Лекция 10
Группы

▷Автоморфизмы и симметрии ▷Групповой закон композиции ▷Симметрические группы ▷Группы Галуа ▷Группы многогранников ▷Смежные классы и теорема Лагранжа ▷Действие группы на множестве: формула для длины орбиты ▷Фактор-группы, нормальные подгруппы и строение гомоморфизмов ▷Цикловой тип подстановки ▷Строение групп $\mathfrak{S}_3$, $\mathfrak{S}_4$, $\mathfrak{S}_5$, $\mathfrak{A}_3$, $\mathfrak{A}_4$, $\mathfrak{A}_5$ ▷Простота знакопеременных групп $\mathfrak{A}_n$ с $n \geq 5$

§1. Что такое группа

Все познаётся в сравнении, и основным источником информации о математических объектах является исследование их взаимодействия между собой. Если мы рассматриваем множества, наделённые той или иной структурой, то их взаймодействия друг с другом — это отображения из одних в другие, сохраняющие эту структуру. Изучать такие взаймодействия можно по двум направлениям: выяснять внутреннее устройство каждого отдельно взятого отображения, либо описать строение всего множества взаймодействий, рассматривая его как некий новый математический объект. Первую возможность демонстрируют теоремы о гомоморфизмах полей и колец, доказанные нами в первых лекциях. В этой лекции мы обсудим вторую возможность.

1.1. Эндоморфизмы и симметрии. Сразу ясно, что множество отображений наделено естественной алгебраической структурой. А именно, последовательно выполняя два отображения:

$$f\colon X \longrightarrow Y \quad \text{и} \quad g\colon Y \longrightarrow Z$$

мы получаем новое отображение $g \circ f : X \longrightarrow Z$, называемое *композицией* f и g (обратите внимание на то, что *первое* из двух последовательно выполнямых отображений в обозначении $g \circ f$ записано *справа*). Операция композиции, очевидно, определена не для любых пар (f, g), но уж если определена, то ассоциативна: $(h \circ g) \circ f = h \circ (g \circ f)$, хотя и не коммутативна. Мы уже встречались с подобной ситуацией, когда изучали алгебру матриц (что не удивительно, ибо матрицы представляют собой лишь удобное алгебраическое обозначение для *линейных отображений* векторных пространств и модулей).

Задача 10.1. Придумайте пример двух некоммутирующих отображений из некоторого множества X в себя.

Если ограничиться рассмотрением одного единственного объекта X,то композиция уже будет определена для любых $f, g : X \longrightarrow X$. Множество всех отображений из X в себя (сохраняющих алгебраическую структуру на X, буде таковая имеется) наазывается *полугруппой эндоморфизмов* объекта X и обозначается $\mathrm{End}(X)$. Взаимно-однозначные эндоморфизмы $f : X \longrightarrow X$ называются *автоморфизмами* или *симметриями* объекта X и их совокупность (группа) обозначается $\mathrm{Aut}\,(X)$.

Множество симметрий отражает взаймодействие объекта X самого с собой, т. е. его «внутренний характер», а потому является важнейшим источником информации об X. Способы судить об X глядя на $\mathrm{Aut}\,(X)$ называются *соображениями симметрии*. С древнейших времён они имеют статус наиболее изящных среди физических и математических рассуждений. Говоря по-учёному, свойства X адекватно кодируются алгебраической структурой на $\mathrm{Aut}\,(X)$. Изучению этой структуры и будет посвящена настоящая лекция. Прежде всего заметим, что ввиду взаимной однозначности у каждой симметрии $X \xrightarrow{f} X$ имеется *обратная симметрия* $X \xleftarrow{f^{-1}} X$.

> Задача 10.2. Докажите, что если X является кольцом (или модулем) и $X \xrightarrow{f} X$ является взаимно-одноэначным гомоморфизмом, то обратное отображение также будет гомоморфизмом.

Множества симметрий с первой половины XIX века стали называть *группами*. Понятие абстрактной группы возникло в XX веке и служит для аксиоматизации алгебраических свойств групп симметрий (которые в XIX веке не считали нужным уточнять, ибо они были всем очевидны из контекста.)

1.2. Определение. *Группой называется всякое множество G, на элементах которого определена бинарная операция $G \times G \longrightarrow G : \quad (f, g) \longmapsto fg$, называемая композицией (а в последнее время чаще – умножением), удовлетворяющая аксиомам:*

(аксиомы группового закона композиции)

(i) ассоциативность:

$$(fg)h = f(gh) \qquad \forall f, g, h$$

(ii) существование единицы (тождественного отображения):

$$\exists e \in G : \quad eg = ge = g \quad \forall g \in G$$

(iii) существование обратного:

$$\forall g \in G \quad \exists g^{-1} : \quad gg^{-1} = g^{-1}g = e$$

> Задача 10.3. Докажите, что единичный элемент единственен, а обратный элемент g^{-1} однозначно определяется по g.

1.3. Определение. *Абелевой группой называется всякая группа G, в которой композиция коммутативна: $fg = gf \quad \forall f, g \in G$.*

В этом случае в аксиомах (ii) и (iii) можно отбросить левое равенство, и аксиомы композиции превратятся в аксиомы сложения векторов. Поэтому операцию в абелевой группе обычно обозначают знаком «+».

