§1. Группы.

1.1. Эндоморфизмы и автоморфизмы. Будем называть *эндоморфизмом* множества X любое отображение $X \longrightarrow X$. Множество всех эндоморфизмов обозначается $\mathrm{End}(X)$.

На $\mathrm{End}(X)$ имеется операция *композиции*: мы пишем $\varphi\circ\psi$ для отображения, переводящего $x \in X$ в $\varphi(\psi(x))$. Эта операция очевидно ассоциативна: $\varphi\circ(\psi\circ\eta) = (\varphi\circ\psi)\circ\eta$ для всех φ, ψ, η. Тождественный эндоморфизм играет роль единицы: $\mathrm{Id}_X\circ\varphi = \varphi\circ\mathrm{Id}_X = \varphi$ для всех φ.

Множество G, снабжённое ассоциативной бинарной операцией с единицей, называется *моноидом*. Таким образом, $\mathrm{End}(X)$ представляет собою моноид. Подчеркнём, что операция композиции не предполагается коммутативной: скажем, в моноиде $\mathrm{End}(X)$ как правило $\varphi\circ\psi \neq \psi\circ\varphi$.

Упражнение 1.1. Приведите какой-нибудь явный пример двух некоммутирующих эндоморфизмов.

Если множество X несёт какую-либо дополнительную алгебраическую структуру (например, является кольцом или модулем), то под эндоморфизмами мы всегда будем понимать гомоморфизмы, сохраняющие эту структуру. Они составляют подмоноид в моноиде всех теоретико множественных эндоморфизмов.

Эндоморфизм $X \xrightarrow{\varphi} X$ называется *автоморфизмом* (или *симметрией*), если он обладает двусторонним обратным, т.е. $\exists\, \varphi^{-1} \in \mathrm{End}(X)$ такой что $\varphi\circ\varphi^{-1} = \varphi^{-1}\circ\varphi = \mathrm{Id}_X$. Множество всех автоморфизмов $X \xrightarrow{\varphi} X$ обозначается $\mathrm{Aut}\,(X)$.

Упражнение 1.2. Убедитесь, что всякий автоморфизм биективен, а когда X является кольцом (или модулем), теоретико множественное обратное отображение φ^{-1} к любому обратимому гомоморфизму $X \xrightarrow{\varphi} X$ также является гомоморфизмом.

Будем называть *группой симметрий* множества X любое подмножество $G \subset \mathrm{Aut}\,(X)$, замкнутое относительно взятия композиций и обращения. Например, множество всех аффинных автоморфизмов $\mathbb{A}^n \xrightarrow{\sim} \mathbb{A}^n$, переводящих в себя некоторую фигуру $\Phi \subset \mathbb{A}^n$, образует такую группу. Эта группа называется *группой фигуры* Φ. Над полем $\mathbb{R}$ различают *собственную* и *несобственную* группы[1].

1.1.1. Пример: группа правильного плоского n-угольника в трёхмерном евклидовом пространстве называется *группой диэдра* и обозначается $\mathfrak{D}_n$. Она состоит из n поворотов плоскости n-угольника на углы $2\pi k/n$ и n симметрий (т.е. поворотов на 180° вокруг подходящих 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. При $n = 2$ многоугольник вырождается в дольку $\circ$, а группа $\mathfrak{D}_2$ чаще обозначается $\mathfrak{V}$ и называется *квадратичной* (или *четвертной*) *группой Клейна*. Она состоит из тождественного преобразования и трёх поворотов на 180°, и может быть иначе описана как группа всех вращений евклидова пространства $\mathbb{R}^3$, переводящих в себя *каждую* из трёх координатных прямых.

1.1.2. Пример: собственная группа правильного тетраэдра содержит 12 вращений: тождественное, 8 поворотов на $\pm120^\circ$ вокруг осей, проходящих через вершину и центр противоположной грани, и 3 поворота на 180° вокруг осей, проходящих через середины противоположных рёбер.

Упражнение 1.3. Проверьте, что других собственных евклидовых автоморфизмов у тетраэдра нет.

Повороты на $\pm120^\circ$ вокруг фиксированной оси вместе с тождественным преобразованием образуют трёхэлементную подгруппу в группе тетраэдра, и всего таких подгупп четыре. Три поворота на 180° вокруг прямых, соединяющих середины противоположных ребер, образуют вместе с тождественным оператором четвертную группу Клейна $\mathfrak{V}$.

