Глава седьмая

ПРОДОЛЖЕНИЕ ТЕОРИИ ГРУПП

Содержание. В §§ 48, 49 обсуждается некоторое обобщение понятия группы. §§ 50—52 содержат важные общие теоремы о нормальных подгруппах и «композиционных рядах», а §§ 53, 54 — специальные теоремы о группах подстановок, которые в дальнейшем потребуются лишь при изложении теории Галуа.

§ 48. Группы с операторами

В этом параграфе будет расширено понятие группы, благодаря чему все рассмотрения получат бо́льшую общность, нужную для дальнейших приложений (главы 17—19). Читатель, интересующийся лишь теорией Галуа, может спокойно пропустить ближайшие два параграфа; под группами (например, конечными группами) он может в дальнейшем подразумевать группы в прежнем смысле.

Пусть даны: во-первых, некоторая группа (в обычном смысле) $\mathfrak{G}$ с элементами a, b, ...; во-вторых, некоторое множество Ω новых объектов η, θ, ..., которые мы называем *операторами*. Пусть каждому θ и каждому a соответствует некоторое «произведение» θa («значение оператора θ, примененного к элементу a»); предполагается, что это произведение вновь принадлежит группе $\mathfrak{G}$. Далее предполагается, что каждый оператор θ «дистрибутивен», т. е.

$$\theta(ab) = \theta a \cdot \theta b. \tag{1}$$

Иначе говоря: «умножение» на оператор θ должно быть эндоморфизмом группы $\mathfrak{G}$[1]). Если выполнены все эти условия, то $\mathfrak{G}$ называется *группой с операторами*, а Ω — *областью операторов*.

Допустимая подгруппа группы $\mathfrak{G}$ (относительно области операторов Ω) — это такая подгруппа $\mathfrak{H}$, которая в свою очередь допускает Ω в качестве области операторов, т. е. если a принадлежит $\mathfrak{H}$, то каждый элемент θa также должен лежать в $\mathfrak{H}$. Если допустимая подгруппа является нормальной, то говорят о *допустимой нормальной подгруппе*.

Примеры. 1. Пусть операторами служат внутренние автоморфизмы группы $\mathfrak{G}$:

$$\theta a = cac^{-1}.$$

---

[1]) Отсюда следует, что при «умножении» на θ единичный элемент переходит в единичный, а обратный — в обратный.

Допустимыми являются те подгруппы, которые вместе с каждым своим элементом a содержат также и все элементы cac^{-1}, т. е. нормальные подгруппы.

2. Пусть операторами служат всевозможные автоморфизмы группы $\mathfrak{G}$. Допустимыми тогда будут те подгруппы, которые при каждом автоморфизме переходят в себя; такие подгруппы называются *характеристическими*.

3. Пусть $\mathfrak{G}$ — некоторое кольцо, рассматриваемое как группа относительно сложения. Пусть областью операторов Ω служит само это кольцо: произведение θa будем понимать просто как произведение в кольце. Тогда (1) является обычным дистрибутивным законом:

$$r(a+b)=ra+rb.$$

Допустимыми подгруппами здесь будут *левые идеалы*, т. е. те подгруппы, которые вместе с каждым a содержат все элементы ra.

4. Из соображений удобства можно операторы θ записывать справа от групповых элементов, т. е. вместо θa писать $a\theta$. Тогда (1) выглядит так:

$$(ab)\,\theta=a\theta\cdot b\theta.$$

Если, например, элементы некоторого кольца (рассматриваемого как аддитивная группа) рассматривать как правые операторы, где $a\theta$ вновь означает произведение в кольце, то в качестве допустимых подгрупп получатся *правые идеалы*.

5. Наконец, часть операторов можно записывать слева, а часть — справа. Например, если в качестве области операторов брать кольцо, действующее на свою аддитивную группу умножением, то его элементы можно рассматривать как *левые* и как *правые мультипликаторы*; в этом случае допустимыми подгруппами будут *двусторонние идеалы*.

6. В соответствии с традицией, *модулем* называют всякую аддитивно записанную абелеву группу. Модуль также может иметь ту или иную область операторов, которая в этом случае называется областью *мультипликаторов*; ее элементы подчинены условиям:

$$\theta(a+b)=\theta a+\theta b.$$

Как правило, оказывается так, что областью мультипликаторов служит некоторое *кольцо* и

$$\left.\begin{aligned}(\eta+\theta)\,a&=\eta a+\theta a,\\(\eta\theta)\,a&=\eta\,(\theta a)\end{aligned}\right\}\qquad(2)$$

(соответственно, если мультипликаторы пишутся справа, то $a(\eta\theta)=(a\eta)\,\theta$). Тогда $(\eta-\theta)\,a=\eta a-\theta a$ и $0\cdot a=0$ (первый нуль — это нулевой элемент кольца, второй нуль — нулевой элемент

модуля). Если $\mathfrak{o}$ — кольцо мультипликаторов, то говорят об *$\mathfrak{o}$-модулях* или о *модулях над кольцом* $\mathfrak{o}$. Если кольцо обладает единичным элементом ε, то очень часто предполагают, что этот единичный элемент одновременно является «единичным оператором», т. е. $\varepsilon \cdot a = a$ для всех a из $\mathfrak{G}$.

7. Любое (правое или левое) векторное пространство над телом K является K-модулем.

8. Совокупность всех эндоморфизмов абелевой группы (т. е. всех гомоморфных отображений в себя) является областью операторов, которая становится кольцом, если сумму и произведение двух гомоморфизмов определить формулами (2) (где справа знак плюс означает операцию над групповыми элементами). Это кольцо называется *кольцом эндоморфизмов* абелевой группы.

