Глава 4. Группы и алгебры

Не имея намерения подменять полноценные учебные курсы, мы хотели бы рассказать о некоторых вопросах алгебры, существенно дополняющих те разделы алгебры и линейной алгебры, которые обычно рассказывают на первых курсах университетов. Далее мы дадим более подробные библиографические указания, но сразу хотели бы обратить внимание читателя на следующие замечательные учебники. Для более глубокого изучения теории групп мы рекомендуем книгу [24], а тем, кто только начинает свое знакомство с теорией групп, советуем замечательную книгу [1]. По конечномерным алгебрам мы ориентируемся на книгу [22], по алгебрам Ли отметим классический учебник [45], а по теории представлений — одну из самых полных (хотя и не простую) книгу [27].

§ 4.1. Графы Кэли

За более систематическим изложением отсылаем читателя к книге [36] и лекциям [28]. Тем, кто заинтересуется прикладными задачами связанными с графами Кэли, можем порекомендовать, например, работу [48].

Пусть $G = \langle X \rangle$ — группа, порожденная конечным набором элементов $X = \{x_1, \dots, x_n\}$. Отметим сразу, что группа может порождаться разными наборами элементов и граф Кэли при этом будет меняться. Ниже мы приведем некоторые примеры.

Задание группы через образующие и соотношения называют *копредставлением группы* и пишут $G = \langle X | R \rangle$.

Определение 4.1. Будем называть *графом Кэли* для данного копредставления группы $G = \langle X | R \rangle$ ориентированный граф, в котором вершины отождествлены с элементами группы, а ребра строятся следующим образом. Из вершины a в вершину b ведет ребро с меткой x_i, если $ax_i = b$. Будем называть его также ребром цвета x_i.

Сразу из определения становится ясен алгебраический смысл графа. А именно, возьмем вершины графа a, b и какой-нибудь непрерывный путь из a в b. Если мы выпишем метки ребер в том порядке в каком они встречаются, с учетом их направления (если мы проходим ребро по направлению, то пишем соответствующую ему метку x_i, а если против направления, то x_i^{-1}), мы получим такое слово (элемент группы) ω, что $a\omega = b$. При этом если мы в нашем пути не проходим одно и то же ребро два раза подряд, то слово у нас получится несократимым. В частности, если выбрать какой-нибудь замкнутый цикл и прочитать слово, которое на нем написано (учитывая направление стрелок), мы получим или соотношение, или следствие из соотношений.

Подчеркнем, что граф Кэли, конечно, зависит от системы порождающих. Ниже мы сформулируем теорему о том, как связаны графы Кэли для различных копредставлений одной группы.

Сразу отметим несколько очевидных свойств графа Кэли Γ:

• граф Γ связен;

• граф Γ вершинно-транзитивен, т. е. для любых двух вершин a, b существует автоморфизм f графа Кэли, переводящий вершину a в вершину b и сохраняющий метки ребер.

Задача 4.2. Постройте граф Кэли для аддитивной группы целых чисел $\mathbb{Z}$.

Решение. Построение графа Кэли для группы $\mathbb{Z} = \langle 1 \rangle$ не составляет труда, поскольку образующая с меткой «1» просто соединяет соседние целые числа. Гораздо интереснее посмотреть на граф Кэли с образующими $x = 2$, $y = 3$.

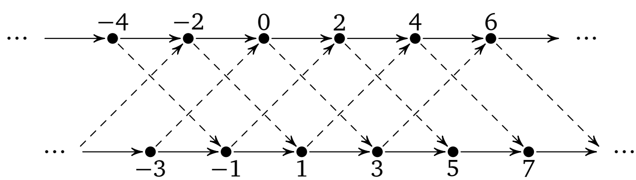

Рис. 1. Группа $\mathbb{Z} = \langle 2, 3 \rangle$

Отметим, что если «прочитать» слова, написанные на гранях, то мы получим соотношения $xy = yx$ и $x^3 \times y^{-2} = 0$, что соответствует понятному соотношению $2 \times 3 - 3 \times 2 = 0$. □

Комментарий. Интересным вопросом является следующий. Может ли быть графом Кэли некоторой группы дерево? Первым примером является, конечно, группа целых чисел. В общем же случае группа, граф Кэли которой — дерево, называется свободной. Термин «свобода» нужно понимать не в политическом смысле, а как свободу от соотношений между элементами группы. Такие группы являются крайне важными объектами в комбинаторной теории групп.

