminf$ нужны, чтобы определить топологию аккуратно, не говоря уже о том, что описанное выше словесное описание работает только для деревьев. Также отмечу, что само определение $x_n \to \infty$ (а также все фигурирующие по ходу дела понятия) не зависят от ω, так как если взять другой ω', то

$$|(x_n,x_m)_\omega - (x_n,x_m)_{\omega'}| \leq d(\omega,\omega')$$

что легко выводится из общей формулы для $(x,y)_z$. Таким образом раз эти выражение отличаются не более чем на фиксированную конечную величину, то

$$\lim_{n,m\to\infty}(x_n,x_m)_\omega=\infty \quad \Longleftrightarrow \quad \lim_{n,m\to\infty}(x_n,x_m)_{\omega'}=\infty$$

Для остальных номинально зависящих от ω встречающихся здесь понятий можно провести такие же рассуждения. Также отмечу, что если $x_n\to\infty$, то (x_n) стремится к бесконечности в классическом смысле, так как если предположить, что для некоторой подпоследовательности n_k и некоторого ω выражение $d(x_{n_k},\omega)$ будет ограниченным, то

$$d(x_{n_k},\omega)=\frac{1}{2}\left(d(x_{n_k},\omega)+d(x_{n_k},\omega)-d(x_{n_k},x_{n_k})\right)=(x_{n_k},x_{n_k})_\omega\to\infty$$

и приходим к противоречию.

На границе группы определено очень полезное и естественное действие:

$$G\curvearrowright\partial G$$

заданное формулой $g\cdot[(x_n)]=[(gx_n)]$. Границу группы иногда можно определять более сложным но и в то же время более геометрическим подходом: заменяя уходящие на бесконечности последовательности уходящими на бесконечность геодезическими путями в $C_A(G)$. Непрерывная и наша дискретная граница получаются гомеоморфными. Также отмечу, что есть идейно близкая к понятию границы и более простая структура, хотя в то же время и более бедная, называемая *количеством концов группы*. Для конечно-порожденной группы количество концов определяется как наименьшее n, что результат любого выкидывания из $C_A(G)$ конечного числа ребер будет иметь не больше n бесконечных компонент связности, иными словами:

$$e(G)=\sup_{\substack{F\subset C_A(G)\\ F\text{ - конечное}}}N(C_A(G)\backslash F)$$

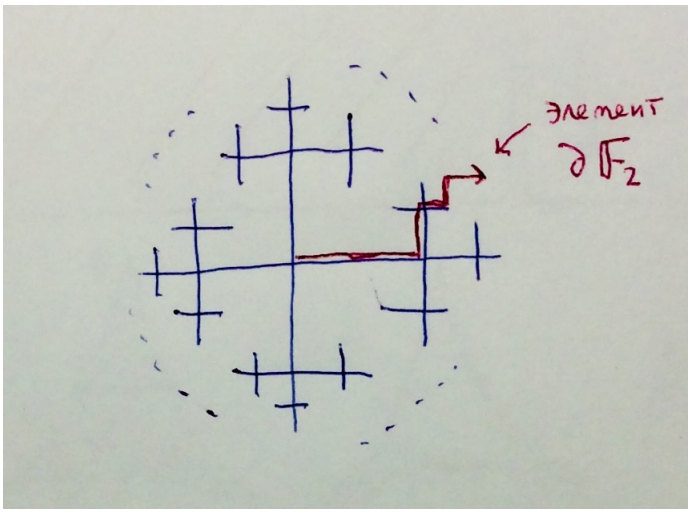
где $N(X)$ - число бесконечных компонент связности X. Увы, топологию здесь ввести нельзя и мы должны довольствоваться просто числом. Замечу, что для данного определения гиперболическая структура не нужна, множество концов обозначается через $e(G)$. К примеру $e(G)=0$ для конечных групп, так как там не может быть бесконечных компонент связности. $e(\mathbb{Z})=2$, так как граф Кэли - это $\mathbb{R}$, сколько бы из него конечных отрезков не выкинуть - всегда будет лишь две бесконечные компоненты связности, каждая из которых уходит в свою бесконечность. $e(\mathbb{Z}^2)=1$, так как ее граф Кэли - это сетка, выкидывая из которой конечное число ребер нельзя нарушить ее связности. При этом $e(\mathbb{F}_2)=\infty$, так как выкидывая конечное число ребер в ее графе Кэли в нужном месте можно сделать сколь угодно много бесконечных компонент связности. На самом деле есть теорема, что для конечно-порожденных групп $e(G)\in\{0,1,2,\infty\}$. Итак, вернемся к границам.

Примеры

• $\partial\mathbb{D} = S^1$, где $\mathbb{D}$ круговая модель плоскости Лобачевского. Для обычного евклидова круга наша граница не определена, так как она определяется только для гиперболических пространств. Точки граничной окружности иногда называют *точками абсолюта.*

• Верен и более общий результат, что: $\partial\mathbb{H}^n = S^{n-1}$ где $\mathbb{H}^n$ стандартное n-мерное гиперболическое пространство, являющееся многомерным обобщением плоскости Лобачевского.

• $\partial\mathbb{F}_2 = K$, где K - канторово множество. Графом Кэли свободной группы является дерево, описывать границу здесь проще через геодезические потоки. Элементом границы является уходящая на бесконечность геодезическая, которую мы будем отождествлять с последовательностью элементов группы, через которые она проходит:



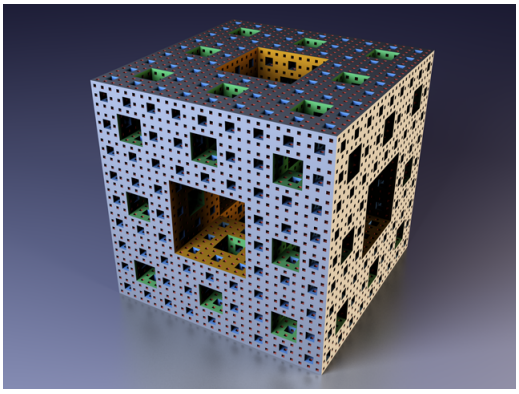
Факторизовать по отношению эквивалентности не нужно, так как в каждом классе эквивалентности содержится только один путь: потому что если $[(x_n)] = [(y_n)]$ - то $\lim(x_n, y_n)_e = \infty$; иными словами у путей (x_n) и (y_n) одинаковый сколь угодно долгий начальный промежуток пути, но это означает, что они совпадают полностью (если считать запрещенным движения по пути назад: если границу определять через геодезические потоки - то это очевидно, если через последовательности - то нужно аккуратно с этим поработать: небольшие откаты назад не играют роли и их можно выкинуть, а большие невозможны). Таким образом:

$$\partial\mathbb{F}_2 \cong \{0,1,2,3\} \times \{0,1,2\}^{\mathbb{N}}$$

что означает, что на первом шаге у нас есть 4 возможные направления, а на каждом последующем всегда есть 3 варианта (возвращаться назад нельзя). Что касается топологии, то раз мы имеем дело с деревом, то базой окрестностей являются параметризованные $r \in \mathbb{N}$ и $(y_n) \in \mathbb{F}_2$ множества, состоящие из всевозможных (x_n), таких, что (x_n) и (y_n) имеют общее начало пути длины r. На уровне последовательностей это означает, что некоторый набор первых координат задается, а остальные - произвольные, что в точности совпадает с базой топологии произведения Тихонова. В случае топологии Тихонова упомянутое выше произведение гомеоморфно множеству Кантора. Также ясно, что $\partial\mathbb{F}_n = K$ при $n \geq 2$, так как принципиально в этих рассуждениях ничего не поменяется. Отмечу,

что $\partial\mathbb{Z} = \{1, -1\}$ - в дословной терминологии этих рассуждений на первом шаге у нас есть 2 варианта движений, а на каждом последующем альтернативы уже нет. Эти две точки соответствуют путям, уходящим в группе вправо и влево на бесконечность.

• Однако, канторово множество в роли границы - это скорее исключение, типичное лишь для групп, чей граф Кэли уж очень похож на деревья. Обычно $\partial G = M$ для в некотором роде типичной гиперболической группы G, где M - это кривая Менгера, которая по аналогии с канторовым множеством строится с помощью деления на 27 одинаковых частей трехмерного куба и последовательного выбрасывания центрального кубика, а также шести к нему примыкающих:



Несмотря на обманчивую трехмерность, формально она является одномерной и имеет массу красивых и важных для топологии в целом свойств. В контексте кривой Менгера показательно следующее утверждение:

Утверждение

Пусть $G = \langle a, b | \ldots \rangle$ порожденная двумя элементами группа со свойством $C'\left(\frac{1}{6}\right)$ (а значит гиперболическая), с конечной абеленизацией G_{ab} и одним концом $e(G) = 1$. Тогда $\partial G = M$.

• Также нужно сказать, что квазиизоморфизм $f : G \underset{q.i.}{\sim} H$ индуцирует гомеоморфизм $f_* : \partial G \to \partial H$, заданный формулой $f_*[(x_n)] = [f(x_n)]$. К примеру, из этого утверждения вытекает, что $\mathbb{H}^n$ и $\mathbb{H}^m$ не являются квазиизометричными при $n \neq m$. Также, если мы знаем границу какой-то гиперболической группы - мы автоматически знаем границы всех квазиизометричных ей групп. К примеру для любой конечной группы G верно $\mathbb{F}_2 \underset{q.i.}{\sim} \mathbb{F}_2 \times G$, причем квазиизометрия задается формулой $\omega \mapsto (\omega, 1)$, а значит $\partial(\mathbb{F}_2 \times G) = K$. Или другой пример: так как $\mathbb{Z} \underset{q.i.}{\sim} D_\infty$, то $\partial D_\infty = \{1, -1\}$.

Что касается свойств упомянутого выше естественного действия гиперболической группы на своей границе, сформулируем без доказательства следующую теорему:

Теорема

Пусть G - гиперболическая группа, $g \in G$ причем $\mathrm{ord}(g) = \infty$. Тогда при $G \curvearrowright \partial G$ у элемента g только две неподвижные точки g_+ и g_- на ∂G, где при секвенциальном подходе к определению границы $g_+ = \{e, g, g^2, g^3, \ldots\}$ и $g_- = \{e, g^{-1}, g^{-2}, g^{-3}, \ldots\}$. Причем g_+ является точкой притяжения, а g_- точкой отталкивания.

Следующее утверждение очень структурно важное, но мы опишем доказательство лишь на идейном уровне:

Теорема

Пусть G - гиперболическая группа без кручения и $g, h \in G$ некоммутирующие элементы. Тогда существует N, что для любых $n, m \geq N$ выполнено

$$\langle g^n, h^m \rangle \cong \mathbb{F}_2$$

Иными словам внутри гиперболических групп типично, что сидит много свободных групп. В частности из этого утверждения вытекает, что если G группа без кручения, и она является одновременно и гиперболической и аменабельной, то $G \cong \mathbb{Z}$. Возьмем произвольный нетривиальный $u \in G$, и пусть вне $\langle u \rangle$ найдется некоторый элемент v. Если $[u, v] = 1$, то $\langle u, v \rangle \cong \mathbb{Z}^2 < G$, что невозможно в гиперболической группе. Ежели $[u, v] \neq 1$, то $\langle u^N, v^N \rangle \cong \mathbb{F}_2 < G$ для некоторого N, что невозможно в аменабельной группе. Таким образом $G = \langle u \rangle \cong \mathbb{Z}$.

Идея доказательства этой теоремы состоит в том, чтобы рассмотреть каноническое действие $G \curvearrowright \partial G$. Известно, что если $[g, h] \neq 1$, то все четыре точки g_+, g_-, h_+, h_- различны. Рассмотрим некоторые их непересекающиеся окрестности соответственно U_+, U_-, V_+, V_-. Тогда из определения точек притяжения и отталкивания будет вытекать, что существует N, что для любых $n, m \geq N$ будет выполнено

$$g^n(\partial G \backslash U_-) \subset U_+ \qquad g^{-n}(\partial G \backslash U_+) \subset U_-$$
$$h^m(\partial G \backslash V_-) \subset V_+ \qquad h^{-m}(\partial G \backslash V_+) \subset V_-$$

А значит для $U = U_+ \cup U_-$ и $V = V_+ \cup V_-$ выполнено условие леммы о пинг-понге, и таким образом $\langle g^n, h^m \rangle \cong \mathbb{F}_2$.