1.4. Определение. *Отображение групп $\varphi : G_1 \longrightarrow G_2$ называется гомоморфизмом групп, если в группе G_2 имеем $\varphi(gh) = \varphi(g)\varphi(h) \quad \forall g, h \in G_1$. Эпи-, моно- и изоморфизмы определяются как обычно.*

§2. Примеры групп

2.1. Подгруппы. Как уже говорилось, группы чаще всего реализуются как подмножества в множестве $\mathrm{Aut}\,(X)$ всех взаимно-однозначных отображений того или иного множества X в себя. Очевидно, что $\mathrm{Aut}\,(X)$ само является группой. Для того чтобы подмножество H группы G составляло группу относительно имеющейся в G композиции необходимо и достаточно, чтобы $\forall h \in H$ обратное отображение h^{-1} также лежало в H и чтобы $\forall h_1, h_2 \in G$ их композиция $h_1 h_2 \in G$. Такие $H \subset G$ называются *подгруппами* в G. Как всегда, эти два условия можно заменить одним.

Задача 10.4. Докажите, что подмножество H в группе G тогда и только тогда составляет группу относительно композиции, имеющейся в G, когда

$$h_1 h_2^{-1} \in H \qquad \forall h_1, h_2 \in H\ .$$

2.2. Симметрическая группа $\mathfrak{S}_n \stackrel{\text{def}}{=} \mathrm{Aut}\,(\{1, 2, \dots, n\})$ — это группа всех взаимно-однозначных отображений множества из n элементов[1] в себя. Каждое такое отображение осуществляет попросту перестановку чисел в строчке $(1, 2, 3, \dots, n)$, поэтому $\mathfrak{S}_n$ иногда называют *группой перестановок*.

Мы уже встречались с группой $\mathfrak{S}_n$ в лекции 6 при исследовании полилинейных косых форм. Эта группа также незримо присутствовала в лекции 8, когда мы занимались симметрическими многочленами. Поскольку перенумерацию переменных в многочлене $f(x_1, \dots, x_n)$ можно воспринимать как результат подстановки в f вместо набора переменных $(x_1, \dots, x_n)$ нового набора переменных $(y_1, \dots, y_n)$, полученного из него перестановкой букв, группу $\mathfrak{S}_n$ называют также *группой подстановок* n аргументов.

Задача 10.5. Вспомните, колько всего подстановок имеется в $\mathfrak{S}_n$.

Ответ: $n!$.

2.2.1. Предложение. *Любая конечная группа из n элементов допускает гомоморфное вложение в $\mathfrak{S}_n$.*

Доказательство. Занумеруем элементы группы G и сопоставим каждому элементу $h \in G$ взаимно-однозначное отображение множества этих номеров на себя, индуцированное умножением на h: номер k, соответствующий элементу $g \in G$, переведем в номер элемента hg. Отображение номеров будет взаимно-однозначным, поскольку взаимно-однозначным будет отображение $g \mapsto hg$ (ибо $hg_1 = hg_2$ после умножения слева на h^{-1} превращается в $g_1 = g_2$). Построенное отображение $G \longrightarrow \mathfrak{S}_n$, очевидно, является гомоморфизмом и инъективно, поскольку если h_1 и h_2 одинаково переставляют элементы G, то в частности и $h_1 e = h_2 e$, т. е. $h_1 = h_2$.
□

Задача 10.6. Докажите что любая абстрактная группа изоморфна некоторой подгруппе группы всех взаимно-однозначных отображений подходящего множества X в себя.

2.3. Группа Галуа. Пусть $f \in \mathbb{Q}[x]$ - неприводимый многочлен и $K \supset \mathbb{Q}$ - поле разложения f (т. е. поле, в котором f раскладывается на линейные множители, и которое вкладывается в любое другое такое поле). Поле K можно получить, последовательно присоединяя к $\mathbb{Q}$

[1] в качестве которых обычно берут первые n натуральных чисел

недостающие корни f (см. лекцию 3). Группа автоморфизмов поля K называется *группой Галуа* многочлена f над $\mathbb{Q}$ и обозначается $\mathrm{Gal}(f/\mathbb{Q})$ или $\mathrm{Gal}(K/\mathbb{Q})$ или просто $\mathrm{Gal}(f)$.

Пусть $(\vartheta_1, \ldots, \vartheta_n)$ — множество всех (автоматически попарно-различных) корней f в K. Любой элемент из K может быть выражен в виде значения некоторого многочлена $F(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ на наборе $(\vartheta_1, \ldots, \vartheta_n)$, поэтому действие любого автоморфизма $\sigma : K \longmapsto K$ из группы Галуа однозначно опредеыяется тем, как он действует на ϑ_i. С другой стороны, всякий автоморфизм поля K действует тождественно на простом подполе $\mathbb{Q} \subset K$, в частности, переводит в себя коэффициенты f, а стало быть отображает корни f в корни f. Следовательно, группа Галуа $\mathrm{Gal}(f)$ отождествляется с подгруппой в группе $\mathfrak{S}_n$ перестановок корней $(\vartheta_1, \ldots, \vartheta_n)$.

Группы Галуа были впервые рассмотрены Лагранжем в 1770г для того, чтобы описать такие полиномиальные выражения от $x_1, \ldots, x_n$, значения которых на корнях $(\vartheta_1, \ldots, \vartheta_n)$ данного многочлена лежат в $\mathbb{Q}$. Если значение $F(\vartheta_1, \ldots, \vartheta_n) \in \mathbb{Q}$, то (по определению группы Галуа) оно не меняется при всех перестановках корней ϑ_i из группы Галуа. *Теорема Лагранжа* утверждает, что верно и обратное:

2.3.1. Предложение. (Теорема Лагранжа) *Если функция не меняет значение при всех перестановках из группы Галуа, то это значение рационально.*

2.3.2. Комментарий: Из основной теоремы о симметрических многочленах тривиально следует, что таковыми заведомо являются функции от $\vartheta_1, \ldots, \vartheta_n$, инвариантные относительно *вообще всех* перестановок ϑ_i, ибо такие функции выражаются через коэффициенты уравнения. Теорема Лагранжа является более тонким фактом, поскольку устанавливает рациональность не только симметрических функций, но функций, инвариантных относительно, вообще говоря, меньшей, группы Галуа. Поэтому равенство $F(\vartheta_1, \ldots, \vartheta_n) = q \in \mathbb{Q}$ для такой функции F означает наличие *нетривиального* соотношения между корнями, не вытекающего из теоремы Виета. Ясно, что чем меньше группа Галуа, тем больше у нас таких соотношений, и тем проще решать уравнение. И наоборот, уравнения, группа которых совпадает с $\mathfrak{S}_n$, максимально трудны для решения, ибо между их корнями нет никаких соотношений, кроме вытекающих из теоремы Виета.