Упражнение 1.4. Убедитесь, что никаких других подгрупп в группе тетраэдра нет.

Упражнение 1.5. Выясните, сколько элементов имеется в собственных и несобственных группах пяти платоновых тел[2] в $\mathbb{R}^3$.

[1] во второй допускаются операторы, меняющие ориентацию пространства, в первой — нет

[2] т.е. правильных тетраэдра, куба, октаэдра, додекаэдра и икосаэдра

1.1.3. Пример: симметрическая и знакопеременная группы. Группа $\mathfrak{S}_n = \mathrm{Aut}\,(\{1, 2, \dots, n\})$ всех взаимно однозначных отображений n-элементного множества в себя называется *симметрической группой* (или *группой перестановок*). Она состоит из $n!$ элементов. Чётные перестановки образуют в $\mathfrak{S}_n$ подгруппу $\mathfrak{A}_n$, называемую *знакопеременной группой*. Отметим, что занумеровав вершины правильного тетраэдра числами 1, 2, 3, 4, мы можем сопоставить каждому преобразованию из (несобственной) группы тетраэдра перестановку вершин, осуществляемую этим преобразованием. Получается сохраняющее композицию отображение из группы тетраэдра в группу $\mathfrak{S}_4$.

Упражнение 1.6. Проверьте, что это отображение биективно, причём собственная группа тетраэдра изоморфно переводится им в знакопеременную группу $\mathfrak{A}_4$.

1.2. Абстрактные группы. Вообще, (абстрактной) *группой* называется произвольный моноид, в котором каждый элемент обратим, т. е. любое множество G с ассоциативной операцией $(g, h) \mapsto gh$, обладающее единичным элементом $e \in G : ge = eg = g \quad \forall\, g \in G$, и такое, что $\forall\, g \in G$ $\exists\, g^{-1} : gg^{-1} = g^{-1}g = e$.

Упражнение 1.7. Убедитесь, что единичный элемент $e \in G$ единственен (в любом моноиде), а обратный элемент g однозначно определяется по g для любого $g \in G$.

Упражнение 1.8. Докажите, что подмножество $H \subset G$ тогда и только тогда образует подгруппу, когда $h_1 h_2^{-1} \in H \;\forall\, h_1, h_2 \in H$.

Если операция в группе коммутативна, т. е. $gh = hg$ для всех$g, h \in G$, группа G называется *абелевой*. Операция в абелевых группах обычно обозначается знаком «+», поскольку определяющие группу свойства превращаются в этой ситуации в свойства сложения векторов в модуле или сложения чисел в коммутативном кольце.

1.3. Гомоморфизмы. Отображение групп $G \xrightarrow{\varphi} H$ называется *гомоморфизмом*, если

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) \quad \forall\, g_1, g_2 \in G \;.$$

Поскольку $\varphi(g) = \varphi(ge) = \varphi(g)\varphi(e)$, домножая это равенство слева на $\varphi(g)^{-1}$, получаем $\varphi(e) = e$. Похожая выкладка: $e = \varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$ показывает, что $\varphi(g^{-1}) = \varphi(g)^{-1}$.

1.3.1. Пример: реализация абстрактной группы как группы симметрий. Всякая группа G допускает гомоморфные вложения $G \overset{\gamma}{\hookrightarrow} \mathrm{Aut}\, X$ в группы автоморфизмов разнообразных множеств X. Например, в качестве X можно взять саму группу G (рассматриваемую как множество) и для каждого $g \in G$ положить

$$\gamma(g) : G \xrightarrow{x \mapsto gx} G \;. \tag{1-1}$$

Поскольку отображение $\gamma\left(g^{-1}\right)$ обратно к отображению $\gamma(g)$, все отображения $\gamma(g)$ являются автоморфизмами множества G.

Упражнение 1.9. Убедитесь, что $\gamma(g_1 g_2) = \gamma(g_1) \circ \gamma(g_2)$ и $\gamma(g_1) \neq \gamma(g_2)$ при $g_1 \neq g_2$.