Замечание:

На самом деле верен более сильный факт, что в произвольной гиперболической группе G (не обязательно с отсутствующим кручением) и для произвольных ее элементов $g_1, \ldots, g_n \in G$ для некоторого N верно $\langle g_1^N, \ldots, g_n^N \rangle \cong \mathbb{F}_r$, где $r \leq n$. Ясно, что ранг свободной группы может быть меньше n, так как к примеру некоторые g_i могут совпадать. Также, если все элементы g_i будут иметь конечный порядок, то $r = 0$ и N обязана делиться на порядок каждого элемента. Также отмечу, что в самой сильной формулировке лишь найдется степень N, что такая подгруппа будет свободной, и она не обязана быть свободной для всех степеней начиная с некоторого номера, как в нашей теореме. Объяснить это тоже очень просто - опять же если некоторый g_i имеет кручение, то N обязана делиться на порядок этого g_i, иначе в группе $\langle g_1^N, \ldots, g_n^N \rangle$ появится кручение - и она не сможет быть свободной. Из этой теоремы вытекает альтернатива Титса для гиперболических групп: а именно любая гиперболическая группа оказывается либо почти разрешимой (т.е. содержащей разрешимую подгруппу конечного индекса), либо содержит в качестве подгруппы $\mathbb{F}_2$. Альтернатива Титса - довольно популярное в теории групп понятие, впервые возникшее в работе Титса, где он доказал, что конечно-порожденная линейная над полем группа либо почти разрешима, либо содержит $\mathbb{F}_2$. После этой работы альтернативой Титса стали называть выполнение одного из этих двух условий. Однако не все группы удовлетворяют альтернативе Титса, к примеру она не выполняется для группы Григорчука, которую мы упоминали, когда обсуждали аменабельные группы в контексте необычности ее функции роста.

==========

Задачи для самостоятельной работы

- *Является ли группа $G = \langle a, b, c, d | abcdbadc = 1\rangle$ гиперболической?*
- *Описать алгоритм разрешения проблемы равенства слов в группе с копредставлением $\mathbb{Z}^2 = \langle a, b | [a, b] = 1\rangle$.*
- *Пусть $\mathbb{Z} \hookrightarrow \mathbb{Z}^2$, где порождающий $1 \mapsto x$ и $x \neq 0$. Считая что метрики на группах стандартные, выяснить, при каких x такой гомоморфизм будет квазиизометрическим вложением, и при каких x образ $\mathbb{Z}$ при гомоморфизме будет квазивыпуклым. В частности из ответа на эту задачу можно сделать вывод, что в $\mathbb{Z}^2$ понятия квазивыпуклости и квазиизометричности для подгрупп неэквивалентны.*
- *При $n \geq 3$ является ли группа $SL_n(\mathbb{Z})$ гиперболической? Является ли группа $SL_2(\mathbb{Z})$ гиперболической?*
- *Пусть $G = \langle x, y : [x, y]^2 = 1\rangle$. Докажите, что $[x^{1000}, y^{1000}]^{1000} \neq 1$ в группе G.*
- *Пусть $G_1 \times G_2$ гиперболическая. Доказать, что одна из этих двух групп G_i является гиперболической, а вторая - конечной.*
- *Квазиизометричны ли пространства $A = \{1, 2, 3, 4, \ldots\}$ и $B = \{1^2, 2^2, 3^2, 4^2, \ldots\}$ с индуцированными из $\mathbb{R}$ метриками?*
- *Пусть G гиперболическая группа. Доказать, что для всех отличных от нуля n, m группа Баумслага-Солитера $B(n, m)$ не может быть вложена в G.*
- *Вычислить функцию Дэна $D(n)$ для $B(1, 2) = \langle a, b | b^{-1}ab = a^2\rangle$.*
- *Вычислить минимальное значение для константы гиперболичности δ для плоскости Лобачевского в дисковой модели, где плоскость - это внутренность единичного круга, а прямые - окружности, перпендикулярные границе этого круга.*

Остаточно конечные группы

Так сложилось, что в русской литературе нет единодушия насчет того, как называть эти группы: и *остаточно конечные группы* также называют *финитно аппроксимируемыми* или даже *аппроксимативно конечными*, и на этой почве иногда разгораются ожесточенные споры. Мне же терминология "остаточно конечных" кажется более естественной и правильной: так как во-первых это более дословный перевод их английской версии residually finite, и там в отношении с этими группами жесткая определенность с терминологией, во-вторых все аппроксимации обычно ассоциируются с приближением относительно некоторой метрики, но аппроксимация здесь в том понятии, в котором она есть, ни с какой метрикой не связана; более того, понятие остаточной конечности основывается на поведении факторов группы, которые в некотором смысле можно воспринимать как деление групп. И понятие "остаток" легче внедряется в ассоциативную последовательность "деление", "частное" и т.д., чем слово аппроксимация. Ну и в-третьих, и это самое главное, что это понятие не оторвано от общей математической канвы, и аналогичные понятия есть и в других алгебраических структурах. К примеру в C^*-алгебрах есть два принципиально различающихся класса алгебр, в некотором смысле приближаемых конечномерными алгебрами: это *residually finite-dimensional C^*-algebras* (определение в точности повторяет определение остаточно конечных групп, переведенное на язык алгебр) и *approximately finite-dimensional C^*-algebras*: и если residualy finite-dimensional переводить как аппроксимативно конечномерные, то я даже боюсь подумать о том, как же тогда переводить approximately finite-dimensional. Нужно понимать, что это некий частный случай общей категорной конструкции, где всегда "аппроксимация" - это инъективное вложение чего-то, а "остаточность" - это эпиморфное отображение на что-то. И идеологически более правильным, как мне кажется, аппроксимативно конечными называть либо группы, представимые в виде возрастающего счетного объединения конечных групп, либо даже LEF-группы А.М. Вершика (locally embedded into the class of finite groups): то есть что-то более идейно близкое к аменабельности, но это лишь мои мысли вслух и только лишь моя точка зрения.

Определение

Группа G называется остаточно конечной, если для любого $g \in G$, что $g \neq 1$, существует гомоморфизм $\pi : G \to F$ в конечную группу, что $\pi(g) \neq 1$

Иными словами гомоморфизмы в конечные группы разделяют элементы (ясно, что если $g \neq h$, то если определение применить для gh^{-1}, то получим гомоморфизм π, что $\pi(g) \neq \pi(h)$). В зависимости от задачи иногда удобно работать с некоторыми эквивалентными (даже тавтологическими) переформулировками данного определения, самые важные из которых мы отразим в следующем утверждении:

Утверждение

Следующие условия эквивалентны:

- *Группа G является остаточно конечной.*
- *Для любого $g \in G$, что $g \neq 1$, существует нормальная подгруппа конечного индекса $N \lhd G$, что $g \notin N$ (или что то же самое $\pi(g) \neq 1$, где $\pi : G \to G/N$ канонический эпиморфизм).*
- *Существуют конечные группы F_λ, где $\lambda \in \Lambda$, что $G \hookrightarrow \prod\limits_{\lambda \in \Lambda} F_\lambda$.*

Первые два условия эквивалентны из-за естественного соответствия $\pi \leftrightarrow \operatorname{Ker}\pi$ между гомоморфизмами в конечные группы и нормальными подгруппами конечного индекса: и для фиксированного $g \neq 1$ если π из первого пункта, то $\operatorname{Ker}\pi$ подходит во втором пункте, и если N из второго пункта, то гомоморфизм $G \to G/N$ подходит для первого пункта.

Для (1) $\Rightarrow$ (3) рассмотрим для каждого нетривиального g отделяющий его от тривиального элемента гомоморфизм $\pi_g : G \to F_g$ в некоторую конечную группу. Тогда рассмотрим

$$\pi : G \to \prod_{g \in G} F_g$$

действующий по формуле $\pi(h) = (\pi_g(h))_{g \in G}$. Ясно, что этот гомоморфизм инъективный, так как образ нетривиального g как минимум в g-ой координате будет нетривиальным. Отсюда в частности вытекает, что в случае счетных G достаточно ограничиться счетными произведениями. Что касается (3) $\Rightarrow$ (1), то если у нас есть инъективный гомоморфизм $\pi : G \to \prod\limits_{\lambda \in \Lambda} F_\lambda$, то для любого нетривиального $g \in G$ будет выполнено $\pi(g) \neq 1$, а значит будет нетривиальной как минимум одна координата λ, таким образом гомоморфизм $\pi_\lambda : G \to F_\lambda$ будет искомым. Также остаточную конечность G можно еще эквивалентно почти тавтологически переформулировать как

$$\bigcap_{\substack{[G:N] < \infty \\ N \lhd G}} N = \{1\}$$

Замечания:

Кстати, хочу отметить, что из остаточной конечности вытекает, что для любого конечного множества элементов $M \subset G$ можно построить гомоморфизм $\pi : G \to F$ в конечную группу, что $\pi(m) \neq \pi(n)$ для любых $m \neq n$, где $n, m \in M$, иными словами построить гомоморфизм в конечную группу, инъективный на любом наперед заданном конечном множестве. Для этого достаточно применить определение ко всем нетривиальным элементам вида mn^{-1}, где $m, n \in M$, затем построить для них отделяющий этот элемент от 1 гомоморфизм в конечную группу $\pi_{(m,n)} : G \to F_{(m,n)}$, а заметим взять прямую сумму этих гомоморфизмов $\pi = \oplus\pi_{(m,n)} : G \to \oplus F_{(m,n)}$.

*В теории групп кроме остаточно конечных групп рассматривают также и остаточно *** группы, где вместо *** вы можете подставить ваш самый любимый класс групп. Следующее место по популярности после остаточно конечных делят: остаточно p-группы, остаточно свободные группы, остаточно разрешимые группы и остаточно аменабельные группы, хотя и другие версии остаточности тоже рассматриваются. Многие теоремы на другие версии остаточности переносятся дословно, некоторые с небольшими модификациями - нужно смотреть насколько в доказательстве существенно использовалась конечность. К примеру если в только что доказанной эквивалентности заменить конечные группы на любой другой класс - то ничего не поменяется, и фактически можно утверждать, что группа является остаточно свободной $\Leftrightarrow$ когда она вкладывается в произведение свободных групп; но не всегда все так просто, к примеру, возникнут трудности с переносом замечания про отделимость гомоморфизмами любого конечного множества на случай остаточно свободных*

групп - так как прямое произведение свободных групп свободной не является и даже в свободную не вкладывается. Некоторые классы остаточности рассматривать бессмысленно: к примеру нетрудно заметить, что по только что доказанной теореме остаточно абелевы группы вкладываются в произведение абелевых, иными словами сами являются абелевыми, теряя тем самым содержательность, потому что осмысленно рассматривать группы, которые вкладываются в произведение чего-то хорошего, но при этом сами этим хорошим не являются. Также отмечу, что в некоторых случаях остаточности могут всплывать утверждения, исключительные именно для их класса и непереносимые на другие классы остаточности: например верно утверждение, что:

Группа G является остаточно разрешимой $\Leftrightarrow \bigcap\limits_n G^{(n)} = \{1\}$.

Для $\Rightarrow$ заметим, что если вдруг найдется нетривиальный $g \in G^{(n)}$ для любого n, то из остаточной разрешимости G строим гомоморфизм $\pi : G \to K$ в разрешимую K, что $\pi(g) \neq 1$. Пусть n это ступень разрешимости K, тогда имеем:

$$\pi(G^{(n)}) < K^{(n)} = \{1\}$$

то есть $\pi(g) = 1$, и приходим к противоречию.