2.3.3. Набросок доказательства теоремы Лагранжа. В терминах полей теорема Лагранжа утверждает, что если элемент $\alpha \in K$ инвариантен относительно всех автоморфизмов K, то $\alpha \in \mathbb{Q}$. Чтобы убедиться в этом, надо уметь строить для каждого $\alpha \notin \mathbb{Q}$ автоморфизм поля K, сдвигающий α. Мы наметим доказательство в серии задач:

Задача 10.7. Докажите, что K конечномерно как векторное пространство над $\mathbb{Q}$.
Указание: вспомните явное построение K.

Задача 10.8. Докажите, что все элементы $\alpha \in K \setminus \mathbb{Q}$ алгебраичны над $\mathbb{Q}$ и имеют степень ≥ 2.
Указание: векторы $1, \alpha, \alpha^2, \ldots$ не могут быть линейно независимы, ибо $\dim(K) < \infty$.

Задача 10.9. Пусть $\alpha \in K \setminus \mathbb{Q}$ и $f \in \mathbb{Q}[x]$ — минимальный многочлен для α. Докажите, что отображение, переводящее α в любой другой корень f, единственным образом продолжается до автоморфизма поля $\mathbb{Q}[\alpha]$ (наименьшего подполя в K , содержащего α).

Задача 10.10. Докажите, что автоморфизм из предыдущей задачи можно продолжить с $\mathbb{Q}[\alpha]$ на всё поле K.
Указание: надо вместо расширения $K \supset \mathbb{Q}$ рассмотреть расширение $K \supset \mathbb{Q}[\alpha]$ и

проделать с ним всё то же самое.

2.4. Группы многогранников. Отображение пространства на себя, сохраняющее расстояние между точками, называется *движением*. Очевидно, движения составляют подгруппу в группе всех взаимно-однозначных отображений $\mathbb{R}^3$ на себя. Движения бывают *собственные* и *несобственные*, смотря по тому, переводят они стандартно ориентированный базис в $\mathbb{R}^3$ в стандартный, или в нестандартный (см. рис.3 на стр. 82). Движение F тогда и только тогда является собственным, когда его можно непрерывно продеформировать в тождественное, т. е. построить такое непрерывно зависящее от $t \in [0,1]$ семейство движений $F(t)$, что $F(0) =$ тождественmому движению, а $F(1) = F$. Собственные движения составляют подгруппу в группе движений. Движения (соответственно собственные движения), переводящие в себя фиксированную фигуру $\mathfrak{F} \subset \mathbb{R}^3$ составляют подгруппу в группе всех движепий (соответственно всех собственных движений). Она называется *группой фигуры* $\mathfrak{F}$ (соответственно *собственной группой фигуры* $\mathfrak{F}$)

2.4.1. Пример. Группа самосовмещений правильного плоского n-угольника в пространстве называется *группой диэдра порядка* $2n$ и обозначается $Д_n$. Она состоит из $2n$ элементов: n поворотов на углы $2\pi k/n \quad (k = 0, 1, \dots n-1)$ и n симметрий (т. е. поворотов на 180° вокруг прямых в пространстве). При чётном n оси симметрий бывают двух типов: соединяющие противоположные вершины и соединяющие середины противоположных рёбер. При нечётном n все оси одинаковы (см. рис.1)

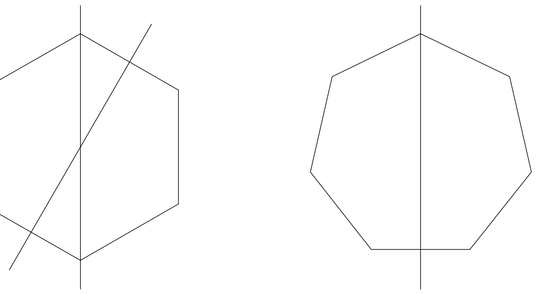


Рис. 1. Геометрически различные оси диэдров.

2.4.2. Пример. Группа собственных самосовмещений правильного тетраэдра состоит из 12 вращений вокруг его центра: тождественного самосовмещения, восьми поворотов на $\pm 120°$ вокруг осей, проходящих через вершину и центр противоположной грани (см. рис.2), и трёх поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер. Никаких других собственных симметрий нет.

В самом деле, зафиксируем какие-либо четыре вращения t_1, t_2, t_3, t_4, переводящие вершину 1 соответственно в вершины 1, 2, 3 и 4, и пусть s_0, s_1, s_2 – это три (с учётом тождественного) вращения тетраэдра, сохраняющие вершину 1 на месте. Поскольку движение вполне определяется тем, куда оно переводит вершины, каждое вращение можно единственным способом записать в виде $g = s_i t_j$, так что мы действительно имеем ровно $3 \cdot 4 = 12$ вращений. Нетрудно дать явное описание всех подгрупп группы тетраэдра. Ясно, что она содержит 4 подгруппы, состоящие каждая из трёх (с учётом тождественного) поворотов вокруг прямой, проходящей через вершину и центр противоположной грани. Кроме того, три поворота на 180° вокруг прямых, соединяющих середины противоположных ребер, вместе с тождественным преобразованием составляют подгруппу из 4 элементов (убедитесь в этом!). Она называется *квадратичной группой Клейна*.