Далее при изображении графов мы будем игнорировать направление ребер в случаях, когда ориентация легко восстанавливается. Также кратные ребра (т. е. когда соответствующая образующая имеет порядок 2) обычно рисуют как одно ребро. Именно в этом смысле нужно понимать следующий граф Петерсена, где короткие ребра понимаются как кратные.

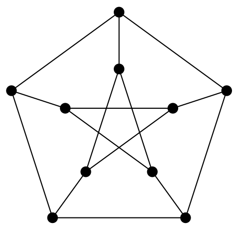

Рис. 2. Граф Петерсена

Задача 4.3. Докажите, что граф Петерсена является вершинно-транзитивным, но не является графом Кэли ни для какой группы.

Решение. Понятно, что такой граф задается образующими x и a, где $x^5 = a^2 = e$. С учетом того, что в графе 10 вершин, можно было бы перебрать все группы из 10 элементов и доказать, что ни у одной из них нет такого графа Кэли. Но мы пойдем более «технологичным» путем. Ясно, что ориентацию вершин можно задать несколькими способами, однако решение будет идентичным. Одна из ориентаций дает нам соотношения $axa = x^3$ и $x = ax^2a$. Отсюда получаем, подставляя одно из них в другое, что $a^2x^2a^2 = x^3$, значит, так как $a^2 = e$, мы имеем $x^2 = x^3$, и потому $x = e$, чего быть не может, поскольку в группе должно быть 10 элементов. □

В дальнейшем нам пригодятся такие важные характеристики графов, как расстояние и диаметр.

Определение 4.4. Будем называть *расстоянием* между вершинами a и b графа длину минимального пути (без учета ориентации ребер) из a в b. Максимальное расстояние между вершинами для конечных графов будем называть *диаметром* графа.

Задача 4.5. Дан деревянный куб с пронумерованными вершинами. Какого минимального количества поворотов на $\frac{\pi}{2}$ и $\frac{2\pi}{3}$ вокруг осей вращения куба достаточно, чтобы получить из одного положения другое?

Решение. Начнем с того, что группа вращений куба изоморфна группе перестановок S_4. В самом деле, любая перестановка больших диагоналей куба задает некоторый поворот, и обратно, любой поворот задается некоторой перестановкой диагоналей. Интересующие нас повороты — это, по сути, образующие группы S_4 порядка 4 (повороты на $\frac{\pi}{2}$) и 3 (повороты на $\frac{2\pi}{3}$).

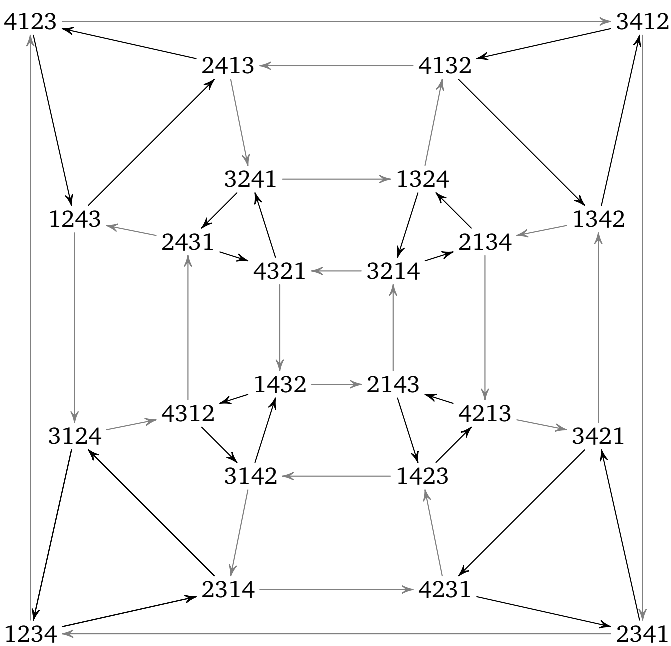

Рис. 3. Граф Кэли для группы S_4

Итак, нашу задачу можно переформулировать следующим образом. Каково минимальное (по ребрам) расстояние между двумя произвольными вершинами графа Кэли с указанными образующими? В силу вершинной транзитивности нашего графа достаточно проверять расстояние от вершины, соответствующей тождественной перестановке. В данном случае граф Кэли достаточно несложен и легко рисуется, откуда получаем, что минимальное необходимое количество поворотов равно 3. □