Для $\Leftarrow$ заметим, что раз $\bigcap\limits_n G^{(n)} = \{1\}$, то для $g \neq 1$ найдется n, что $g \notin G^{(n)}$. Таким образом $\pi(g) \neq 1$ для $\pi : G \to G/G^{(n)}$, причем группа $G/G^{(n)}$ является разрешимой, так как $\left(G/G^{(n)}\right)^{(n)} = \{1\}$, что в свою очередь вытекает из почти тавтологического факта, что $\pi(G^{(m)}) = (\pi(G))^{(m)}$ для любого m и для любого гомоморфизма π (в частности и для нашего).

Простейшие примеры и основные свойства

• Очевидно, что любая конечная группа G является остаточно конечной (также как и то, что группа из класса *** является остаточно ***).

• Группа $\mathbb{Z}$ является остаточно конечной, так как в аддитивной записи любой ненулевой $m \in \mathbb{Z}$ не делится на какое-то число n, а потому его образ при гомоморфизме $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ будет ненулевым.

• Пусть G, H являются остаточно конечными - тогда и $G \times H$ является остаточно конечной. Действительно, если взять нетривиальный $(g, h) \in G \times H$, то хотя бы одна из его координат будет нетривиальной (пусть это будет g), так как G остаточно конечная - то рассмотрим гомоморфизм $\pi : G \to F$ в конечную группу, что $\pi(g) \neq 1$, тогда ясно, что гомоморфизм $\pi \times 1 : G \times H \to F$, $(\pi \times 1)(g, h) = \pi(g)$ является отделяющим (g, h) от единицы гомоморфизмом.

• Также очевидно, что если G - остаточно конечная и $H < G$, то остаточно конечной является и H: возможно, здесь проще воспользоваться третьим пунктом теоремы о том, что остаточная конечность эквивалентна возможности вложения группы в произведение конечных: ясно, что это свойство переносится на произвольные подгруппы. Также верно следующее утверждение:

Утверждение

Пусть G, H остаточно конечны, тогда $G * H$ тоже остаточно конечна.

Сначала заметим, что достаточно рассматривать лишь случай конечных G и H. Действительно, в общем случае остаточно конечных G, H рассмотрим нетривиальный элемент $\omega = g_1 h_1 \dots g_n h_n$ представленный в виде *несократимого* слова (здесь не важно с какой буквы начинается и на какую заканчивается слово, а потому будем считать, что оно имеет такой вид). Мы уже обсуждали, что в остаточно конечных группах гомоморфизмы в конечные группы могут разделять не только единичные элементы, но и целые конечные множества, а потому рассмотрим такие подгруппы конечного индекса $A \lhd G$ и $B \lhd H$, что все $g_i \notin A$ и все $h_i \notin B$. Тогда ясно, что при естественном гомоморфизме $G * H \to (G/A) * (G/B)$ слово ω перейдет в несократимое, а потому нетривиальное (потому что каждая буква будет нетривиальным элементом и сокращений не может быть, так как в слове стыкуются буквы из разных групп). Но при этом группы G/A и H/B будут конечными, а потому если научимся строить разделяющие гомоморфизмы для их свободных произведений, то научимся и для свободных произведений остаточно конечных групп.

Итак пусть G, H конечные группы. Рассмотрим

$$\Omega_m = \{ \text{ множество несократимых слов } G * H \text{ длины } \leq m\}$$

Так как группы G и H конечны, то множество Ω_m является конечным для любого m. А дальше можно рассмотреть действие $G \curvearrowright \Omega_m$, заданное формулой:

$$g \cdot \omega = \begin{cases} g\omega, & \text{если } |g\omega| \leq m \\ \omega, & \text{иначе} \end{cases}$$

где $|\omega|$ это длина слова ω после приведения его к несократимому виду. Для проверки, что это действие, фактически нужно убедиться только в $(ab)\omega = a(b\omega)$ в ситуации, когда мы можем попасть в условие "иначе" (в противном случае все действует как левое умножение, что является действием). Но это практически очевидно: если мы находимся в пограничном случае $|\omega| = m$, то если ω начинается с буквы из G - то это обычное левое умножение, если с буквы из H, то как левая так и правая часть равенства $(ab)\omega = a(b\omega)$ будут равны ω, так как и в левой и правой части словá умножениями не могут быть изменены, так как при любом варианте умножения на нетривиальную букву получается слово длины $m+1$ (либо длины m в вырожденном случае умножения на 1, к примеру в случае умножения на ab, когда $a = b^{-1}$, но умножение на единицу тоже слово не меняет). Так как действие - это фактически гомоморфизм в $S(\Omega_m)$, то мы получаем гомоморфизм $G \to S(\Omega_m)$. Точно такой же формулой задается действие $H \curvearrowright \Omega_m$, а значит и гомоморфизм $H \to S(\Omega_m)$. Из свойства универсальности мы получаем гомоморфизм:

$$\gamma : G * H \to S(\Omega_m)$$

И по построению ясно, что если $|\omega| = m$, то $\gamma(\omega) \cdot 1 = \omega$, иными словами этот элемент нетривиальным образом действует на единичном слове, а потому $\gamma(\omega) \neq 1$, причем группа $S(\Omega_m)$ является конечной. Это окончательно доказывает остаточную конечность группы $G * H$.

Замечание:

Так как ранее мы показали, что $\mathbb{Z}$ является остаточно конечной, то из этого утверждения вытекает, что свободные группы $\mathbb{F}_n$ тоже являются остаточно конечными. Остаточно конечной является и группа $\mathbb{F}_\infty$, так как в любом слове ω будет фигурировать лишь конечное число порождающих n, а потому можно рассмотреть композицию гомоморфизмов

$$\mathbb{F}_\infty \to \mathbb{F}_n \to F$$

где первый гомоморфизм просто тождественный на первых n порождающих и тривиальный на всех остальных, и фактически он оставляет наше слово ω неизменным; а второй гомоморфизм - это просто некоторый гомоморфизм π в конечную группу, что $\pi(\omega) \neq 1$, построение которого возможно из-за остаточной конечности $\mathbb{F}_n$. Кстати, точно такие же рассуждения позволяют доказать обобщение только что доказанного утверждения: а именно, что если G_i являются остаточно конечными, то и $G = \bigstar_i G_i$ тоже является остаточно конечной (где произведение может быть бесконечным), потому что для любого нетривиального слова нужны буквы только из конечного числа G_i и группу можно отобразить на их конечное произведение, каждый сомножитель из этого списка отображая тождественно, а все остальные сомножители переводя в 1. А дальше воспользоваться остаточной конечностью свободного произведения конечного числа остаточно конечных групп, что в свою очередь получается из многократного применения только что доказанного утверждения.

Другой важный класс остаточно конечных групп получается из следующей теоремы:

Теорема (А.И. Мальцев)
Пусть $G < GL_n(k)$ конечно-порожденная группа, k - поле. Тогда G является остаточно конечной.

Подгруппы группы $GL_n(k)$ называют *линейными*: чаще всего в случае если k - поле, но иногда и в случае, если k - кольцо. Доказательство этой теоремы сложное и существенно опирается на нетривиальную теорию колец, из-за того, что в условии поле произвольное. Если приблизительно описывать идею доказательство (чтобы было ясно, что происходит и почему нужны такие условия), то доказательство примерно такое: пусть $g_1, \ldots, g_r$ симметричный набор порождающих группы G, пусть F - кольцо, порожденное всеми матричными элементами матриц, соответствующих всем порождающим группы $g_1, \ldots g_r$ (а значит и все матричные коэффициенты матриц, соответствующих элементам группы G, будут тоже из F). Дальше если взять произвольный $g \neq 1$ и произвольный ненулевой матричный коэффициент x матрицы $g - 1$, то используя, что k это поле, можно построить такой идеал $m \lhd F$, что $x \notin m$ и F/m конечно. А значит g переходит не в 1 при сквозном гомоморфизме

$$G < GL_n(F) \to GL_n(F/m)$$

причем группа $GL_n(F/m)$ является конечной. Условие конечной порожденности G очень важное, и чуть-чуть позже мы убедимся в этом, доказав, что все $GL_n(\mathbb{C})$ не является остаточно конечной.

Утверждение

Пусть G является делимой, тогда G не является остаточно конечной.

На самом деле верен даже более сильный факт, что не только гомоморфизмы из делимой группы в конечную не разделяют элементов, но даже, что любой гомоморфизм в конечную группы оказывается тривиальным, то есть переводит абсолютно все элементы в 1. Напомню, что *делимыми* называют группы G, что для любого $g \in G$ и любого n существует $h \in G$, что $g = h^n$, иными словами можно извлекать корни любой степени (в абелевом случае и аддитивной записи - делить на любое число - отсюда и название). Рассмотрим произвольный $\pi : G \to F$, где F конечная группа, порядок которой равен n. Пусть $g \neq 1$, из делимости получим, что существует h, что $g = h^n$, а значит $\pi(g) = \pi(h^n) = (\pi(h))^n = 1$, то есть любой такой гомоморфизм тривиальный.

Пример

Доказать, что группа $GL_n(\mathbb{C})$ не является остаточно конечной.

Для доказательства достаточно проверить делимость $GL_n(\mathbb{C})$; для этого для произвольного g рассмотрим базис, в котором g будет иметь жорданову форму. Матрица g приобретает блочную структуру, а потому делимость достаточно проверять для каждого жорданова блока. Но легко заметить, что для матрицы:

$$h = \begin{pmatrix} \sqrt[n]{\lambda} & 1 & & \\ & \sqrt[n]{\lambda} & 1 & \\ & & \ddots & 1 \\ & & & \sqrt[n]{\lambda} \end{pmatrix}$$

где $\sqrt[n]{\lambda}$ это какой-то один фиксированный корень n-ой степени из λ, матрица h^n будет иметь такую же жорданову форму, что и стандартный жорданов λ-блок J_λ размера $r \times r$ (потому что ранг матрицы $h^n - \lambda$ будет равен $r - 1$), иными словами будет существовать некоторое C, что $(C^{-1}hC)^n = J_\lambda$. Таким образом, если каждый блок делим - то и любая матрица делима. Хотя отмечу, что здесь очень важна обратимость матрицы, так как хорошо известно, что у матрицы

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

нет квадратного корня.

Мальцев сформулировал и доказал свою теорему для полей k, часто она обобщается и на кольца, хотя с кольцами обычно все сложно. Однако в конкретных простых и часто встречающихся примерах ситуация оказывается очень прозрачной, например верно следующее утверждение:

Утверждение
Пусть $G < GL_n(\mathbb{Z})$, тогда G является остаточно конечной.

Причем замечу, что мало того, что $\mathbb{Z}$ это только кольцо, так еще утверждение оказывается верным вне зависимости от того, сколько у G порождающих. Напомню, что $GL_n(\mathbb{Z}) = \{x \in M_n(\mathbb{Z}) : \det(x) = \pm 1\}$. Доказательство повторяет идею Мальцева, за той лишь разницей, что с таким простым кольцом многое упрощается: рассмотрим нетривиальный $g \in G$, тогда ненулевая матрица $g - 1$ будет целочисленной. Возьмем любой ненулевой матричный коэффициент этой матрицы - ясно, что он не делится на некоторое натуральное m, и тогда этот g перейдет не в 1 при гомоморфизме $GL_n(\mathbb{Z}) \to GL_n(\mathbb{Z}_m)$, причем группа $GL_n(\mathbb{Z}_m)$ конечна.