Отметим, что отображение (1-1) при $g \neq e$ не является автоморфизмом G как *группы*, поскольку

$$g(g_1 g_2) \neq (gg_1)(gg_2) \quad \text{при } g \neq e \;.$$

Можно, однако, задать и гомоморфизм из G в группу *групповых* автоморфизмов $\mathrm{Aut}\, G$. А именно, сопоставим элементу $g \in G$ *автоморфизм сопряжения*

$$\mathrm{Ad}_g : G \xrightarrow{x \mapsto gxg^{-1}} G \;. \tag{1-2}$$

Упражнение 1.10. Убедитесь, что Ad_g является при фиксированном g обратимым гомоморфизмом, а также что отображение $\mathrm{Ad} : G \xrightarrow{g \mapsto \mathrm{Ad}_g} \mathrm{Aut}\,(G)$ является гомоморфизмом групп.

В отличие от предыдущего вложения в теоретико-множественные автоморфизмы, гомоморфизм Ad может не быть вложением: например, когда группа G абелева, $\mathrm{Ad}\,(G) = \{\mathrm{Id}_G\}$ состоит из одного лишь тождественного автоморфизма.

1.3.2. Ядро и образ. Со всяким гомоморфизмом $G \xrightarrow{\varphi} H$ можно связать две подгруппы:

$$\textit{ядро } \ker\varphi = \{g \in G \mid \varphi(g) = e\} \subset G \;,$$
$$\textit{образ } \operatorname{im}\varphi = \varphi(G) \subset H \;.$$

Упражнение 1.11. Убедитесь, что φ инъективен тогда и только тогда, когда $\ker\varphi = \{e\}$.

Отметим, что подгруппа $\ker\varphi$ обладает замечательным свойством:

$$g\cdot\ker\varphi\cdot g^{-1}\subset\ker\varphi \quad \forall\, g\in G\ , \tag{1-3}$$

которое, вообще говоря, не выполнено для *произвольного* расширения групп $H\subset G$.

Упражнение 1.12. Рассмотрим группу $\mathfrak{S}_n = \mathrm{Aut}\big(\{1,2,\dots,n\}\big)$ всех перестановок n-элементного множества. В какую подгруппу перейдёт подгруппа $\mathrm{Aut}\big(\{1,2,\dots,(n-1)\}\big)\subset\mathfrak{S}_n$ (все перестановки первых $n-1$ элементов) при сопряжении транспозицией 1-го и n-того элемента?

Подгруппа $H\subset G$, такая что $gHg^{-1}\subset H \quad \forall\, g\in G$, называется *нормальной*. Вложение нормальной подгруппы в объемлющую группу обозначается значком $H\lhd G$.

1.3.3. Факторизация. Для любой нормальной подгруппы $H\lhd G$ можно построить группу G/H и сюрьективный гомоморфизм $G\xrightarrow{\pi} G/H$, такой что $\ker\pi = H$, и для любого гомоморфизма групп $G\xrightarrow{\psi} S$, переводящего всю подгруппу H в единицу, будет *существовать единственный* гомоморфизм групп $G/H\xrightarrow{\widetilde{\psi}} S$, такой что $\psi=\widetilde{\psi}\circ\pi$, т. е. диаграмма

$$\begin{tikzcd} G \arrow[rr, "\psi"] \arrow[dr, "\pi"'] & & S \\ & G/H \arrow[ur, "\widetilde{\psi}"'] & \end{tikzcd} \tag{1-4}$$

будет коммутативна. А именно, разобьём G в объединение *левых смежных классов*, т. е. подмножеств вида

$$gH \overset{\text{def}}{=} \{gh\mid h \text{ пробегает } H\}\,.$$

Упражнение 1.13. Убедитесь, что для произвольной (не обязательно нормальной) подгруппы $H\subset G$ левые смежные классы g_1H, g_2H либо не пересекаются, либо полностью совпадают (т. е. что отношение $g_1\sim g_2$, означающее, что $g_1^{-1}g_2\in H$, рефлексивно, симметрично и транзитивно).

Обозначим множество смежных классов через G/H и введём на нём операцию, индуцированную с G, т. е. положим $g_1H\cdot g_2H \overset{\text{def}}{=} (g_1g_2)H$. Нормальность подгруппы H обеспечивает корректность этого определения: если $g_1'H = g_1H$, $g_2'H = g_2H$, т. е. $g_1' = g_1h_1$, $g_2' = g_2h_2$ для некоторых $h_1,h_2\in H$, то $g_1'g_2'H = g_1h_1g_2h_2H = g_1g_2g_2^{-1}h_1g_2h_2H = g_1g_2H$, поскольку $g_2^{-1}h_1g_2\in H$ из-за нормальности H.