Задача 10.11. Убедитесь, что других подгрупп в группе тетраэдра нет.

Задача 10.12. Сколько вращений имеется в собственной группе куба?

Задача 10.13. Сколько движений в полной группе тетраэдра?

2.5. Разбиение группы на смежные классы. Пусть $H \subset G$ - подгруппа в группе. Тогда мы можем рассмотреть множество всех «параллельных переносов» gH подгруппы H на всевозможные $g \in G$. Множество

$$gH \stackrel{\text{def}}{=} \{gh:\, h \in H\}$$

называется *левым смежным классом* группы G по подгруппе H. Смежные классы составляют разбиение G на *непересекающиеся подмножества*. Действительно, если $g_1H \bigcap g_2H \neq \emptyset$ и $g_1h_1 = g_2h_2$ для некоторых $h_1, h_2 \in H$, то $g_1 = g_2h_2h_1^{-1}$, а т. к. H – подгруппа, то $h_2h_1^{-1} = h \in H$. Поэтому $g_1 \in g_2H$, а стало быть $g_1H \subset g_2H$. По аналогичным причинам имеется и обратное включение $g_2H \subset g_1H$, так что $g_1H = g_2H$, если только $g_1H \bigcap g_2H \neq \emptyset$.

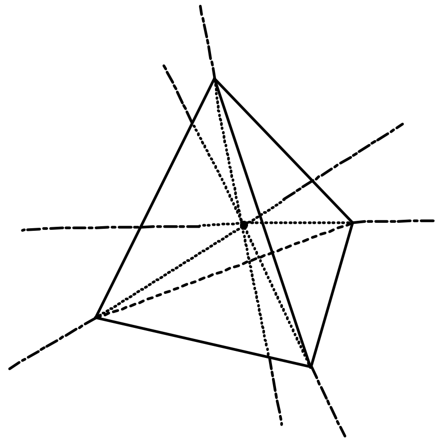


Рис. 2. Оси третьего порядка в правильном тетраэдре

Кроме того, все смежные классы состоят из "одинакового числа элементов", а точнее говоря, умножение на g слева: $h \mapsto gh$ задает взаимно-однозначное соответствие между H и gH (обратным к нему будет умножение элементов gH слева на g^{-1}). Следствием такого разбиения G на непересекающиеся биективно соответствующие друг другу смежные классы является

2.6. Теорема. (Теорема Лагранжа.) *Число элементов конечной группы G делится нацело на число элементов любой её подгруппы $H \subset G$.*

2.7. Порядок и индекс. Число элементов в конечной группе G называется *порядком группы* и обозначается $|G|$. Число смежных классов группы G по подгруппе H называется *индекспм подгруппы* H в G и обозначается $|G:H|$.

2.7.1. Следствие. *Если $|G| < \infty$, то $|H| \cdot |G:H| = |G|$ $\forall$ подгруппы $G \subset H$.*

2.8. Циклические группы. Произведения $\underbrace{\varrho \cdot \varrho \cdot \dots \cdot \varrho}_{n}$ и $\underbrace{\varrho^{-1} \cdot \varrho^{-1} \cdot \dots \cdot \varrho^{-1}}_{n}$ обозначаются через ϱ^n и ϱ^{-n} соответственно. Группа G называется *циклической*, если все её элементы являются целыми степенями некоторого одного элемента $\varrho \in G$, называемого *образующей*.

Множество всех степеней ϱ^n, $n \in \mathbb{Z}$), произвольного элемента ϱ в любой группе составляет циклическую подгруппу, называемую *циклической подгруппой, порождённой* ϱ. Если порядок этой группы конечен, то он называется также *порядком элемента* ϱ (и сам ϱ называется в этом случае *элементом конечного порядка*).

Задача 10.14. Докажите, что порядок элемента $g \in G$ можно иначе описать как наименьшее $n \in \mathbb{N}$, такое что $g^n = e$.

2.8.1. Следствие. *Всякий элемент конечной группы имеет конечный порядок и этот порядок делит порядок группы.*

2.8.2. Следствие. *Группа простого порядка не содержит нетривиальных подгрупп (отличных от $\{e\}$ и от самой себя).*

Задача 10.15. Докажите, что всякая циклическая группа порядка n изоморфна аддитивной группе кольца $\mathbb{Z}/n\mathbb{Z}$ (в частности все её элементы представляются *натуральными* степенями образующей.

§3. Действие группы на множестве

Ситуация, когда абстрактная группа G выступает как группа отображений какого-либо множества X в себя, формализуется так:

3.1. Определение. *Действием группы G на множестве X называется отображение*

$$G \times X \longrightarrow X \ : \quad (g, x) \mapsto g(x) \ ,$$

удовлетворяющее условиям: $gh(x) = g(h(x)) \quad \forall\, g, h \in G$ *и* $e(x) = x \quad \forall\, x \in X$.

3.2. Терминология. Поскольку каждый элемент $g \in G$ обладает обратным, все отображения $X \stackrel{g}{\longrightarrow} X$, индуцированные действием, являются взаимно-однозначными. Поэтому действие группы G на множестве X можно иначе описать как гомоморфизм $G \longrightarrow \operatorname{Aut} X$ из G в группу $\operatorname{Aut} X$ всех биекций X на себя.