В частности из этого утверждения вытекает доказанный нами раньше факт остаточной конечности свободной группы $\mathbb{F}_r$, так как $\mathbb{F}_r \hookrightarrow \mathbb{F}_2 \hookrightarrow SL_2(\mathbb{Z})$. Напомню, что в первой части методички мы выясняли, что свободная группа порождается 2×2 матрицами Санова:

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad \text{и} \qquad \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

Все это говорит о том, что в некотором смысле матричные группы очень похожи на остаточно конечные в случае конечно-порожденных групп, причем они так похожи, что при неглубоком погружении в эту теорию очень грубо можно считать, что это одно и то же (даже несмотря на их некоторые внутренние структурные различия): причем кроме теоремы Мальцева существует еще связь в обратную сторону, а именно естественное отображение $S_n \hookrightarrow GL_n(\mathbb{Z})$, отправляющее перестановку σ в соответствующий матричный сдвиг $T_\sigma e_i = e_{\sigma(i)}$. На практике оказывается, что в конечно-порожденном случае теорема Мальцева покрывает очень широкий спектр остаточно конечных групп, однако все примеры остаточно конечных и нелинейных групп строятся сложно, и классическим таким примером является пример Друту и Сапира (Drutu, Sapir) нелинейной остаточно конечной группы

$$G = \langle a, b | b^{-2}ab^2 = a^2 \rangle$$

При этом в бесконечно-порожденном случае линейные и остаточно конечные группы уже никак не связаны: к примеру $\mathbb{Q}$ не является остаточно конечной (из-за того, что она является делимой), но при этом эта группа линейна, например, можно построить вложение $\mathbb{Q} \to SL_2(\mathbb{Q})$, заданное формулой:

$$q \mapsto \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}$$

Ясно, что это гомоморфизм. Обратные примеры остаточно конечных нелинейных групп в бесконечно-порожденном случае строятся намного проще чем в конечно-порожденном: к примеру, $G = \bigoplus_{n=1}^{\infty} \mathbb{Z}_2$ является остаточно конечной, но при этом нелинейной, так как если бы существовал инъективный гомоморфизм $G \to GL_n(k)$ (где k это поле), то порождающие бы отобразились в бесконечную серию коммутирующих между собой симметрий, при этом любая симметрия s (то есть матрица с условием $s^2 = 1$) допускает разложение $s = 1 - 2p$, где p - это проектор (в данном случае $p = \frac{1+s}{2}$), причем соответствующие попарно коммутирующим

симметриям проекторы будут тоже попарно коммутировать, откуда легко вытекает, что для этих симметрий будет существовать общий для всех диагонализующий базис (для проекторов это условие проще проверять чем для симметрий). Для иллюстрации идеи доказательства рассмотрим простой случай двух коммутирующих проекторов p, q: рассматривая первый проектор мы получаем, что k^n раскладывается в прямую сумму $\operatorname{Im} p$ и $\operatorname{Im}(1-p)$. Так как $[q,p]=0$, то каждое из этих пространств будет инвариантным для q (к примеру, для $\operatorname{Im} p$ рассуждения такие: $x \in \operatorname{Im} p \Rightarrow qx = qpx = p(qx) \in \operatorname{Im} p$), таким образом каждое из этих пространств π в свою очередь раскладывается в прямую сумму пересечений π с $\operatorname{Im} q$ и $\operatorname{Im}(1-q)$ (возможно тривиальных, если некоторые пересечения тривиальны, например $\operatorname{Im} p \cap \operatorname{Im} q = \{0\}$). Таким образом, пространство k^n раскладывается в прямую сумму всевозможных пересечений $\operatorname{Im} p$, $\operatorname{Im}(1-p)$ с $\operatorname{Im} q$ и $\operatorname{Im}(1-q)$, и соединяя воедино базисы всех этих подпространств мы получаем базис всего пространства, в котором все проекторы диагонализируемы. В общем случае коммутирующих $p_1, \ldots, p_m$ заметим, что $V = V_1 \cap V_2 \cap \ldots \cap V_m$ будет инвариантно для любого из этих проекторов, здесь каждое V_i - это либо $\operatorname{Im} p_i$ либо $\operatorname{Im}(1-p_i)$, так как если $v \in V$ и через q_i обозначить соответственно либо p_i либо $(1-p_i)$, то

$$p_j v = p_j(q_1 q_2 \ldots q_m)v = (q_1 q_2 \ldots q_m)p_j v \in V$$

также легко понять, что k^n раскладывается в прямую сумму всевозможных V. И если взять базисы в каждом из этих пространств, то вместе они будут базисом всего пространства, в котором все эти проекторы одновременно диагонализуются.

Но раз у них есть общий диагонализующий базис, то нетрудно понять, что в $GL_n(k)$ существует самое большое 2^n попарно коммутирующих симметрий (так как на каждом базисном векторе в их общем диагонализующем базисе они могут быть равны либо 1, либо -1). Но при этом нам нужно как-то уместить в $GL_n(k)$ бесконечное число коммутирующих симметрий, что невозможно, а значит $G = \bigoplus_{n=1}^{\infty} \mathbb{Z}_2$ нелинейна.

Что касается групп, не являющихся остаточно конечными, то мы с вами уже разбирали прием, согласно которому любой гомоморфизм делимых групп в конечные группы является тривиальным, а значит они не могут быть остаточно конечными. Другой простой класс - это бесконечные простые группы: они тоже очевидно не будут являться остаточно конечными: из-за того что как и в случае с делимыми группами любой их гомоморфизм в конечную группу $\pi : G \to F$ будет тривиален, так как $\ker(\pi) \lhd G$ должно быть конечного индекса (потому что $[G : \ker(\pi)] = |G/\ker(\pi)| \leq |F|$), но из-за простоты в G вообще нет нетривиальных нормальных подгрупп. Ну и как следствие получаем, что группа $A_\infty = \bigcup_n A_n$ не является остаточно конечной.

Строить конечно-порожденные группы, не являющиеся остаточно конечными, намного сложнее, и классическим примером является группа Баумслага-Солитера, но сначала мы бездоказательно сформулируем очень важную теоретико-групповую лемму, которая понадобится нам в доказательстве:

Лемма (Бриттон (Britton), 1963)
Пусть в произвольной группе G дан изоморфизм $\alpha : A \to B$ между двумя подгруппами $A, B < G$. Рассмотрим $HNN(G) = \langle G, t : t^{-1}at = \alpha(t), a \in A\rangle$. Пусть

$$\omega = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} \dots g_{n-1} t^{\varepsilon_n} g_n$$

где каждый ε_i равен 1 или -1. Тогда если $\omega = 1$ в $HNN(G)$, то либо $n = 0$ и $g_0 = 1$, либо существует i, такое что $\varepsilon_i = -1$, $\varepsilon_{i+1} = 1$ и $g_i \in A$ или $\varepsilon_i = 1$, $\varepsilon_{i+1} = -1$ и $g_i \in B$.

Ясно, что в этой группе можно совершать сокращения как $t^{-1}at = \alpha(a)$, так и $tbt^{-1} = \alpha^{-1}(b)$ если перебросить сопряжение вправо, то есть фактически с подсловами $t^{-1}at$ и tbt^{-1} можно сделать хоть что-то с использованием определяющих соотношений группы. И фактически лемма Бриттона говорит, что если $\omega = 1$ для $\omega \in HNN(G)$, то либо слово тривиально, либо слово допускает очевидные сокращение с использованием определяющих соотношений, что на интуитивном уровне кажется очень правдоподобно: так как если в слове не встречаются описанные в условии леммы ситуации, то со словом с помощью определяющих соотношений вообще нельзя ничего сделать, ни на грамм его не получается сократить. Однако все равно это нестрогие рассуждения не претендующие на доказательство, но лишь помогающие лучше понять природу этой леммы, потому что сокращения могут рождаться не только из определяющих соотношений r, но и из их сопряжений $s^{-1}rs$. Чаще всего на практике лемма Бриттона используется в своей контрапозиционной форме: а именно *если в ω нет подслов вида $t^{-1}at$ и tbt^{-1}, и при этом $n \neq 0$, то* $\omega \neq 1$. Лемма эта очень мощная и позволяет проводить прямые и строгие выкладки с конкретными элементами из HNN-расширений (фактически, она помогает строго обосновать в HNN-расширениях рассуждения в духе "в слове ничего не получается сократить - значит оно нетривиальное"). Из этой леммы почти автоматом получается множество структурных результатов про HNN-расширения: например, что элементы конечного порядка в $HNN(G)$ сопряжены некоторому элементу из G (идеологически это утверждение напоминает ранее доказанный нами факт, что элементы конечного порядка в свободных произведениях сопряжены элементам конечного порядка в сомножителях свободного произведения). Отмечу также, что лемма Бриттона работает и для слов, либо начинающихся, либо заканчивающихся со степени t: потому что мы оказывается именно в таких ситуациях, если соответственно $g_0 = 1$ либо $g_n = 1$. Также отмечу, что лемма Бриттона прекрасно работает с высокими степенями t, а не только ± 1: и высокие степени можно получить, если правильные $g_i = 1$. К примеру, легко доказать, что $t^{-2}gt^2 \neq 1$, где $g \notin A$, применяя лемму Бриттона к слову $t^{-1}et^{-1}gtet$, где $e = 1$. В случае же $A = B = G$ мы помним, что $HNN(G) = G \rtimes \mathbb{Z}$ и лемма Бриттона в этом случае не особо нужна, так как любой элемент $\omega \in G \rtimes \mathbb{Z}$ имеет вид $\omega = gt^m$, где $g \in G$ и $m \in \mathbb{Z}$, и такие слова сравнивать между собой и с 1 легко и без леммы Бриттона. Итак возвращаемся к остаточно конечным группам:

Пример
Группа $B(2,3) = \langle a, b |\ b^{-1}a^2b = a^3 \rangle$ *не является остаточно конечной.*

Если честно, то учитывая сколько раз эта группа нам уже встретилась, хочется прямо сказать: "все дороги в мире групп ведут к группе Баумслага-Солитера". Рассмотрим произвольный гомоморфизм $\pi : B(2,3) \to F$ в конечную группу, и пусть порядок F равен n. В конце главы про гиперболичность мы с вами доказывали, что из определяющего соотношения $b^{-1}a^2b = a^3$ по индукции легко вывести соотношение $b^{-m}a^{2^m}b^m = a^{3^m}$ для любого m. Пусть $A = \pi(a)$ и $B = \pi(b)$. Тогда раз n это порядок F, то получаем $B^n = 1$, а значит:

$$A^{2^n} = B^{-n}A^{2^n}B^n = A^{3^n}$$

иными словами $A^{3^n-2^n} = 1$, откуда получаем, что $3^n - 2^n$ делится на $\mathrm{ord}(A)$, и раз $3^n - 2^n$ нечетное, то и $\mathrm{ord}(A)$ нечетное. Группа $\langle A \rangle$ является циклической группой нечетного порядка, а потому она порождается A^2 так как 2 взаимно просто с $\mathrm{ord}(A)$. Отсюда мы приходим к выводу, что $A = (A^2)^k$ для некоторого k. Таким образом мы получим, что

$$B^{-1}AB = B^{-1}(A^2)^kB = (B^{-1}A^2B)^k = A^{3k}$$

от этого соотношения в чистом виде мало пользы, так как оно зависит от k, которое для каждой группы F свое. Но от этой зависимости легко избавиться, если заметить, что:

$$[A, B^{-1}AB] = [A, A^{3k}] = 1$$

Таким образом мы можем резюмировать, что для любого гомоморфизма $\pi : G \to F$ в конечную группу $\pi([a, b^{-1}ab]) = 1$ (заметьте как красиво мы избавились от k). Но при этом $B(2,3) = HNN(\mathbb{Z})$, где $\mathbb{Z} = \langle a \rangle$ и определяющий HNN-расширение изоморфизм α в данном случае склеивает $\alpha : \langle a^2 \rangle \to \langle a^3 \rangle$, причем в аддитивной записи этот изоморфизм $2\mathbb{Z} \to 3\mathbb{Z}$ действует по формуле $2n \mapsto 3n$ (а в мультипликативной $a^{2n} \mapsto a^{3n}$). Тогда применяя лемму Бриттона можно убедиться в нетривиальности этого коммутатора (в копредставлении группы Баумслага-Солитера b играет роль t из леммы Бриттона):

$$[a, b^{-1}ab] = ab^{-1}aba^{-1}b^{-1}a^{-1}b \neq 1$$

так как в это слово не входят подслова вида $b^{-1}a^{2j}b$ или $ba^{3j}b^{-1}$. Таким образом этот нетривиальный элемент переходит в 1 при любом гомоморфизме в конечную группу, а значит $B(2,3)$ не является остаточно конечной.