Упражнение 1.14. Проверьте, что G/H группа, а также что *гомоморфизм факторизации*

$$G\xrightarrow{g\mapsto gH} G/H$$

имеет H своим ядром и обладает описанным выше свойством универсальности.

Легко видеть, что верно и обратное: если группа G каким-то образом разбита на классы эквивалентности $G=\bigsqcup\limits_g [g]$, и на множестве $\widetilde{G}$ этих классов $[g]$ корректно индуцируется структура группы по правилу $[g_1][g_2]=[g_1g_2]$, то все классы с неизбежностью являются левыми смежными классами по некоторой нормальной подгруппе. В самом деле, отображение

$$G\xrightarrow{g\mapsto[g]}\widetilde{G}$$

является в этом случае гомоморфизмом групп с ядром $[e]$. Тем самым, $[e]\lhd G$ и $[g]=g[e] \quad \forall\, g\in G$.

Упражнение 1.15. Проверьте, что всякий гомоморфизм групп $G_1\xrightarrow{\varphi} G_2$ раскладывается в композицию сюръекции, изоморфизма и вложения: $G_1\xrightarrow{\pi} G_1/\ker\varphi\simeq \mathrm{im}\,\varphi\xrightarrow{\iota} G_2$

1.3.4. Пример: гомоморфизм $\mathfrak{D}_3\xrightarrow{\sim}\mathfrak{S}_3$, который сопоставляет самосовмещению треугольника возникающую при этом перестановку его вершин, не имеет ядра, т. к. движение треугольника, оставляющее все вершины на месте, тождественно. Тем самым, это вложение, а значит — изоморфизм, поскольку обе группы имеют одинаковое число элементов. Аналогичным образом устанавливается изоморфизм между несобственной группой тетраэдра и группой перестановок $\mathfrak{S}_4$ четырёх его вершин (ср. с упр. 1.6).

1.4. Действия. Гомоморфизм $G \xrightarrow{\varrho} \mathrm{Aut}\,(X)$ группы G в группу взаимно однозначных отображений некоторого множества X в себя называется *действием* группы G на X, или её *представлением* автоморфизмами X. Действие ϱ называется *эффективным*, если $\ker\varrho = \{e\}$, т. е. все неединичные элементы группы представляются нетождественными отображениями. Действие называется *транзитивным*, если любой элемент $x \in X$ можно перевести в любой другой элемент $x' \in X$ некоторым преобразованием из группы.

Если G действует на X, то для произвольного подмножества $Y \subset X$ подгруппы

$$\mathrm{Stab}(Y) = \{g \in G \mid gy = y \quad \forall\, y \in Y\,\}$$
$$\mathrm{Norm}(Y) = \{g \in G \mid g(Y) = Y\}$$

называются *стабилизатором* и, соответственно, *нормализатором* подмножества Y. Стабилизатор является нормальной подгруппой в нормализаторе (но не во всей группе G), и фактор группа $\mathrm{Norm}(Y)/\mathrm{Stab}(Y)$ эффективно действует на Y. Если $Y = \{x\}$ состоит из одной точки, нормализатор совпадает с централизатором. Действие называется *свободным*, если стабилизаторы всех точек тривиальны.

Важными примерами действий являются рассмотренные в n° 1.3.1 действия группы G на себе левыми сдвигами и сопряжениями.

Действие левыми сдвигами называется *левым регулярным* действием. Оно свободно и транзитивно. Действие сопряжениями называется *присоединённым* действием. Оно, как мы видели, бывает неэффективным. Его ядро образует в G нормальную абелеву подгруппу, которая состоит из преобразований, коммутирующих со всеми элементами группы, и называется *центром* группы G:

$$Z(G) = \ker \mathrm{Ad} \ = \{g \in G\,|gh = hg \quad \forall\, h \in G\,\}\ .$$

Стабилизатор заданного элемента $h \in G$ при присоединённом действии, т. е. подгуппа

$$Z(h) \stackrel{\mathrm{def}}{=} \mathrm{Stab}(h) = \{g \in G \mid gh = hg\}\ , \tag{1-5}$$

обычно называется *централизатором* этого элемента.