Комментарий. На самом деле конструкция, предложенная нами в предыдущей задаче, очень важная. По сути, граф Кэли дает нам возможность найти алгоритм (и найти оценку необходимого количества шагов) поиска для двух данных элементов группы a, b слова минимальной длины ω, для которого $a\omega = b$. Эти соображения оказываются чрезвычайно важными, например, в теории алгоритмов (ниже мы укажем приложение к задаче сортировки массива). Но есть применения и, скажем, к головоломкам. Так, *числом бога* для головоломки называют минимальное необходимое количество действий, достаточных для того, чтобы решить головоломку из любого изначального состояния. Например для кубика Рубика это число равно 20. Доказательство этого факта опирается на серьезные вычисления, которые стали возможными совсем недавно, с появлением суперкомпьютеров. Подробнее об этом можно прочитать в [49]. Хочется отметить, что вычисление диаметра графа Кэли оказывается нетривиальной задачей даже для «детского» кубика $2 \times 2 \times 2$, про что можно прочитать в работе [48].

Задача 4.6. Найдите диаметр графа Кэли группы S_n, порожденной транспозициями вида $(i\ i{+}1)$.

Решение. В решении нам, конечно, нужно проверить и корректность условия, а именно показать, что любая перестановка раскладывается в произведение транспозиций указанного вида. Проверку того, что ни одну из транспозиций убрать нельзя, оставляем читателю в качестве упражнения.

Пусть имеется перестановка $\sigma \in S_n$. Будем называть *числом беспорядков* количество таких упорядоченных пар (i, j), $i < j$, что $\sigma(i) > \sigma(j)$. Понятно, что умножение на транспозицию вида $(i\ i{+}1)$ меняет число беспорядков на 1. Если перестановка σ нетривиальна, то найдется такая пара $(i, i+1)$, что $\sigma(i) > \sigma(i+1)$. Заметим, что у перестановки $\sigma \circ (i\ i{+}1)$ количество беспорядков на 1 меньше, чем у перестановки σ. Мы всегда можем повторить ту же процедуру, если количество беспорядков не нулевое. По индукции получаем, что в результате мы сведем все к тождественной перестановке. Теперь вычислим максимальное количество необходимых действий. Больше всего беспорядков в перестановке вида $\sigma(j) = n - j$, их $n(n-1)/2$, что и является диаметром графа Кэли. □

Комментарий. Внимательный читатель сразу поймет, что диаметр такого графа Кэли — это не что иное, как максимальное число шагов в сортировке «пузырьком» массива из n элементов. Конечно, подобная интерпретация годится и для других алгоритмов. Таким образом, известный вопрос о количестве минимально необходимых операций для сортировки массива сводится к вопросу поиска минимального диаметра графа Кэли в зависимости от выбранной системы порождающих. Разумеется, мы тут полностью игнорируем такие вопросы, как количество необходимой памяти и разная затратность операций. За соответствующими деталями отсылаем читателя к специализированной литературе.

Разговаривая о графах Кэли, нельзя не упомянуть и некоторые их геометрические свойства. Например, в случае конечных групп планарными являются только графы конечных подгрупп группы SO(3) (теорема Машке [50]). Пример конечной группы с непланарным графом Кэли предлагаем читателю привести самостоятельно. Интерес представляет и наличие в графе гамильтонова цикла, т. е. такого цикла, который проходит по всем вершинам ровно один раз. Группы, в которых есть гамильтонов цикл, мы будем называть гамильтоновыми.

Задача 4.7. Докажите, что у группы диэдра D_n есть минимальный граф Кэли, который является гамильтоновым.

Под минимальным мы понимаем граф для системы образующих, из которой нельзя ничего убрать.

Решение. Для решения достаточно подобрать удобную систему образующих. Выберем естественную систему образующих из симметрии τ и поворота φ многоугольника на угол $\frac{2\pi}{n}$. Тогда граф Кэли представляет собой два многоугольника, у которых последовательно соединены вершины, т. е. выполняется (легко проверяемое) соот-

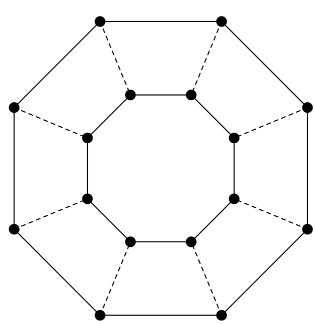

Рис. 4. Группа диэдра D_8

ношение $\tau\varphi\tau=\varphi^{-1}$. Так что гамильтонов цикл легко предъявить:

$$\varphi \to \ldots \to \varphi^n = \mathrm{id} \to \tau \to \tau\varphi \to \ldots \to \tau\varphi^{n-1} \to \varphi,$$