Для понимания общей картины происходящего с группами Баумслага-Солитера сформулируем без доказательства следующую теорему:

Теорема (Meskin)
Группа $B(n,m)$ *является остаточно конечной* $\iff |m| = 1$, *или* $|n| = 1$, *или* $|n| = |m|$.

Пример

Группа Хигмана $H = \langle a, b, c, d |\ a^{-1}ba = b^2, b^{-1}cb = c^2, c^{-1}dc = d^2, d^{-1}ad = a^2 \rangle$ *не является остаточно конечной.*

Для доказательства нам сперва понадобится следующий теоретико-числовой факт: *для любого* n *наименьший простой делитель* n *меньше наименьшего простого делителя* $2^n - 1$. Для его доказательства рассмотрим некоторый простой делитель p числа $2^n - 1$ (ясно, что p нечетное). Пусть r минимальное такое, что p делит $2^r - 1$. Далее заметим, что раз p - нечетное простое число, то по малой теореме Ферма $2^{p-1} - 1$ делится на p.

Также если p делит $2^m - 1$, то r делит m, потому что если поделить с остатком $m = \alpha r + \beta$ и записать делимость через модульные равенства, то получим $2^m = 1 \mod p$, а также $2^r = 1 \mod p$, таким образом:

$$1 = 2^m = (2^r)^\alpha 2^\beta = 1^\alpha 2^\beta = 2^\beta \mod p$$

и мы приходим к противоречию, так как выбирали r минимальным с условием $2^r = 1 \mod p$. Отсюда вытекает, что r делит как n, так и $p - 1$. И если рассмотреть произвольный простой делитель q числа r, то он тоже будет делить и n, и $p - 1$, в частности $q \leq p-1 < p$. И если объединить все эти наши рассуждения, то получается, что для любого простого делителя p числа $2^n - 1$ мы нашли простой q, делящий n, и для которого $q < p$, что доказывает наше вспомогательное теоретико-множественное утверждение.

Возвращаясь к группе Хигмана: мы докажем более сильный факт, что любой гомоморфизм $\pi : H \to F$ в конечную группу тривиален. Пусть $\pi(a) = A$, $\pi(b) = B$, $\pi(c) = C$ и $\pi(d) = D$. Нетрудно заметить, что если хотя бы один из низ равен 1 (пусть это будет $A = 1$), тогда и все остальные равны 1, так как с учетом тривиальности одного их порождающих соотношения тривиализуются: $A^{-1}DA = D^2 \Rightarrow D = 1$, далее $D^{-1}CD = C^2 \Rightarrow C = 1$ и так далее. Поэтому можем считать, что порядки образов порождающих A, B, C, D отличны от 1. Рассмотрим среди них тот, у которого самый маленьких простой делитель из всех, из равноправия можем считать, что это B. Пусть $\mathrm{ord}(A) = n_A$ и $\mathrm{ord}(B) = n_B$. Тогда из $A^{-1}BA = B^2$ легко вытекает:

$$B = A^{-n_A} B A^{n_A} = B^{2^{n_A}}$$

а значит $B^{2^{n_A}-1} = 1$, откуда получаем, что n_B делит $2^{n_A}-1$, а значит любой простой делитель n_B является и простым делителем $2^{n_A}-1$; и из нашего теоретико-числового утверждения мы получаем, что наименьший простой делитель n_A будет меньше наименьшего простого делителя $2^{n_A}-1$, который в свою очередь $\leq$ наименьшего простого делителя n_B и приходим к противоречию.

Замечания:

• *Легко заметить, что в доказательстве фактически нигде не используется, что в копредставлении группы соотношением $x^{-1}yx = y^2$ запутываются именно 4 порождающих, а потому утверждение о тривиальности любого гомоморфизма в конечную группу верно для модификации группы Хигмана с любым количеством запутывающихся порождающих. Правда если число порождающих ≤ 3, то группа оказывается тривиальной и утверждение становится бессодержательным (тривиальность группы Хигмана с 3 порождающими раньше всплывала в качестве упражнения в первой части методички), если же число порождающих ≥ 4, то группа нетривиальна (мы это докажем только в случае 4 порождающих). Чтобы не стрелять из пушки по воробьям в таких задачах на проверку группы на тривиальность сперва полезно вычислить абеленизацию, и добавляя коммутационные соотношения на все порождающие, 4 наши соотношения превращаются в $a = b = c = d = 1$, поэтому $H_{ab} = \{1\}$, и удача обошла нас стороной (так как если $G_{ab} \neq \{1\}$, то сразу вытекло бы $G \neq \{1\}$). Для того, чтобы показать, что группа Хигмана H нетривиальна, можно заметить, что она представляется в виде амальгамированного произведения:*

$$H \cong A \underset{\substack{c=x \\ a=y}}{*} B$$

где $A = \langle a, b, c |\ a^{-1}ba = b^2, b^{-1}cb = c^2\rangle$ и $B = \langle x, d, y |\ x^{-1}dx = d^2, d^{-1}yd = y^2\rangle$ являются двумя изоморфными группам, которые нетривиальны потому что их абеленизации нетривиальны, а амальгамирование берется по общей подгруппе $\langle a, c\rangle \cong \langle y, x\rangle$ (подгруппы изоморфны, так как они просто одинаковые с точностью до переобозначения порождающих в копредставлениях A и B). Так как сомножители нетривиальны, то и само амальгамированное произведение нетривиально.

Амальгамированным произведением $A \underset{C}{*} B$ двух групп A и B по группе C вместе с гомоморфизмами $\alpha_A : C \to A$ и $\alpha_B : C \to B$ называют:

$$A \underset{C}{*} B = A * B/_{\sim}$$

где отношение $\sim$ фактически отождествляет в амальгамированном произведении (которое еще иногда называют амальгамой) элементы в A и B являющиеся образом одного и того же элемента группы C, и в некотором смысле подгруппу C можно считать общей для A и B в амальгаме. Более формально $A \underset{C}{*} B = (A * B)/N$, где N - нормальное замыкание элементов вида $\alpha_A(c)\alpha_B(c^{-1})$ где $c \in C$. На уровне копредставлений если $A = \langle S_A |\ R_A\rangle$, $B = \langle S_B |\ R_B\rangle$, $C = \langle S_C |\ \ldots\rangle$, то

$$A \underset{C}{*} B = \langle S_A, S_B |\ R_A, R_B, \alpha_A(c) = \alpha_B(c) \text{ для любого } c \in S_C\rangle$$

Иными словами, чтобы выписать копредставление для амальгамы - нужно выписать все порождающие и соотношения вместе для A и B, а также дописать дополнительные соотношения, отождествляя все порождающие C с их образами в A и B. Есть удобная словесная модель для амальгамы, согласно которой амальгама $A \underset{C}{*} B$ изоморфна множеству классов эквивалентностей слов, составные буквы которых являются либо элементами A, либо элементами B, умножение

есть просто формальное приписывание слов друг к другу, если встречаются подряд две буквы из одного сомножителя - то их можно перемножить как групповые элементы: и вот это в точности модель свободного произведения. A в амальгаме помимо этого добавляется только, что элементы подгруппы $\alpha_A(C)$ можно трактовать и как элемент B, и наоборот для $\alpha_B(C)$; в теории групп типично, что α_A и α_B являются инъективными, а потому C можно воспринимать просто как общую подгруппу A и B, и фактически в словесной модели элементы C можно воспринимать как элементы и A, и B одновременно со всеми вытекающими для возможных сокращений последствиями. В случае нашей группы Хигмана $C = \langle a, c\rangle \cong \langle x, y\rangle$, а α_A и α_B словесно-тождественные вложения этой группы в A и B.

Очень легко проверить, что $A \underset{\{1\}}{*} B = A * B$, а также $A \underset{A}{*} A = A$ для любых групп A, B. Также упомяну топологическую теорему Зейферта - ван Кампена, что если $U, V \subset X$ два линейно связных подпространства топологического пространства X с линейно связным пересечением $W = U \cap V$, то

$$\pi_1(U \cup V) = \pi_1(U) \underset{\pi_1(W)}{*} \pi_1(V)$$

таким образом фундаментальная группа склейки двух пространств по общему подпространству равна просто амальгаме фундаментальных групп U и V. Замечу, что индуцируемый вложением $W \subset U$ гомоморфизм $\pi_1(W) \to \pi_1(U)$ совершенно не обязан быть инъективным.

• *Отмечу также, что пафос только что доказанного утверждения о том, что любой гомоморфизм $H \to F$ в конечную групп тривиален, заключается во-первых в том, что конечно-определенные примеры в таких ситуациях строить особенно сложно. А во-вторых в том, что тривиальность гомоморфизма $H \to F$ вытекала из невозможности нетривиальной реализации конкретных соотношений в конечных группах вместо абстрактных и общих рассуждений о делимости или простоте группы, из которых тоже вытекала бы тривиальность гомоморфизма и которые мы проводили для доказательства отсутствия остаточной конечности у групп вроде $\mathbb{Q}$, $GL_n(\mathbb{C})$ и A_∞. Работа этих методов основана на очень глубоком погружении в структуру группы (например проверка простоты, фактически, означает, что мы должны все нормальные подгруппы сравнить с исходной группой), тогда как это доказательство показывает, что не нужно погружаться глубоко, и вот только эти 4 соотношения все ломают (как и в случае групп Баумслага-Солитера, но у них все-таки есть нетривиальные гомоморфизмы в конечные группы). Также отмечу, что группа Хигмана не является простой: вытекает это из упомянутого выше представления амальгамой:*

$$H \cong A \underset{C}{*} A$$

где, напомню, $A = \langle a, b, c |\ a^{-1}ba = b^2, b^{-1}cb = c^2\rangle$, мы можем считать, что сомножители совпадают, так как они отличаются только переобозначением порождающих. Рассмотрим нетривиальную нормальную подгруппу $N \lhd A$ (например, можем взять $N = [A, A]$, так как у A нетривиальная абеленизация

$$A/[A, A] = A_{ab} = \langle a, b, c |\ b = 2b, c = 2c\rangle = \langle a, b, c |\ b = 0, c = 0\rangle = \langle a\rangle \cong \mathbb{Z}$$

где здесь все записано в аддитивной записи, а значит в предположении, что все элементы коммутируют), также легко проверить, что $N \cap C \lhd C$, а значит существует естественный нетривиальный гомоморфизм:

$$H \cong A \underset{C}{*} A \to (A/N) \underset{C/(C\cap N)}{*} (A/N)$$

Ядро этого гомоморфизма будет нетривиальной нормальной подгруппой в H. Также отмечу, что тривиальность любого гомоморфизма в конечную группу в немного других терминах означает, что в H нет нетривиальных нормальных подгрупп конечного индекса.

У остаточно конечных групп существует масса приложений, я расскажу про два наиболее ярких: связанные с хопфовыми группами и алгоритмической разрешимостью.

Определение
Группа G называется хопфовой (или группой Хопфа, Hopfian group), если для любой $N \lhd G$, такой что $G/N \cong G$, выполнено $N = \{1\}$.