1.4.1. Орбиты. Множество всех элементов, которые можно получить, действуя на данный элемент $x \in X$ всевозможными автоморфизмами из группы G, называется *орбитой* элемента x и обозначается Gx. Транзитивность действия означает равенство $Gx = X$ для всех $x \in X$. Обобщением упр. 1.13 является

1.4.2. ЛЕММА. *Пусть группа G действует на некотором множестве X. Тогда X распадается в объединение непересекающихся орбит, причём точки каждой орбиты Gx находятся в биективном соответствии с левыми смежными классами группы G по подгруппе* $\mathrm{Stab}(x)$*, а стабилизаторы всех точек, лежащих в одной орбите, сопряжены: если $y = gx$, то*

$$\mathrm{Stab}(y) = g \cdot \mathrm{Stab}(x) \cdot g^{-1} = \{ghg^{-1} \mid h \in \mathrm{Stab}(x)\}$$

(в частности, стабилизаторы всех точек из одной орбиты равномощны).

Доказательство. Отношение $y \in Gx$ очевидно рефлексивно, симметрично и транзитивно, поэтому орбиты образуют разбиение множества X. Если $y = gx$, то

$$\{h \in G \mid hx = y\} = \{h \in G \mid hx = gx\} = \{h \in G \mid g^{-1}h \in \mathrm{Stab}(x)\} = g \cdot \mathrm{Stab}(x)\ ,$$

т. е. множество всех преобразований из G, переводящих x в y, в точности образует левый смежный класс, что задаёт биекцию между $G/\mathrm{Stab}(x)$ и Gx. Наконец, при $y = gx$ условия $hx = x$ и $ghg^{-1}y = y$ очевидным образом равносильны. □

1.4.3. СЛЕДСТВИЕ (ФОРМУЛА ДЛЯ ДЛИНЫ ОРБИТЫ). *Если конечная группа G действует на множестве X, то $|Gx| = |G| : |\mathrm{Stab}(x)|$ для любого $x \in X$.* □

1.4.4. Пример: группы правильных многогранников в $\mathbb{R}^3$. Группа правильного многогранника транзитивно действует на множестве вершин. Стабилизатор вершины вкладывается в группу многоугольника, натянутого на концы всех выходящих из этой вершины рёбер, и в случае собственной группы состоит из всех поворотов этого многоугольника, а в случае несобственной группы содержит кроме поворотов и все отражения диэдральной группы. По формуле для длины орбиты получаем, что собственные группы тетраэдра, октаэдра и икосаэдра состоят, соответственно, из $3 \cdot 4 = 12$, $4 \cdot 6 = 24$ и $5 \cdot 12 = 60$ элементов. В несобственных группах элементов вдвое больше. Группа куба изоморфна группе октаэдра, а группа додекаэдра — группе икосаэдра, поскольку эти многогранники аффинно двойственны друг другу[3].

Группа куба действует перестановками на множестве его диагоналей, что даёт гомоморфизм этой группы в группу $\mathfrak{S}_4$. Ядром этого действия являются изометрии, для которых диагонали куба служат собственными векторами с собственными значениями ± 1. Поскольку симметрия в плоскости, проходящей через пару диагоналей, меняет две другие диагонали местами, собственные значения преобразования, лежащего в ядре, либо все равны 1, либо все равны -1, т. е. ядро состоит ровно из двух преобразований $\pm\mathrm{Id}$. В частности, собственная группа куба вкладывается в $\mathfrak{S}_4$, а стало быть, изоморфна $\mathfrak{S}_4$, ибо обе группы состоят из 24 элементов.

С другой стороны, собственная группа куба действует на множестве пар противоположных граней, что даёт гомоморфизм группы куба в $\mathfrak{S}_3$, ядром которого является четвертная группа Клейна $\mathfrak{V}$ (переводящая в себя каждую из координатных осей, соединяющих центры противоположных граней). Учитывая предыдущее отождествление собственной группы куба с $\mathfrak{S}_4$ и равенство $24/4 = 6$, мы получаем нормальность $\mathfrak{V}$ в $\mathfrak{S}_4$ и изоморфизм $\mathfrak{S}_4/\mathfrak{V} = \mathfrak{S}_3$.

Упражнение 1.16. Убедитесь, что $\mathfrak{V}$ вложена в $\mathfrak{S}_4$ как подгруппа, состоящая из тождественного отображения и трёх пар непересекающихся транспозиций: $(12)(34)$, $(13)(24)$ и $(14)(23)$.

Упражнение 1.17. Убедитесь, что диагонали граней додекаэдра образуют на его поверхности пять кубов и действие группы додекаэдра на этих пяти кубах устанавливает изоморфизм собственной группы додекаэдра со знакопеременной группой $\mathfrak{A}_5$.