что и завершает решение задачи. □

Комментарий. Легко придумать и другие гамильтоновы циклы в таком графе. Однако если взять группу перестановок S_n, то задача становится уже менее простой. Тем не менее отметим, что если породить группу перестановок транспозицией и циклом максимальной длины, то гамильтонов цикл также может быть построен ([51], лемма 3). В общем же случае до сих пор неизвестно, каждый ли граф Кэли даже для группы перестановок S_n содержит в себе гамильтонов цикл (это предположение называется гипотезой Ловаса). Впрочем, известно, что при $|G| \to \infty$ вероятность существования гамильтонова цикла стремится к единице. Но также известно, что вершинной транзитивности для существования гамильтонова цикла недостаточно. Например, упомянутый нами выше граф Петерсена гамильтонова цикла в себе не содержит.

Задача 4.8. Докажите, что если у графов групп $A=\langle x_i\rangle$, $B=\langle y_j\rangle$ есть графы Кэли с гамильтоновым циклом, то и у графа группы $A\times B$ тоже.

Решение. Для удобства будем обозначать элементы группы A через a_i, и пусть гамильтонов путь имеет вид $e=a_0 \to a_1 \to \ldots \to a_n \to e$, аналогично для группы B. Поясним, как устроен граф Кэли для $A\times B$. Между вершинами (a, b) и (a', b') имеется ребро с меткой (x_i, y_j), если $ax_i=a'$, $by_j=b'$. В таком случае с учетом наших обозначений у нас будут ребра между (a_i, b_j) и $(a_{i'}, b_{j'})$, если $|i-i'|+|j-j'|=1$.

Понятно, что при фиксированном $b\in B$ множество элементов вида (a, b) отождествляется с элементами группы A и в таком «слое» у нас будет гамильтонов цикл. Это и дает ключ к построению гамильтонова цикла во всей группе:

$$\begin{aligned}(a_0, b_0) \to (a_1, b_0) \to \ldots \to (a_n, b_0) \to (a_n, b_1) \to&\\ \to (a_{n-1}, b_1) \to \ldots \to (a_n, b_n) \to (a_0, b_0).&\end{aligned}$$

Отметим, что «склеивать» циклы можно и другими способами. □

Комментарий. Отсюда, конечно, получается, что, например, в абелевых группах (кроме «патологического» случая группы $\mathbb{Z}_2$) обязательно есть граф Кэли с гамильтоновым циклом. Можно доказать, что на самом деле любой граф Кэли для абелевой группы будет гамильтоновым. Подробнее о гамильтоновых путях и циклах в графах Кэли можно прочесть, например, в работе [51].

§ 4.2. Кватернионы

Кватернионы — очень интересный математический объект, и, кроме того, они имеют многочисленные применения в физике. О романтической истории открытия кватернионов (и других алгебр с делением) можно прочитать, например, в работе [6]. Далее мы опишем применение кватернионов к задаче описания вращений трехмерного пространства (см. с. 182 и далее). Заинтересовавшемуся читателю сразу порекомендуем прочитать книги [26, § 4], [47, § 8], а также брошюры [2], [44] и книгу [22].

Напомним (см., например, [13]), что *алгебра кватернионов* $\mathbb{H}$ является алгеброй над $\mathbb{R}$ с базисом $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ со следующей таблицей умножения:

$\times$	$\mathbf{1}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	$-\mathbf{1}$	$\mathbf{k}$	$-\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	$-\mathbf{1}$	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	$-\mathbf{1}$

(61)

Таким образом, $\mathbf{1}$ — «обычная» единица (нейтральный элемент относительно умножения). Из соотношений (61) следует, что данная алгебра ассоциативна[1], но не коммутативна; более того, любой ее ненулевой элемент имеет мультипликативный обратный, т. е. $\mathbb{H}$ — *алгебра с делением* (= некоммутативное поле, называемое также *телом*).

Отметим, что кватернионы дают простой, но нетривиальный пример неабелевой группы.

Задача 4.9. Докажите, что $\mathbb{Q}_8 := (\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}, \times)$ является группой, и постройте ее граф Кэли.

Решение. Во-первых, из соотношений (61) следует, что множество $\mathbb{Q}_8$ замкнуто относительно операции умножения. Во-вторых, свойство ассоциативности для каждого набора из трех элементов легко проверяется непосредственно с помощью соотношений (61) (или

[1] Заметим, что ассоциативность умножения в алгебре следует из ассоциативности умножения базисных векторов.