В таких группах любой эпиморфизм $\alpha : G \to G$ группы на себя является изоморфизмом: потому что по теореме о гомоморфизме $G = \operatorname{Im}\alpha \cong G/\ker\alpha$ и из хопфовости получаем $\ker\alpha = \{1\}$, то есть α изоморфизм. Верно и обратное: что если любой эпиморфизм является изоморфизмом - то группа хопфова: потому что тогда естественный гомоморфизм $G \to G/N$ будет являться изоморфизмом, откуда вытекает, что $N = \{1\}$. Любая конечная группа является хопфовой из соображений мощности, группа $G = \mathbb{Z}$ тоже является хопфовой, потому что все ее нетривиальные подгруппы имеют конечный индекс, а потому G/N является конечной и не может быть изоморфна бесконечной G. С примерами нехопфовых групп мы с вами уже встречались раньше: к примеру мы обсуждали пример не являющегося изоморфизмом эпиморфизма $\alpha : S^1 \to S^1$ группы комплексных чисел с модулем равным 1, заданного формулой $z \mapsto z^2$. Другой классический пример это группа $G = \bigoplus\limits_{n\in\mathbb{N}} \mathbb{Z}_2 = \mathbb{Z}_2^\infty$ с эпиморфизмом $\alpha : \mathbb{Z}_2^\infty \to \mathbb{Z}_2^\infty$, заданным формулой:

$$\alpha(x_1, x_2, x_3, \ldots) = (x_2, x_3, \ldots)$$

Это эпиморфизм с ядром, порожденным $(1, 0, 0, \ldots)$. Строить же конечно-порожденные примеры нехопфовых групп намного сложнее; и во многом остаточно конечные группы исторически привлекли внимание математиков как раз потому, чтобы лучше разобраться в природе конечно-порожденных хопфовых групп. Лучше всего взаимосвязь остаточно конечных групп с хопфовыми группами отражается в следующей теореме:

Теорема

Пусть G конечно-порожденная остаточно конечная группа. Тогда G хопфова группа.

Пусть G не является хопфовой, а значит существует некоторый не являющийся изоморфизмом эпиморфизм $\alpha : G \to G$. Раз он не является изоморфизмом, то найдется $1 \neq g \in \ker \alpha$. Так как G остаточно конечна, то рассмотрим гомоморфизм в конечную группу $\varphi : G \to F$, что $\varphi(g) \neq 1$. Так как α эпиморфизм, то мы можем образовать последовательность, состоящую из g, некоторого его прообраза, прообраза его прообраза и так далее, более формально $\{g_0, g_1, g_2, \ldots\}$, такую что $g_0 = g$ и $\alpha(g_{i+1}) = g_i$. Теперь мы можем рассмотреть гомоморфизмы:

$$\varphi \circ \alpha^{(n)} : G \to F$$

И нетрудно заметить, что $\varphi \circ \alpha^{(n)}(g_n) = \varphi(g) \neq 1$ и $\varphi \circ \alpha^{(n)}(g_k) = 1$ для $k < n$. Таким образом это бесконечная серия попарно различных гомоморфизмов (и заодно задним числом мы получили, что все g_i тоже попарно различны). И мы приходим к противоречию, потому что у конечно-порожденной группы в заданную конечную группу F может быть только конечное число различных гомоморфизмов (потому что для образа каждого порождающего у вас максимум $|F|$ возможностей).

Таким образом все обсуждаемые нами ранее конечно-порожденные остаточно конечные группы, например $\mathbb{F}_2$, $B(1, n)$, $\mathbb{Z}_n * \mathbb{Z}_m$ и т.д., автоматически будут хопфовыми (и любой их эпиморфизм на себя будет изоморфизмом), и эта теорема обеспечивает нас очень широким классом хопфовых групп. Эта теорема фактически означает, что в конечно-порожденном случае понятие хопфовости есть просто ослабленная версия остаточной конечности: к сожалению или счастью в обратную сторону эта теорема не верна, как мы увидим чуть позже на примере групп Баумслага-Солитера. Также отмечу, что в бесконечно-порожденном случае нет вообще никакой связи между остаточной конечностью и хопфовостью: к примеру группа $\bigoplus_{n \in \mathbb{N}} \mathbb{Z}_2$ является остаточно конечной, но при этом она, как мы уже выясняли, не является хопфовой. В случае с бесконечными суммами групп: остаточная конечность эквивалентна остаточной конечности каждого прямого слагаемого, тогда как отсутствие хопфовости можно добиться просто некоторой однородностью слагаемых, чтобы существовал гомоморфизм сдвига аргументов или некоторая его модификация.

Так как эта теорема работает только в одну сторону - то даже зная критерий остаточной конечности групп Баумслага-Солитера $B(n, m)$, она не обеспечит нас примером нехопфовой группы Баумслага-Солитера (контрапозиция этой теоремы это *нехопфовость* $\Rightarrow$ *отсутствие остаточной конечности*).

Пример

Пусть m и n взаимно простые. Тогда группа $B(m,n) = \langle a, b |\ b^{-1}a^m b = a^n \rangle$ не является хопфовой.

Рассмотрим $\phi : B(m,n) \to B(m,n)$ на порождающих заданный следующим образом $b \mapsto b$, $a \mapsto a^m$. Так как единственное определяющее соотношение переходит в единицу:

$$\varphi(b^{-1}a^m b a^{-n}) = b^{-1}(a^m)^m b (a^{-n})^m = (b^{-1}a^m b)^m (a^{-n})^m = 1$$

поэтому это отображение продолжается до гомоморфизма всей группы $\phi : B(m,n) \to B(m,n)$.

Так как m и n взаимно просты, то для некоторых целых x, y будет выполнено $xm + yn = 1$, а значит:

$$a = a^{xm+yn} = (a^m)^x (a^n)^y = (a^m)^x (b^{-1}a^m b)^y = (\varphi(a))^x (\varphi(b^{-1}ab))^y \in \operatorname{Im}\varphi$$

А значит если все порождающие группы попадают в образ, то этот гомоморфизм является эпиморфизмом. С другой стороны он не является изоморфизмом: так как $B(m,n) = HNN(\mathbb{Z})$, где расширение $\mathbb{Z}$ строится по изоморфизму $m\mathbb{Z} \to n\mathbb{Z}$, то можем заключить из леммы Бриттона, что $[a, b^{-1}ab] = ab^{-1}aba^{-1}b^{-1}a^{-1}b \neq 1$ потому что в этом слове не встречаются подслова вида $b^{-1}a^{mx}b$ или же $ba^{ny}b^{-1}$; но при этом

$$\varphi([a, b^{-1}ab]) = [a^m, b^{-1}a^m b] = [a^m, a^n] = 1$$

Таким образом φ - это не являющийся изоморфизмом эпиморфизм, а значит $B(m,n)$ не является хофовой.

Замечу, что доказательство очень сильно напоминает доказательство отсутствия остаточной конечности для $B(2,3)$: та же нетривиальность коммутатора $[a, b^{-1}ab]$ по лемме Бриттона, и те же попытки перенести коммутируемость a и $b^{-1}a^m b$ на более низкие степени. Чтобы понимать общую картину - без доказательства сформулируем критерий хопфовости для групп Баумсалага-Солитера:

Теорема

Группа $B(n,m)$ является хопфовой $\iff$ или $|m| = 1$, или $|n| = 1$, или же $\pi(n) = \pi(m)$, где $\pi(k)$ есть множество простых делителей числа k.

Полезно на эту теорему смотреть через призму теоремы Мескина, согласно которой остаточная конечность эквивалентна $|m| = 1$, или $|n| = 1$, или же $|m| = |n|$, что, разумеется, является более сильным условием чем в только что сформулированной теореме. В частности отсюда мы получаем, что группа $B(2,4)$ является хопфовой, но при этом она не является остаточно конечной.

Второе приложение связано с алгоритмической разрешимостью и основано на следующем утверждении:

Утверждение

Пусть $G = \langle A|\ R\rangle$ конечно-определенная остаточно конечная группа. Тогда в G разрешима проблема равенства слов.

Считаем, что A - симметричное множество порождающих. Сначала заметим, что проверка того, что заданное на порождающих отображение $A \to S_n$ продолжается до гомоморфизма $G \to S_n$, проверяется за конечное число шагов, так как для проверки нужно лишь проверить, что все соотношения из R отправляются в 1. Таким образом можно построить алгоритм, выдающий последовательность $\{\alpha_1, \alpha_2, \alpha_3, \ldots\}$ всевозможных гомоморфизмов во всевозможные S_n: просто перечисляем все функции $A \to S_n$ и оставляем те, которые отправляют R в 1.

С другой стороны можно построить алгоритм, выдающий все тривиальные слова: потому что по определение тривиальное слово обязательно представляется в виде произведения сопряжений соотношений из R, поэтому можно задать такое перечисление - сначала выписать все сопряжения словами из одной буквы (в алфавите A) слов из R, потом всевозможные произведения не более двух сопряжений слов из R словами длины не более 2, потом произведения не более чем трех сопряжений слов из R словами длины не более 3 и так далее. Иными словами:

$$x^{-1}r_1x \qquad (y^{-1}r_2y)(z^{-1}r_3z) \qquad \ldots$$

где $r_i \in R \cup e$, а x - однобуквенное слово, y, z - двухбуквенные слова и т.д. Уточню, что эти слова еще нужно привести, то есть провести все сокращения подслов вида aa^{-1} для $a \in A$. В результате мы получим перечисление $\langle\langle R\rangle\rangle = \{q_1, q_2, q_3, \ldots\}$ всех слов из $\mathbb{F}(A)$, тривиальных в G.

И для проверки $\omega \in \mathbb{F}(A)$ на тривиальность в G нам нужно запустить параллельно два этих алгоритма: чередовать побуквенное сравнение ω с последующим q_i с проверкой того, что $\alpha_i(\omega) \neq 1$ (группа S_n конечная, а потому в ней алгоритмически разрешима проверка равенства слов). И если $\omega = 1$ в G, тогда в какой-то момент получится побуквенное равенство $\omega = q_i$. Если же $\omega \neq 1$, тогда из остаточной конечности существует гомоморфизм в конечную группу $G \to F$ отделяющий ω от 1, и если взять его композицию с гомоморфизмом Кэли $F \to S(F) = S_{|F|}$, то получится, что для некоторого гомоморфизма i выполнено $\alpha_i(\omega) \neq 1$, потому что α_i перечисляет все гомоморфизмы во всевозможные S_n. Таким образом за конечное число шагов мы определили верно ли, что $\omega = 1$.

Замечания:

• *Отмечу, что остаточная конечность использовалась для того, чтобы алгоритмически перечислить все гомоморфизмы во всевозможные S_n, так как они вместе разделяют все элементы группы. Если бы этой последовательности не было - мы бы за конечное число шагов смогли определить, что $\omega = 1$, но если вдруг $\omega \neq 1$, то алгоритм зависнет и будет работать бесконечно долго, хотя по определению алгоритмической разрешимости должен работать конечное число шагов. Несмотря на то, что множество нетривиальных слов $\{g_1, g_2, g_3, \ldots\}$ - это в точности дополнение к $\langle\langle R\rangle\rangle = \{q_1, q_2, q_3, \ldots\}$, и оно является счетным множеством, но типично, что это множество неперечислимо, то есть нельзя записать алгоритм, который в качестве результата работы выдал бы нам эту*

последовательность. И фактически мы доказали, что в остаточно конечном случае это сделать все-таки можно.