Упражнение 1.18*. Покажите, что несобственная группа додекаэдра *не изоморфна* симметрической группе $\mathfrak{S}_5$.

1.5. Порядок, индекс и классы сопряжённости. Число элементов $|G|$ конечной группы G называется *порядком* этой группы. Число смежных классов[4] $|G/H|$ группы G по какой-либо подгруппе H называется *индексом* этой подгруппы в G.

Группа G транзитивно действует на множестве левых смежных классов G/H левыми умножениями, при этом стабилизатором класса eH является сама подгруппа H. Из формулы для длины орбиты получается равенство

$$|G/H| = |G|/|H| \,, \tag{1-6}$$

означающее, в частности, что порядок и индекс любой подгруппы $H \subset G$ нацело делят порядок группы.

Орбиты присоединённого действия $\mathrm{Ad} : G \longrightarrow \mathrm{Aut}\,(G)$, которое представляет каждый элемент $g \in G$ автоморфизмом сопряжения $\mathrm{Ad}_g : h \longmapsto ghg^{-1}$, называются *классами сопряжённости*. По формуле для длины орбиты число элементов в классе сопряжённости C_h данного элемента $h \in G$ равно индексу централизатора этого элемента (ср. с (1-5)) :

$$|C_h| = |G|/|Z(h)| \,, \quad \text{где} \quad Z(h) = \{g \in G \mid gh = hg\} \tag{1-7}$$

Подгруппа $\mathrm{Ad}\,(G) \lhd \mathrm{Aut}\,(G)$ является нормальной, т. к. для любого автоморфизма $G \xrightarrow{\psi} G$ и любого $g \in G$ имеется очевидное равенство $\psi \circ \mathrm{Ad}_g \circ \psi^{-1} = \mathrm{Ad}_{\psi(g)}$. Эта подгруппа называется

[3] один является выпуклой оболочкой центров граней другого и наоборот

[4] ещё раз отметим, что G/H — это всего лишь множество, которое наследует структуру группы если и только если $H \lhd G$ *нормальна*

группой *внутренних автоморфизмов* группы G, а фактор $G/\mathrm{Ad}(G)$ — группой *внешних автоморфизмов*. Так, все автоморфизмы абелевой группы являются внешними. Группы, не имеющие нетождественных внешних автоморфизмов, называются *совершенными*.

Упражнение 1.19*. Покажите, что симметрические группы $\mathfrak{S}_3$, $\mathfrak{S}_4$, $\mathfrak{S}_5$ совершенны, а $\mathfrak{S}_6$ — нет.

1.6. Циклические группы. Наименьшая подгруппа, содержащая заданный элемент $g \in G$, — это абелева группа $\langle g \rangle \overset{\text{def}}{=} \{g^m \mid m \in \mathbb{Z}\}$, образованная всевозможными целыми[5] степенями элемента g. Группа G называется *циклической*, если $G = \langle g \rangle$ для некоторого $g \in G$. Всякий такой элемент $g \in G$ называется *образующей* циклической группы G.

Для любого элемента g произвольной группы G имеем эпиморфизм абелевых групп

$$\mathbb{Z} \xrightarrow{m \mapsto g^m} \langle g \rangle \ . \tag{1-8}$$

Если он инъективен, то $\langle g \rangle \simeq \mathbb{Z}$. В этом случае g называется *элементом бесконечного порядка*. Если гомоморфизм (1-8) имеет ненулевое ядро, то это ядро является $\mathbb{Z}$-подмодулем в $\mathbb{Z}$, и значит, имеет вид $(k) = k \cdot \mathbb{Z}$, где $k \in \mathbb{N}$ является наименьшим натуральным числом, лежащим в этом подмодуле, т. е. является минимальным положительным показателем степени, в которой $g^k = e$. В этом случае $\langle g \rangle \simeq \mathbb{Z}/(k)$ и $|\langle g \rangle| = k$. Число k называется *порядком* элемента g.

Упражнение 1.20. Пусть g порождает циклическую группу G порядка k. Покажите, что
а) образующие G суть элементы g^m с $\text{нод}(m,k) = 1$;
б) автоморфизмы G суть отображения $x \longmapsto x^m$, где $\text{нод}(m,k) = 1$.