Действие называется *точным*, если этот гомоморфизм инъективен, т. е. разные элементы $g \in G$ задают разные отображения $X \stackrel{g}{\longrightarrow} X$.

Действие называется *транзитивным*, если $\forall x_1, x_2 \in X \quad \exists g \in G: \quad g(x_1) = x_2$, т. е. любой элемент из X можно перевести в любой другой подходящим преобразованием из G.

Множество всех $g \in G$, оставляющих на месте некий фиксированный элемент $x \in X$ (т. е. таких что $g(x) = x$) называется *стабилишзатором* элемента x и обозначается G_x. Стабилизатор, очевидно, является подгруппой в G.

3.3. Орбиты. Множество $x \in X$, которые можно получить из данного элемента $x_0 \in X$ при помощи преобразований из G называется *орбитой* элемента x_0 и обозначается $G(x_0)$. Таким образом, действие транзитивно, если орбита каждого элемента совпадает со всем X. В общем случае множество X, на котором действует группа G, *распадается в объединение непересекающихся орбит*.

Действительно, если $G(x_1) \bigcap G(x_2) \neq \emptyset$ и $x = gx_1 = hx_2$ для каких-то $g, h \in G$, то $x_1 = g^{-1}hx_2$. Потому $x_1 \in G(x_2)$, а значит $G(x_1) \subset G(x_2)$. Аналогично, $G(x_2) \subset G(x_1)$, — так что пересекающиеся орбиты в действительности совпадают, и действие группы G на X можно изучать отдельмо на каждой орбите (где оно транзитивно).

3.3.1. Лемма. *Пусть группа G действует на некоторпм множестве X. Тогда орбита каждого элемента $x \in X$ находится в биективном соответствии с левыми смежными классами группы G по подгруппе G_x.*

Доказательство. Сопоставим каждому элементу gx смежный класс gG_x. Это сопоставление корректно, поскольку из равенства $g_1x = g_2x$ вытекает, что $g_1^{-1}g_2 \in G_x$, а значит

$$g_1 G_x = g_1(g_1^{-1}g_2)G_x = g_2 G_x.$$

Обратное отображение, переводящее смежный класс gG_x в элемент gx также, очевидно, корректно, а потому мы имеем дело с биекцией.

□

3.3.2. Следствие. (Формула для длины орбиты.) *Если G конечна, то $|G(x)| = |G| : |G_x|$.*

□

3.3.3. Следствие. *Стабилизаторы всех элементов одной орбиты состоят из одного и того же числа элементов.*

□

Это следствие можно уточнить. А именно, пусть H - это стабилизатор элемента x, а $y = g(x)$. Тогда стабилизатор y есть $gHg^{-1} = \{ghg^{-1} \quad \forall h \in H\}$. Действительно,

$$gHg^{-1}y = gHg^{-1}gx = gHx = gx = y$$

и если $hy = y$, то

$$g^{-1}hgx = g^{-1}hy = g^{-1}y = x$$

т. е. $g^{-1}hg \in H$, а значит $h \in gHg^{-1}$. Легко видеть, что отображение $G \xrightarrow{\mathrm{Ad}\,(g)} G$, заданное правилом $h \longmapsto ghg^{-1}$, является *автоморфизмом*[2] группы G. Наше уточнение предыдущего следствия теперь можно сформулировать так:

3.3.4. Следствие. *Стабилизаторы элементов x и gx сопряжены при помощи g:*

$$G_{gx} = gG_xg^{-1} .$$

□

Задача 10.16. Докажите, что отображение $G \xrightarrow{\mathrm{Ad}} \mathrm{Aut}\, G$, переводящее элемент $g \in G$ в автоморфизм сопряжения $G \xrightarrow{\mathrm{Ad}(g)} G$ является гомоморфизмом[3].

3.4. Нормальные подгруппы и простота. Подгруппа $H \subset G$ называется *инвариантной* (или *нормальной*), если $gHg^{-1} = H \quad \forall g \in G$, т. е. если все внутренние автоморфизмы группы G сохраняют H (в этом случае пишут $H \triangleleft G$). Группа G называется *простой*, если у неё нет нормальных подгрупп, отличных от $\{e\}$ и G. В частности, све конечные группы простого порядка являются простыми.

§4. Факторизация

4.1. Корректность группового закона на факторе. Выясним, когда на фактор-множестве группы G по какому-либо разбиению на классы можно ввести структуру группы, индуцированную с G, т. е. определив групповую операцию над классами разбиения формулой $[h][g] = [hg]$.

Как и в случае колец, легко видеть, что главное препятствие состоит в возможной *некорректности* этого определения, поскольку если оно корректно, аксиомы группы будут тривиально переноситься с группы G на фактор, в частности, единицей в факторе будет класс $[e]$, а обратным классом к классу $[g]$ будет класс $[g^{-1}]$.

Для корректности правила $[h][g] = [hg]$ необходимо прежде всего, чтобы класс $[e]$ *составлял нормальную подгруппу* в G. Действительно, $\forall g \in [e]$ класс $[g^{-1}]$ должен совпасть с

[2] он называется *автоморфизмом сопряжения* элементом g

[3] его образ называется группой *внутренних автоморфизмов* группы G

$[e^{-1}] = [e]$, и стало быть, $g^{-1} \in [e]$. Аналогично, $\forall g, h \in [e]$ класс $[gh] = [g][h] = [e][e] = [e]$, т. е. $gh \in [e]$. Поетому $[e]$ – подгруппа в G. Более того, $\forall g \in G$ и $\forall h \in [e]$ имеем

$$[ghg^{-1}] = [g][h][g^{-1}] = [g][e][g^{-1}] = [geg^{-1}] = [e]$$

откуда $g[e]g^{-1} \subset [e] \quad \forall g \in G$, а значит $g[e]g^{-1} = [e]$ (т. к. заменив g на g^{-1}, получим обратное включение).Поэтому $[e]$ – нормальная подгруппа.