• *Кстати, отмечу, что для построения второго алгоритма конечность R была непринципиальна, и хватало бы простой перечислимости R для алгоритмического задания всех тривиальных слов. Что же качается перечисления всех гомоморфизмов α_i, то здесь конечность R принципиально нужна, так как в противном случае проверить, что функция $A \to S_n$ продолжается до гомоморфизма, за конечное число шагов не получится.*

• *Возможно упоминание конечной определенности и алгоритмической разрешимости равенства слов вместе впустило шторм воспоминаний и мыслей о гиперболических группах, и это правильный потом мыслей. Ясно, что конечно-определенная остаточно конечная группа не обязана быть гиперболической: можно рассмотреть пример того же $\mathbb{Z}^2$. А вот вопрос о том, всякая ли гиперболическая группа является остаточно конечной, остается открытым по сей день.*

Ну и в самом конце хочется сказать несколько слов об очень далеко идущем обобщении понятия остаточной конечности: фактически остаточная конечность означает, что гомоморфизмы в конечные группы в некотором смысле кодируют всю содержащуюся о группе информацию. Но в последние годы в математике вместе с классическими понятиями стало модным рассматривать их более гибкие версии, где вместо конкретных точных равенств допускается погрешность. В данном случае можно гомоморфизмы заменить почти гомоморфизмами и прийти к понятию *софических групп (sofic groups).* Впервые их рассмотрел тоже М.Л. Громов в попытке разобраться всякая ли группа является сюръюнктивной (surjunctive group, не путайте с сюръективностью). Вопрос этот открыт по сей день, но на пути к нему люди приходят к интересным и красивым классам групп. Софические группы называются так, потому что sofic с иврита переводится как "конечный". Итак перейдем к базовым определениям. Пусть $\theta, \tau \in S_n$. Тогда расстоянием Хэмминга между ними называют:

$$d_H(\theta, \tau) = \frac{1}{n}\Big|\{j \in \{1, 2, \ldots, n\} : \theta(j) \neq \tau(j)\}\Big|$$

иначе говоря доля точек с различными образами. В частном случае $d_H(\theta, 1)$ это доля точек, не являющихся неподвижными для θ (иначе говоря сдвигаемых). Очевидно, что $d_H(\theta, \tau) = d_H(\alpha\theta, \alpha\tau) = d_H(\theta\alpha, \tau\alpha)$ для любой α. Из этих свойств также вытекает, что $d_H(\theta, \tau) = d_H(\tau^{-1}\theta, 1)$ если положить $\alpha = \tau^{-1}$.

Определение

Счетная группа G называется софической, если для любого $\varepsilon > 0$ и для любого конечного множества $F \subset G$ для некоторого n существует отображение $\sigma : G \to S_n$, что:

• *$d_H(\sigma(gh), \sigma(g)\sigma(h)) < \varepsilon$ для любых $g, h \in F$.*

• *$d_H(\sigma(g), 1) > r(g) > 0$ для любого $g \in F \backslash \{1\}$ и для некоторой зависящей только от g функции $r(g)$.*

Отображения $\sigma : G \to S_n$, для которых выполняется первое из двух свойств называют (F, ε)-почти гомоморфизмом. Во-первых, заметим, что если $1 \in F$, то с учетом инвариантности расстояния Хэмминга относительно сдвигов мы получаем $d_H(\sigma(1), 1) = d_H(\sigma(1)\sigma(1), \sigma(1 \cdot 1)) < \varepsilon$, а потому при таких отображениях образ 1 близок к настоящей единице. Также отмечу, что почти гомоморфизмы не обязаны в общем случае быть близки к обычным классическим гомоморфизмам, более того иногда у группы есть много почти гомоморфизмов даже тогда, когда у нее совсем нет нетривиальных настоящих гомоморфизмов (например, в случае простых групп).

Также отмечу, что угнетающая и зависящая от g константа может быть заменена на любую универсальную константу $C \in (0, 1)$, и чтобы в этом убедиться используют такой трюк: рассмотрим гомоморфизм $S_n \to S_{n^2} = S(\{1, 2, \ldots, n\} \times \{1, 2, \ldots, n\})$, такой что $\theta \mapsto \theta^{\otimes 2}$, действующая как θ в каждой координате $\theta^{\otimes 2}(x, y) = (\theta(x), \theta(y))$. Так как неподвижные точки для данной перестановки совпадают с точками, у которых обе координаты неподвижны для θ, то

$$1 - d_H(\theta^{\otimes 2}, 1) = (1 - d_H(\theta, 1))^2$$

А значит $d_H(\theta^{\otimes 2}, 1) = 1 - (1 - d_H(\theta, 1))^2$. Но на этом можно не останавливаться и вместо $S_n \to S_{n^2}$ рассмотреть $S_n \to S_{n^k}$ отображающий θ в действующую на $\{1, 2, \ldots, n\}^k$ и определяемую аналогичной формулой перестановку $\theta^{\otimes k}$, и в этом случае мы получим:

$$d_H(\theta^{\otimes k}, 1) = 1 - (1 - d_H(\theta, 1))^k$$

и раз $(1 - d_H(\theta, 1)) < 1 - r(g) < 1$, то всегда можно подобрать такое достаточно большое k, чтобы $d_H(\theta^{\otimes k}, 1) > C$ было сколь угодно близко к 1. Ясно, что аналогичную процедуру мы можем проделать для всего конечного множества F, и в роли k в таком случае нужно взять максимум по всем степеням k для всех элементов из F.

Но вы справедливо возразите: что при переходе от отображения $G \to S_n$ к его композиции с гомоморфизмом $S_n \to S_{n^k}$ меняется расстояние Хэмминга не только для второго условия в лучшую сторону, но и для первого в худшую. Однако это не так страшно, потому что величина k зависит только от $r(g)$ и константы C, а потому она уже определена до того, как мы подбираем отображение $G \to S_n$, а потому мы можем подготовиться заранее - и вместо (F, ε)-почти гомоморфизма строить (F, ε')-почти гомоморфизм с настолько маленьким ε', чтобы после композиции с $S_n \to S_{n^k}$ оценка на расстояние в первом условии стала ε. Чуть более конкретно, если $d = d_H(\sigma(gh), \sigma(g)\sigma(h))$ и $d_{new} = d_H((\sigma(gh))^{\otimes k}, (\sigma(g))^{\otimes k}(\sigma(h))^{\otimes k})$, то:

$$d_{new} = 1 - (1 - d)^k < 1 - (1 - \varepsilon')^k \leq k\varepsilon' = \varepsilon$$

Поэтому если положить $\varepsilon' = \frac{\varepsilon}{k}$, то после перехода к $\sigma^{\otimes k}$ мы получим нужную оценку. Иными словами сформулированное выше определение будет эквивалентно определению, где $r(g)$ заменено, скажем, на $\frac{1}{2}$. Должен отметить, что определение с $r(g)$ более структурно и идейно правильное, лучше отражает природу софических групп, и с ним проще работать так как оно менее ограничительное, тогда как определение с конкретной константой проще воспринимается.

Если представить нашу софическую (а значит по определению счетную) группу в виде объединения $G = \bigcup\limits_n F_n$ возрастающей цепочки конечных множеств $F_n \subset F_{n+1}$,

то для $\varepsilon = \frac{1}{n}$ для некоторых k_n используя определение можно построить отображения $\sigma_n : G \to S_{k_n}$, для которых:

$$d_H(\sigma_n(gh), \sigma_n(g)\sigma_n(h)) \to 0$$

$$d_H(\sigma_n(g), 1) \geq r(g) \qquad \text{для } g \neq 1$$

последовательность σ_n, удовлетворяющая первому условию, называется *асимптотическим гомоморфизмом* (ну а если выполняется два условия, то говорят о *точным асимптотическом гомоморфизме*), и фактически асимптотический гомоморфизм - эта последовательность очень удачных почти гомоморфизмов. Хотя асимптотический гомоморфизм не является гомоморфизмом, и даже вообще говоря не является отображением в некоторое конкретное множество - есть конструкция, позволяющая смотреть на него как на гомоморфизм в некоторую хитрую группу: пусть как и раньше произведение симметрических групп будет множеством всевозможных наборов, а для суммы мы будем рассматривать ее "пополненную версию", идейно более близкую к сумме банаховых пространств:

$$\prod_n S_{k_n} = \{(\theta_n)_n \mid \theta_n \in S_{k_n}\}$$

$$\overline{\bigoplus_n} S_{k_n} = \{(\theta_n)_n \mid \theta_n \in S_{k_n} \text{ и } d_H(\theta_n, 1) \to 0\}$$

И тогда по нашим $\sigma_n : G \to S_{k_n}$ мы можем построить настоящий гомоморфизм:

$$G \to \prod_n S_{k_n} / \overline{\bigoplus_n} S_{k_n}$$

заданный как $g \mapsto [\sigma(g)]$, где $\sigma(g) = (\sigma_1(g), \sigma_2(g), \ldots)$, а $[\sigma(g)]$ - его образ в факторе под действием канонического эпиморфизма. Просто проверяется, что такое отображение является гомоморфизмом, потому что

$$d_H(\sigma_n(gh)(\sigma_n(h))^{-1}(\sigma_n(g))^{-1}, 1) = d_H(\sigma_n(gh), \sigma_n(g)\sigma_n(h)) \to 0$$

А значит $\sigma(gh)(\sigma(h))^{-1}(\sigma(g))^{-1} \in \overline{\bigoplus_n} S_{k_n}$, иными словами $\sigma(gh) = \sigma(g)\sigma(h)$ в факторе. Инъективность получается как раз из условия $d_H(\sigma_n(g), 1) \geq r(g)$ для $g \neq 1$ (поэтому мы ранее и говорили, что определение софических групп с $r(g)$ более естественно: так как софические группы нужно воспринимать как подгруппы такого универсального фактора, и инъективность вложения здесь означает отделимость от нуля последовательности $d_H(\sigma_n(g), 1)$ неким зависящим от g выражением, чтобы g не попал в $\overline{\bigoplus}$. И здесь излишне требовать универсальной для всей группы оценки). Также отмечу, что верно и обратное: что если $G < \prod_n S_{k_n} / \overline{\bigoplus_n} S_{k_n}$, то можно рассмотреть произвольный подъем до $\prod_n S_{k_n}$ (иными словами в каждом смежном классе выбрать представителя), и фактически получить отображение $\sigma = (\sigma_1, \sigma_2, \ldots) : G \to \prod_n S_{k_n}$, компоненты которого σ_n будут образовывать точный асимптотический гомоморфизм, ну и имея σ_n легко строить все необходимые для определения почти гомоморфизмы. Таким образом, мы получаем очень важное утверждение:

Утверждение
Счетная группа G софическая $\Leftrightarrow G \hookrightarrow \prod\limits_n S_{k_n}/\overline{\bigoplus\limits_n} S_{k_n}$.

Замечание:
Очень часто вместо факторизующего $\overline{\bigoplus\limits_n} S_{k_n}$ *рассматривают:*

$$\overline{\bigoplus_{\mathcal{U}}} S_{k_n} = \{(\theta_n)_n \mid \theta_n \in S_{k_n} \ \ и \ \lim_{n\to\mathcal{U}} d_H(\theta_n, 1) = 0\}$$

где расстояния Хэмминга $d_H(\theta_n, 1)$ *стремятся к нулю не в классическом смысле, а по некоторому ультрафильтру* $\mathcal{U}$. *Так как предел по ультрафильтру совпадает с классическим при условии существовании классического, то получаем:*

$$\overline{\bigoplus_n} S_{k_n} < \overline{\bigoplus_{\mathcal{U}}} S_{k_n}$$

Проводя точно такие же рассуждения, какие мы проводили и с фактором по классической сумме, мы получим, что софичность счетной группы G *эквивалентна* $G \hookrightarrow \prod\limits_n S_{k_n}/\overline{\bigoplus\limits_{\mathcal{U}}} S_{k_n}$. *Преимущество подхода с ультрафильтрами заключается в том, что в таком случае расстояние Хэмминга можно определить и между* $\tilde{\theta}, \tilde{\tau} \in \prod\limits_n S_{k_n}/\overline{\bigoplus\limits_{\mathcal{U}}} S_{k_n}$ *по формуле (где* θ *и* τ *это некоторые представители из смежных классов* $\tilde{\theta}$ *и* $\tilde{\tau}$ *соответственно):*

$$d_H(\tilde{\theta}, \tilde{\tau}) = \lim_{n\to\mathcal{U}} d_H(\theta_n, \tau_n)$$

которая очевидно не зависит от выбора представителей в смежных классах, потому что $\lim\limits_{n\to\mathcal{U}} d_H(a_n, b_n) = 0$ *для* a, b *из одного смежного класса; также напомню, что предел по ультрафильтру существует для любого ограниченной последовательности. Поэтому в данном случае на* G *возникает естественная связанная со структурой почти гомоморфизмов метрика. Одновременно и к плюсам и минусом можно отнести тот факт, что подгруппа* $\overline{\bigoplus\limits_{\mathcal{U}}} S_{k_n}$ *"больше"* $\overline{\bigoplus\limits_n} S_{k_n}$, *а потому соответствующий фактор будет "меньше", что дает более обременительное условие на софичность: проверка группы на софичность проходит сложнее, но если софичность группы дана в условии - то мы получаем больше информации про группу. К минусам такого подхода можно отнести то, что ультрафильтры неконструктивные и очень сложные, и лишают конструкции и доказательства возможности потрогать и прочувствовать их со всех сторон.*

Также отмечу, что может возникнуть естественное желание навести порядок с непонятной последовательностью $\{k_n\}$ и работать просто с $\prod\limits_n S_n$ - и на самом деле этого можно добиться. С этой целью можно заметить, что для $m < n$ существует естественное вложение $S_m < S_n$, индуцированное вложением $\{1, 2, \ldots, m\} \subset \{1, 2, \ldots, n\}$, иными словами для которого образ перестановки неподвижен на всех $i > m$; отмечу, что всегда можно добиться, чтобы последовательность $\{k_n\}$

была возрастающей: так как у почти гомоморфизма $G \to S_n$ всегда можно увеличить n, взяв композицию с гомоморфизмом $S_n \to S_{nm}$, действующему по правилу $\sigma \mapsto \sigma \times \dots \sigma$, иными словами, множество из nm разбивается на блоки по n элементов, и новая перестановка действует на каждом из таких блоков как σ. Замечу, что при таком подходе не меняется расстояние Хэмминга, так как не меняется доля сдвигаемых элементов - а потому новый почти гомоморфизм $G \to S_{nm}$ будет с теми же параметрами (если бы параметры были другие - все могло бы сломаться, так как вместе они уже могли бы не дать асимптотический гомоморфизм).