Если группа G конечна, то каждый элемент $g \in G$ имеет конечный порядок, нацело делящий $|G|$ согласно (1-6). В частности, $g^{|G|} = e$ для всех $g \in G$. Отметим, что порядок образующей совпадает с порядком группы, и для для того, чтобы группа G была циклической, необходимо и достаточно, чтобы в ней существовал элемент, порядок которого в точности равен порядку группы.

1.6.1. Пример: мультипликативные подгруппы поля. Покажем, что любая конечная подгруппа G в мультипликативной группе $\Bbbk^*$ ненулевых элементов произвольного поля $\Bbbk$ всегда является циклической.

Упражнение 1.21. Пусть элементы g, h абелевой группы G имеют порядки k, n, и пусть $k = k_1k_2$, $n = n_1n_2$, где $\text{нод}(k_1,n_1) = 1$ и $n_1k_1 = \text{нок}(n,k)$. Покажите, что порядок элемента $g^{n_2}h^{k_2}$ равен $\text{нок}(n,k)$.

Из задачи вытекает, что в конечной абелевой группе всегда есть элемент, порядок которого k является наименьшим общим кратным порядков всех элементов группы[6], а значит, все элементы группы удовлетворяют уравнению $x^k = 1$. Поскольку в поле у этого уравнения имеется не более k корней, k не может быть меньше $|G|$. А т. к. k одновременно должен делить $|G|$, получаем $k = |G|$.

1.6.2. Пример: цикловой тип перестановки. Циклическая подгруппа $\langle \sigma \rangle$, порождённая любой перестановкой $\sigma \in \mathfrak{S}_n$, действует на множестве $\{1, 2, \dots, n\}$, разбивая его в объединение непересекающихся орбит, которые называются *независимыми циклами* перестановки σ. Пусть имеется m таких орбит $Gx_1, Gx_2, \dots, Gx_m$. Тогда

$$\sigma = \tau_1 \tau_2 \cdots \tau_m \tag{1-9}$$

где действие перестановки τ_i состоит в сдвиге на один шаг вдоль i-той орбиты

$$x_i \xmapsto{\sigma} \sigma x_i \xmapsto{\sigma} \sigma^2 x_i \xmapsto{\sigma} \ \cdots \ \xmapsto{\sigma} \sigma^{\lambda_i - 1} x_i \xmapsto{\sigma} \sigma^{\lambda_i} x_i = x_i \ ,$$

где мы обозначили длину i-той орбиты через λ_i. Разложение (1-9) называется *разложением в независимые циклы*. Все эти циклы перестановочны: $\tau_i\tau_j = \tau_j\tau_i$, и порядок перестановки σ равен $\text{нок}(\lambda_1, \lambda_2, \dots, \lambda_m)$.

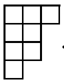
Упражнение 1.22. Покажите, что перестановка σ чётна тогда и только тогда, когда в её разложении (1-9) число циклов чётной длины чётно.

Набор длин циклов $(\lambda_1, \lambda_2, \dots, \lambda_m)$ составляет разбиение числа n и называется *цикловым типом* перестановки σ. Удобно представлять его диаграммой Юнга. Например, перестановка

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 6 & 8 & 2 & 3 & 7 & 4 \end{pmatrix} \in \mathfrak{S}_8$$

[5] как обычно, мы полагаем $g^{-n} \overset{\text{def}}{=} (g^{-1})^n$ для $n \in \mathbb{N}$

[6] это легко вывести и из общей теоремы о строении конечных абелевых групп

распадается в произведение четырёх циклов: $\sigma = (152)\cdot(36)\cdot(48)\cdot(7)$ и имеет цикловой тип . Все перестановки заданного циклового типа λ получаются всевозможными заполнениями n клеток диаграммы λ числами $\{1, 2, \dots, n\}$ без повторений и действуют циклическими сдвигами вдоль строк. Так, предыдущей перестановке σ отвечает заполнение

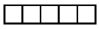
$$\begin{array}{|c|c|c|}\hline 1&5&2\\ \hline 3&6\\ \cline{1-2} 4&8\\ \cline{1-2} 7\\ \cline{1-1}\end{array}\,.$$

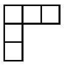
Поскольку заполненная диаграмма Юнга перестановки $\varrho\sigma\varrho^{-1}$ получается применением перестановки ϱ к элементам заполненной диаграммы перестановки σ, две перестановки сопряжены тогда и только тогда, когда они имеют одинаковый цикловой тип. Таким образом, классы сопряжённости $C_\lambda \subset \mathfrak{S}_n$ взаимно однозначно соответствуют n-клеточным диаграммам Юнга λ.