Второе необходимое условие — классы разбиения должны совпадать с левыми смежными классами по $[e]$. Действительно, если $h \in [g]$, то

$$[e] = [gg^{-1}] = [g][g^{-1}] = [h][g^{-1}] = [hg^{-1}]$$

поэтому $hg^{-1} \in [e]$, а значит $h \in g[e]$. Наоборот, если $h \in g[e], h = gt$ (где $t \in [e]$), то

$$[h] = [gt] = [g][t] = [g][e] = [ge] = [g],$$

т. е. $h \in [g]$.

4.2. Теорема. *Фактор-множество группы G, по некоторому разбиению тогда и только тогда является группой, когда это разбиение есть разбиение на (левые) смежные классы по некоторой нормальной подгруппе $H \triangleleft G$.*

Доказательство. Осталось проверить лишь корректность определения композиции классов $g_1H \circ g_2H = (g_1g_2)H$. Пусть $t_1 \in g_1H$, скажем $t_1 = g_1h_1$, и $t_2 \in g_2H$, скажем $t_2 = g_2h_2$. Тогда $t_1t_2 = g_1h_1g_2h_2$. Поскольку H нормальна, элемент $g_2^{-1}h_1g_2 \in H$, т. е. $g_2^{-1}h_1g_2 = h$ для некоторого $h \in H$, а потому $h_1g_2 = g_2h$, и стало быть $t_1t_2 = g_1g_2hh_2$. Но тогда $t_1t_2H = g_1g_2H$. Теорема доказана.
□

Слово "левый" в условии теоремы взято в скобки, поскольку имеет место

Задача 10.17. Докажите, что подгруппа $H \subset G$ тогда и только тогда нормальна, когда всякий левый смежный класс gH совпадает с правым смежным классом Hg.

4.3. Определение. *Группа смежных классов группы G по нормальной подгруппе H называется фактор-группой G по H и обозначается G/H.*

4.4. Строение гомоморфизмов. Отображение $G \longrightarrow G/H: \quad g \longmapsto gH$ является сюръективным гомоморфизмом группы G на фактор-группу G/H. Он называется *гомоморфизмом приведения по модулю H* или *гомоморфизмом факторизации.*

С произвольным гомоморфизмом $G \xrightarrow{\varphi} G$ можно, как обычно, связать

$$\begin{array}{lcl} \textit{ядро} \ \ \ker\varphi & = & \{g_1 \in G_1 \mid \ \ \varphi(g_1) = e\} \\ \textit{образ} \ \ \mathrm{im}\varphi & = & \{g_2 \in G_2 \mid \ \ \exists g_1 \in G_1: \quad \varphi(g_1) = g_2\} \end{array}$$

4.4.1. Лемма. *$\mathrm{im}\,\varphi$ является подгруппой в G_2, а $\ker\varphi$ — нормальной подгруппой в G_1.*

Доказательство. Поскольку $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$, умножив обе части этого равенства на $\varphi(e)^{-1}$, мы получим $\varphi(e) = e$. Но тогда $\forall g \in G_1$ имеем

$$e = \varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$$

откуда $\varphi(g^{-1}) = \varphi(g)^{-1}$. Поэтому $\forall g, h \in G_1$ имеем $\varphi(gh^{-1}) = \varphi(g)\varphi(h)^{-1}$, а стало быть, $\mathrm{im}\,\varphi \subset G_2$ — подгруппа.

Если $h_1, h_2 \in \ker\varphi$, то $\varphi(h_1h_2^{-1}) = \varphi(h_1)\varphi(h_2)^{-1} = e \cdot e = e$, а значит $\forall h_1, h_2 \in ker\varphi \quad h_1h_2^{-1}$ также лежит в $\ker\varphi$, и $\ker\varphi$ — подгруппа в G_1. Более того,

$$\forall g \in G_1 \qquad \varphi(g(\ker\varphi)g^{-1}) = \varphi(g)\varphi(\ker\varphi)\varphi(g)^{-1} = \varphi(g)e\varphi(g)^{-1} = e$$

поэтому $\ker\varphi$ — нормальна.

Последнее можно было бы проверить и иначе: $\operatorname{im}\varphi$ есть фактор-группа G_1 по разбиению, относящему в один класс все элементы, имеющие один и тот же образ относительно φ. По теореме, доказанной в предыдущем параграфе, это означает, что $\operatorname{im}\varphi$ есть фактор группы G_1 по (автоматически нормальной) подгруппе $\ker(\varphi)$, что и требовалось.

4.4.2. Следствие. *Каноническое отображение*

$$\tilde{\varphi}\colon \operatorname{im}\varphi \longrightarrow G_1/\ker\varphi$$

переводящее каждый $\varphi(g) \in \operatorname{im}\varphi$ в класс $[g] \bmod \ker\varphi$ является корректно определённым изоморфизмом между образом и фактором по ядру.

4.4.3. Следствие. *Простая группа не имеет нетривиальных фактор-групп, а всякий гомоморфизм из простой группы является либо вложением, либо отображением в единицу.*

4.4.4. Следствие. (Теорема о стороении гомоморфизма групп) *Всякий гомоморфизм групп $\varphi\colon G_1 \longrightarrow G_2$ может быть разложен в композицию эпиморфизма факторизации по ядру, изоморфизма этого фактора с образом и вложения образа:*

$$\begin{tikzcd}
G_1 \arrow[r, "\varphi"] \arrow[d, "эпи"'] & G_2 \\
G_1/\ker\varphi \arrow[r, "\tilde{\varphi}", "изо"'] & \operatorname{im}\varphi \arrow[u, "моно"']
\end{tikzcd}$$

§5. Симметрические группы

5.1. Группы многогранников Следующие ниже примеры служат неплохой иллюстрацией всех предыдущих конструкций с группами.