И опираясь на гомоморфизмы $S_m < S_n$ а также замечание, что $\{k_n\}$ можно сделать возрастающей, мы можем построить согласованный на прямых суммах инъективный гомоморфизм:

$$\pi : \prod_n S_{k_n} \hookrightarrow \prod_n S_n$$

Заданный формулой:

$$(a, b, c, \dots) \mapsto (1, 1, \dots, 1, a, a, \dots, a, b, b, \dots, b, c, c, \dots)$$

где каждая координата отображается описанным выше гомоморфизмом $S_m < S_n$, причем она множится до тех пор, пока n не станет достаточно большим, чтобы вместить следующую компоненту, более формально: i-ая компонента переходит в компоненты с номерами от k_i вплоть до $k_{i+1} - 1$.

Далее можно заметить, что при гомоморфизме $S_m < S_n$ расстояние Хэмминга уменьшается (так как добавляются дополнительные неподвижные точки для перестановки, уменьшая тем самым долю сдвигаемых), а потому из явного вида π довольно нетрудно заметить, что $x \in \overline{\bigoplus_n} S_{k_n} \quad \Leftrightarrow \quad \pi(x) \in \overline{\bigoplus_n} S_n$ (так как если $d_H(x_n, 1) \to 0$ то $d_H(\pi(x)_n, 1) \to 0$ из-за того что при $S_m < S_n$ уменьшается расстояние Хэмминга, с другой стороны если $d_H(x_n, 1) \nrightarrow 0$, то $d_H(\pi(x)_n, 1) \nrightarrow 0$ так как $d_H(\pi(x)_{k_n}, 1) = d_H(x_n, 1)$), а потому π индуцирует вложение даже на уровне факторов:

$$\prod_n S_{k_n} / \overline{\bigoplus_n} S_{k_n} \hookrightarrow \prod_n S_n / \overline{\bigoplus_n} S_n$$

Таким образом мы получаем, что счетная группа G является софической iff она допускает вложение в $\prod_n S_n / \overline{\bigoplus_n} S_n$, что не является принципиальным усилением ранее сформулированного аналогичного критерия с $\{k_n\}$, но сами идеи доказательства хорошо отражают дух работы с расстоянием Хэмминга, ну и плюс ко всему такое вложение эстетически выглядит лучше чем с непонятной последовательностью $\{k_n\}$.

Пример
Счетная остаточно конечная группа G является софической.

Мы помним, что остаточно конечные группы допускают вложение $G \hookrightarrow \prod\limits_n S_n$. Также есть хитрый трюк, который позволяет для некоторой последовательности $\{k_n\}$ построить вложение:

$$\prod_n S_n \hookrightarrow \prod_n S_{k_n} / \overline{\bigoplus_n} S_{k_n}$$

заданное формулой:

$$(a, b, c, d, \ldots) \mapsto (a, a, b, a, b, c, a, b, c, d, \ldots) \cdot \overline{\bigoplus_n} S_{k_n}$$

Закономерность, думаю, здесь более-менее понятна: фактически мы приписываем увеличивающиеся по размеру блоки друг другу, таким образом формируя последовательность в образе. Инъективность этого гомоморфизма будет достигаться за счет того, что в образе каждая компонента встречается бесконечное число раз. Беря композицию этих двух гомоморфизмов мы получаем вложение:

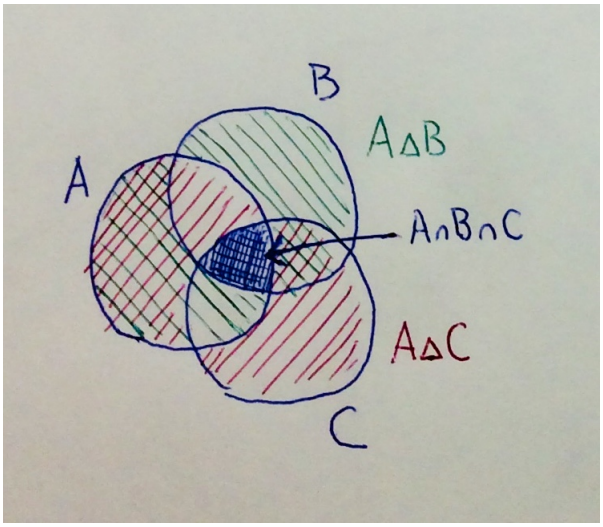
$$G \hookrightarrow \prod_n S_{k_n} / \overline{\bigoplus_n} S_{k_n}$$

Пример
Счетная аменабельная группа G является софической.

Рассмотрим последовательность Фёльнера $F_n \subset G$, и рассмотрим следующие отображения $\sigma_n : G \to S(F_n) = S_{|F_n|}$, заданные формулой:

$$(\sigma_n(g))(x) = \begin{cases} gx, & \text{если } gx \in F_n \\ \text{доопределим до биекции на оставшихся } x \end{cases}$$

Докажем, что эти σ_n вместе образуют необходимый для софичности асимптотический гомоморфизм. Заметим, что отображения $\sigma_n(gh)$ и $\sigma_n(g)\sigma_n(h)$ действуют левым умножением на множестве $F_n \cap (h^{-1}F_n) \cap (h^{-1}g^{-1}F_n)$ (где все фигурирующие перестановки не попадают в зону нашего хаотичного доопределения), а потому на этом множестве $\sigma_n(gh) = \sigma_n(g)\sigma_n(h)$ (в произведении $\sigma_n(g)\sigma_n(h)$ вторым применяется $\sigma_n(g)$, а потому его аргумент должен быть из F_n. Поэтому, чтобы перестановка $\sigma_n(h)$ не выкинула нас из нашего множества, в тройное пересечение мы включаем $h^{-1}F_n$). Рисуя диаграммы Эйлера также легко понять, что: $|A \cap B \cap C| \geq |A| - |A \triangle B| - |A \triangle C|$ (потому что черное пересечение, а также красная и зеленая симметрические разности вместе покрывают все A, причем даже с взаимными наложениями)



С учетом того, что на этом множестве обе перестановки совпадают, получаем, что различаться они могут только вне этого множества, а потому:

$$d_H(\sigma_n(gh),\sigma_n(g)\sigma_n(h)) \leq \frac{|F_n| - |F_n \cap (h^{-1}F_n) \cap (h^{-1}g^{-1}F_n)|}{|F_n|} \leq \frac{|F_n \triangle (h^{-1}F_n)|}{|F_n|} + \frac{|F_n \triangle (h^{-1}g^{-1}F_n)|}{|F_n|} \to 0$$

из определения фёльнеровской последовательности. Аналогично проверяется и второе условие точности полученного асимптотического гомоморфизма: так как в данном случае наоборот, $\sigma_n(g)$ действует как левый сдвиг на $F_n \cap (g^{-1}F_n)$ при $g \neq 1$, а потому там у нее не может быть неподвижных точек, а значит:

$$d_H(\sigma_n(g),1) \geq \frac{|F_n \cap (g^{-1}F_n)|}{|F_n|} \geq 1 - \frac{|F_n \triangle (g^{-1}F_n)|}{|F_n|} \to 1$$

опять из определения последовательности Фёльнера. Таким образом мы получаем доказывающее софичность вложение:

$$G \hookrightarrow \prod_n S(F_n)/\overline{\bigoplus_n} S(F_n)$$

$$g \mapsto (\sigma_1(g),\sigma_2(g),\sigma_3(g),\ldots) \cdot \overline{\bigoplus_n} S(F_n)$$

Замечания:

• *На самом деле класс софических групп намного шире, чем тот, что покрывается этими двумя примерами. К примеру, если объединить идеи этих двух упражнений, то можно показать, что счетные остаточно аменабельные группы являются софическими. Также если G является софической, а A - счетной аменабельной, то $G \rtimes A$ тоже является софической. На самом деле уже эти два факта покрывают настолько широкий класс групп, что нужно очень сильно постараться, чтобы найти группу в него не входящую. Более того, до сих пор остается открытым вопрос, существуют ли вообще в природе счетные группы, не являющиеся софическими. Причем главным претендентом на роль контрпримера является группа Хигмана*

$$H = \langle a,b,c,d \mid a^{-1}ba = b^2, b^{-1}cb = c^2, c^{-1}dc = d^2, d^{-1}ad = a^2 \rangle$$

потому что мы хорошо помним, что у этой группы большие проблемы с гомоморфизмами в конечные группы, и люди думают, что эти проблемы могут мигрировать и на почти гомоморфизмы. Вопрос софичности произвольной счетной группы является крайне значимым, так как софические группы связаны с очень многими сюжетами в математике.

• *В теории групп есть родственное к софичности понятие гиперлинейных групп, которые определяются дословно точно так же и лишь с заменой* S_n *на группу* U_n *унитарных матриц размера* $n \times n$*, а расстояние Хэмминга заменяется на* $\|U - V\|$*, где* $\|T\| = \sqrt{\tau(T^*T)}$ *есть норма Гильберта-Шмидта, а* τ *- нормализованный след. Софические группы являются автоматические гиперлинейными из-за существования гомоморфизма* $S_n \to U_n$*, отправляющего перестановку* θ *в соответствующий сдвиг* $T_\theta e_i = e_{\theta(i)}$*. И если софичность больше связана с алгоритмическими вопросами, то гипелинейность с вопросами структуры факторов фон Неймана. Так как условие гиперлинейности слабее условия софичности, то понятно дело, что до сих пор неизвестно ни одного примера и групп не являющихся гиперлинейными.*

==========

Задачи для самостоятельной работы

• *Является ли S_∞ остаточно конечной?*

• *Доказать, что если G софическая и $H < G$, то H тоже софическая.*

• *Привести пример счетной группы, не являющейся остаточно аменабельной (подсказка = простота).*

• *Не используя теорему Мескина доказать, что $B(1,2)$ является остаточно конечной.*

• *Не используя теорему Мескина доказать, что $B(3,5)$ не является остаточно конечной.*

• *Пусть G является остаточно конечной.*

1) Верно ли, что $G \rtimes \mathbb{Z}_n$ будет остаточно конечной для любого n?

2) Верно ли, что $G \rtimes \mathbb{Z}$ будет остаточно конечной?

• *Пусть G счетная остаточно аменабельная группа. Доказаться, что G софическая.*

• *Проверив, что группа Баумслага-Солитера $B(2,3)$ является остаточно разрешимой, убедиться в ее софичности.*