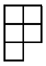
Стабилизатор перестановки, изображаемой заполненной диаграммой λ, состоит из циклических перенумераций внутри строк диаграммы λ и произвольных перестановок строк одинаковой длины между собой[7]. Поэтому число элементов в классе сопряжённости C_λ, отвечающем диаграмме λ, которая имеет k_ℓ строк длины ℓ (для каждого $1 \leqslant \ell \leqslant n$), равно

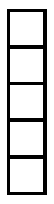
$$|C_\lambda| = \frac{|\mathfrak{S}_n|}{\mathrm{Stab}(\sigma)} = \frac{n!}{(k_1!)\cdot(k_2!)\cdots(k_n!)\cdot 1^{k_1}\cdot 2^{k_2}\cdots n^{k_n}}\,. \tag{1-10}$$

1.6.3. Пример: строение группы $\mathfrak{A}_5$. Элементы из $\mathfrak{A}_5$, попадающие в один класс сопряжённости во всей симметрической группе $\mathfrak{S}_5$, описываются диаграммами Юнга веса 5 с чётным числом строк чётной длины. Таких диаграмм четыре:

 — циклы длины 5, всего 24 шт.

 — циклы длины 3, всего 20 шт.

 — пары независимых транспозиций, всего 15 шт.

 — тождественная подстановка, 1 шт.

Упражнение 1.23. Убедитесь, что все циклы длины 3, равно как и все пары непересекающихся транспозиций сопряжены между собой посредством элементов из $\mathfrak{A}_5$, а вот циклы длины 5 образуют в $\mathfrak{A}_5$ два класса сопряжённости, представленные циклами (12345) и (21345).

Из сказанного вытекает, что в группе $\mathfrak{A}_5$ нет нетривиальных[8] нормальных подгрупп. В самом деле, поскольку нормальная подгруппа $H \subset \mathfrak{A}_5$ вместе с каждым элементом содержит и все его сопряжённые, $|H| = 1 + 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4$, где каждый ε_k равен либо 1, либо 0.

Упражнение 1.24. Проверьте, что $|H|$ делит $|\mathfrak{A}_5| = 60$ только если все ε_i либо одновременно равны нулю, либо одновременно равны 1.

Упражнение 1.25. Докажите, что внутренние автоморфизмы составляют подгруппу индекса 2 в группе всех автоморфизмов группы $\mathfrak{A}_5$.

Указание. Автоморфизм $\mathfrak{A}_5$ действует на циклах длины 5 и является внутренним тогда и только тогда, когда переводит каждый такой цикл в сопряжённый.

1.7. Простые группы. Группы без нетривиальных нормальных подгрупп называются *простыми*. Все циклические группы простого порядка являются простыми. Предыдущий пример показывает, что знакопеременная группа $\mathfrak{A}_5$ проста.

Упражнение 1.26. Докажите, что все знакопеременные группы $\mathfrak{A}_n$ с $n \geqslant 5$ просты.

Указание. Воспользуйтесь индукцией: вложите $\mathfrak{A}_{n-1}$ в $\mathfrak{A}_n$ как стабилизатор n-того элемента и проверьте, что любая нетривиальная нормальная подгруппа в $\mathfrak{A}_n$ имеет нетривиальное (и автоматически нормальное) пересечение с $\mathfrak{A}_{n-1}$.

[7] в последнем случае строки переставляются как единое целое, без перестановок содержимого внутри каждой строки

[8] т. е. отличных от $\{e\}$ и всей группы

Простые группы играют роль «элементарных блоков», из которых строятся все остальные группы. Поскольку ядро гомоморфизма является нормальной подгруппой, любой гомоморфизм переводит простую подгруппу либо в единицу, либо вкладывает в образ инъективно. Отсюда легко выводится, что любая конечная группа G допускает башню подгрупп

$$G = G^0 \supset G^1 \supset G^2 \supset \cdots \supset G^m \supset G^{m+1} = \{e\} ,$$

в которой каждая следующая подгруппа нормальна в предыдущей: $G^{i+1} \lhd G^i$, а все фактор группы G^i/G^{i+1} просты, причём набор этих простых факторов с точностью до перестановки не зависит от выбора башни.

В настоящее время все простые конечные группы перечислены. Создание этого перечня было закончено в 1981 году и потребовало более 100 лет довольно кропотливых трудов.