5.1.1. Изоморфизм $Д_3 \tilde{\to} \mathfrak{S}_3$. Группа $\mathfrak{S}_3$ перестановок множества $\{123\}$ состоит из шести перестановок:

$$E = (123), \qquad T = (231), \qquad T^{-1} = (312),$$

$$\sigma_{12} = (213), \qquad \sigma_{13} = (321), \qquad \sigma_{23} = (132).$$

Перестановки E, T, T^{-1} составляют нормальную циклическую подгруппу.

Группа треугольника $Д_3$ (т. е. множество всех движений трёхмерного пространства, переводящих в себя данный правильный треугольник) также состоит из шести элементов: трёх (с учётом тождественного) поворотов относительно центра, составляющих нормальную подгруппу, и ещё трёх симметрий. Если занумеровать вершины треугольника и сопоставить каждому самосовмещению треугольника соответствующую перестановку номеров вершин, мы получим (очевидно, инъективный) гомоморфизм из $Д_3$ в $\mathfrak{S}_3$. Следовательно, $Д_3$ и $\mathfrak{S}_3$ изоморфны.

Задача 10.18. Составьте таблицы умножения для $\mathfrak{S}_3$ и $Д_3$, и явным сравнением этих таблиц убедитесь, что $Д_3$ и $\mathfrak{S}_3$ изоморфны .

5.1.2. $\mathfrak{S}_4$ и тетраэдр. Обобщая предыдущую конструкцию на тетраэдр, мы можем построить гомоморфизм из полной группы тетраэдра в группу $\mathfrak{S}_4$ перестановок номеров его вершин. Он инъективен, поскольку имеет тривиальное ядро: если движение оставляет на месте все 4 вершины некоторого тетраэдра, то это движение тождественное (почему?). В группе $\mathfrak{S}_4$ имеется 24 перестановки. Но в полной группе тетраэдра также 24 движения: все вершины составляют одну орбиту нашей группы, а стабилизатор вершины состоит из трёх поворотов вокруг высот тетраэдра, проходящих через эту вершину, и трёх симметрий в плоскостях, проходящих через примыкающее к вершине ребро и середину противоположного ребра.

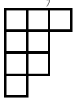
Задача 10.19. Докажите, что стабилизатор вершины изоморфен группе треугольника.

Следовательно, по формуле для длины орбиты (Сл.3.3.2), всего в группе тетраэдра имеется $4 \cdot 6 = 24$ движения, и стало быть, полная группа тетраэдра изоморфна $\mathfrak{S}_4$.

Собственные (сохраняющие ориентацию) вращения тетраэдра составляют, очевидно, нормальную подгруппу в группе тетраэдра. Соответствующая подгруппа в $\mathfrak{S}_4$ называется *знакопеременной группой* на четырёх элементах и обозначается $\mathfrak{A}_4$. Другое название для $\mathfrak{A}_4$,— *группа чётных перестановок*, — обусловлено тем, что каждая из 12 перестановок, составляющих $\mathfrak{A}_4$, может быть получена чётным числом транспозиций, т. е. перестановок какой-либо пары элементов. Действительно, этим свойством обладают все 8 циклов длины 3 (переставляющих по циклу какие-либо 3 элемента, а четвёртый не меняющие), соответствующие поворотам вокруг высот тетраэдра, а также три подстановки (2143), (4321), (3412) из квадратичной группы Клейна.

5.1.3. $\mathfrak{S}_4$ и собственная группа куба. Группа собственных самосовмещений куба состоит из 24 вращений (ибо у куба 8 вершин, а стабилизатор вершины состоит из трёх поворотов на $0°$ и $\pm 120°$ вокруг диагонали, проходящей через вершину). Занумеровав 4 диагонали куба цифрами 1 , 2 , 3 и 4 мы, как и выше, определяем инъективный гомоморфизм из группы куба в $\mathfrak{S}_4$. Поэтому $\mathfrak{S}_4$ изоморфна собственной группе куба.

Задача 10.20. Опишите явно все подгруппы в группе вращений куба. В частности, опишите, каким вращениям куба отвечают несобственные самосовмещения тетраэдра, а каким - собственные.

5.2. Цикловой тип перестановки. Рассмотрим в $\mathfrak{S}_n$ циклическую подгруппу, порождённую элементом g (обозначим её $\langle g \rangle$). Группа $\langle g \rangle$ действует на множестве $\{1, 2, \ldots, n\}$ символов, переставляемых группой $\mathfrak{S}_n$. По n° 3.3 это действие разбивает всё множество $\{1, 2, \ldots, n\}$ в объединение непересекающихся орбит относительно действия g. Эти орбиты называются *независимыми циклами*, поскольку каждая из них состоит из элементов $\{i, gi, g^2 i, \ldots\}$, циклически переставляемых элементом g, и действие g на каждом таком цикле происходит независимо. В частности, это означает, что $g = h_1 h_2 \ldots h_m$, где m - количество циклов, а h_i — циклическая перестановка элементов i-того цикла на 1 шаг. Такое разложение называется *разложением g в произведение независимых циклов*. Набор длин циклов составляет разбиение числа n и называется *цикловым типом g*. Удобно представлять его диаграммой Юнга. Например, перестановка $g \in \mathfrak{S}_8$, переводящая (12345678) в (51682374), распадается в произведение циклов $1 \to 5 \to 2 \to 1$ длины 3, $3 \to 6 \to 3$ длины 2, $4 \to 8 \to 4$ длины 2, $7 \to 7$ длины 1, и её цикловой тип изображается диаграммой Юнга:  .

Задача 10.21. Убедитесь, что две перестановки тогда и только тогда сопряжены в $\mathfrak{S}_n$, когда они имеют одинаковый цикловой тип.

Указание. Запишем в строки диаграммы Юнга номера элементов, циклически переставляемых соответствующими циклами перестановки g, в том порядке, в каком они переходят друг в друга при действии g. Если g и g_1 имеют одинаковый цикловой тип, то $g = hg_1h^{-1}$, где h отображает элемент $\alpha \in \{1, \ldots, n\}$ в элемент, стоящий в той же клеточке диаграммы g, в которой α стоит на диаграмме g_1.

5.3. Знакопеременная подгруппа $\mathfrak{A}_n \subset \mathfrak{S}_n$. Определённый нами в лекции 6 *знак перестановки* является, очевидно гомоморфизмом из симметрической группы $\mathfrak{S}_n$ в группу из двух элементов $\{\pm 1\}$ с операцией умножения. Ядро $\ker(sgn)$ состоит из всех чётных перестановок, которые, тем самым, образуют нормальную подгруппу индекса 2 в $\mathfrak{S}_n$. Она обозначается $\mathfrak{A}_n$ и называется *знакопеременной группой* или *группой чётных подстановок.*

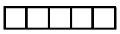
Термин «знакопеременный» связан с тем, что подгруппа $\mathfrak{A}_n$ является *централизатором*[4] множества *знакопеременных* функций — таких функций от n переменных, которые меняют знак при транспозиции любой пары аргументов. Примером знакопеременного многочлена является произведение упорядоченных разностей:

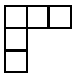
$$\delta(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j) \, .$$

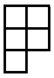
Задача 10.22. Докажите, что всякий знакопеременный многочлен делится (в кольце многочленов от n переменных) на произведение упорядоченных разностей, и частное от этого деления будет симметрическим многочленом.

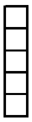
Задача 10.23. Докажите, что перестановка тогда и только тогда чётна, когда в её цикловом типе число циклов чётной длины чётно.

5.3.1. Строение группы $\mathfrak{A}_5$ Опишем классы сопряжённых элементов в $\mathfrak{A}_5$. Для этого сначала опишем классы элементов $\mathfrak{A}_5$, сопряжённых в $\mathfrak{S}_5$. Согласно предыдущему, такие классы соответствуют диаграммам Юнга веса 5 с чётным количеством строк чётной длины. Таких диаграмм имеется всего 4:

 – циклы длины 5, всего $4! = 24$шт. (почему?);

 – циклы длины 3, всего $2 \cdot \binom{5}{2} = 20$шт. (почему?);

 – пары независимых транспозиций, всего $5 \cdot 3 = 15$шт. (почему?);

 – тождественная подстановка, 1шт.

Задача 10.24. Докажите, что все циклы длины 3 сопряжены между собой в $\mathfrak{A}_5$.

Задача 10.25. Докажите, что все пары транспозиций сопряжены между собой в $\mathfrak{A}_5$.

[4] т. е. поточечно оставляет на месте все элементы

Задача 10.26. Докажите, что все циклы длины 5 образуют два класса сопряжённости в $\mathfrak{A}_5$: циклы, сопряжённые циклу $1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5$, и циклы, сопряжённые циклу $2 \longrightarrow 1 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5$.

5.4. Теорема. *Группа $\mathfrak{A}_5$ проста.*

Доказательство. Если подгруппа $H \subset A$ — нормальная, то вместе с каждым элементом она содержит весь класс сопряжённых ему элементов. Всего таких классов в $\mathfrak{A}_5$,— как мы видели в задачах зад.10.24–зад.10.26,— имеется 5, и состоят они из 1, 12, 12, 20 и 15 элементов. Т.к. единица лежит в любой подгруппе, имеем:

$$|H| = 1 + 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4,$$

где все ε_k равны либо 1, либо 0. Непосредственная проверка показывает, что |H| делит $|\mathfrak{A}_5| = 60$ лишь в двух случаях: $\varepsilon_k = 1 \quad \forall k$ и $\varepsilon_k = 0 \quad \forall k$ (убедитесь!), так что непростота $\mathfrak{A}_5$ противоречит теореме Лагранжа (Теор.2.6).

Задача 10.27. Докажите, что все группы $\mathfrak{A}_n$ с $n \geq 5$ просты.

Указание. Воспользуйтесь индукцией. Вложите $\mathfrak{A}_{n-1}$ в $\mathfrak{A}_n$ как стабилизатор символа n, и докажите, что нетривиальная нормальная подгруппа в $\mathfrak{A}_n$ обязана иметь нетривиальное пересечение с $\mathfrak{A}_{n-1}$ (автоматически нормальное в $\mathfrak{A}_{n-1}$)), что противоречит индуктивному предположению о простоте $\mathfrak{A}_{n-1}$.

Задача 10.28. Докажите, что внутренние автоморфизмы составляют подгруппу индекса 2 в группе всех автоморфизмов группы $\mathfrak{A}_5$.

Указание. Всякий автоморфизм $\mathfrak{A}_5$ переводит цикл длины 5 в цикл длины 5 и является внутренним тогда и только тогда, когда переводит циклы длины 5 в сопряжённые циклы длины 5.

Задача 10.29. Докажите, что группа A_5 изоморфна собственной группе икосаэдра.

Указание. Найдите у икосаэдра 5 геометрических подконфигураций, переставляемых его вращениями.