Из этих примеров становится ясным, насколько широки приложения групп с операторами.

Задача 1. Пересечение всех допустимых подгрупп является допустимой подгруппой. То же верно и для нормальных допустимых подгрупп.

Задача 2. Произведение $\mathfrak{A}\mathfrak{B}$ двух перестановочных допустимых подгрупп является допустимой подгруппой. В частном случае модулей: сумма $(\mathfrak{A}, \mathfrak{B})$ двух допустимых подмодулей является допустимым подмодулем.

§ 49. Операторные изоморфизмы и гомоморфизмы

Если $\mathfrak{G}$ и $\overline{\mathfrak{G}}$ — группы с одной и той же областью операторов Ω и задано отображение из $\mathfrak{G}$ в $\overline{\mathfrak{G}}$, при котором каждому элементу a соответствует некоторый элемент $\bar{a}$, а произведению ab — произведение $\bar{a}\bar{b}$, причем элементу θa соответствует элемент $\theta\bar{a}$, то отображение называется *операторным гомоморфизмом*. Если элементы-образы составляют всю группу $\overline{\mathfrak{G}}$, т. е. каждому элементу из $\overline{\mathfrak{G}}$ соответствует по крайней мере один элемент из $\mathfrak{G}$, то налицо гомоморфное отображение группы $\mathfrak{G}$ на группу $\overline{\mathfrak{G}}$. Если же каждому $\bar{a}$ соответствует ровно один a, то имеем *операторный изоморфизм* и пишем $\mathfrak{G} \cong \overline{\mathfrak{G}}$.

Если $\mathfrak{N}$ — допустимая нормальная подгруппа в $\mathfrak{G}$, то элементы ab некоторого смежного класса $\bar{a} = a\mathfrak{N}$ переходят при применении оператора θ в произведения $\theta a \cdot \theta b$, т. е. в элементы смежного класса $\theta a \cdot \mathfrak{N}$. Смежный класс $\overline{\theta a}$ мы называем произведением оператора θ и смежного класса $\bar{a}$. *Тем самым фактор-группа $\mathfrak{G}/\mathfrak{N}$ превращается в группу с той же областью операторов Ω, а отображение $a \longmapsto \bar{a}$ оказывается операторным гомоморфизмом.*

Обратно, если мы будем исходить из операторного гомоморфизма, то, как в § 10, получим теорему о гомоморфизме:

Если группа $\mathfrak{G}$ отображается на группу $\overline{\mathfrak{G}}$ посредством операторного гомоморфизма, то подмножество $\mathfrak{N}$ элементов из $\mathfrak{G}$, которые

соответствуют единичному элементу из $\overline{\mathfrak{G}}$, *является в* $\mathfrak{G}$ *допустимой нормальной подгруппой, а смежные классы по* $\mathfrak{N}$ *взаимно однозначно соответствуют элементам из* $\overline{\mathfrak{G}}$, *причем это последнее соответствие — операторный изоморфизм*:

$$\mathfrak{G}/\mathfrak{N} \cong \overline{\mathfrak{G}}.$$

То, что $\mathfrak{N}$ является нормальной подгруппой, мы знаем еще из § 10. То, что $\mathfrak{N}$ — допустимая подгруппа, очевидно: если a отображается на единичный элемент $\bar{e}$, то θa отображается на $\theta\bar{e} = \bar{e}$, т. е. вместе с a элемент θa также принадлежит группе $\mathfrak{N}$. То, что соответствие между смежными классами и элементами из $\overline{\mathfrak{G}}$ взаимно однозначно, мы уже знаем; то, что это соответствие — операторный изоморфизм, следует из того, что заданное отображение $\mathfrak{G} \to \overline{\mathfrak{G}}$ является операторным гомоморфизмом.

В случае аддитивно записанных групп с областью операторов $\mathfrak{o}$ ($\mathfrak{o}$-модулей, идеалов в $\mathfrak{o}$ и т. д.) операторный гомоморфизм называется *гомоморфизмом модулей*. Заметим, что и в этом случае θa переходит в $\theta\bar{a}$ и θ остается неизменным. В этом и состоит разница между гомоморфизмом модулей и гомоморфизмом колец, при котором ab переходит в $\bar{a}\bar{b}$. Рассмотрим пример: два левых идеала из кольца $\mathfrak{o}$ можно рассматривать как $\mathfrak{o}$-модули; произвольный операторный гомоморфизм переводит a в $\bar{a}$ и произведение ra — в произведение $r\bar{a}$ (r из $\mathfrak{o}$). Но эти же идеалы можно рассмотреть и как кольца, а кольцевой гомоморфизм сопоставляет произведению ra (r из идеала) не $r\bar{a}$, а $\bar{r}\bar{a}$.

Там, где в последующем речь зайдет просто о группах, будут иметься в виду группы с операторами. Под словами «подгруппы» и «нормальные подгруппы» всегда будут молчаливо подразумеваться допустимые подгруппы и допустимые нормальные подгруппы; слова «изоморфизм» и «гомоморфизм» будут означать «операторный изоморфизм» и «операторный гомоморфизм».

Задача 1. Идеалы (1) и (2) в кольце целых чисел изоморфны как модули, но не как кольца.

Задача 2. В кольце пар чисел (a_1, a_2) (§ 11, задача 1) идеалы, порожденные элементами (1, 0) и (0, 1), изоморфны как кольца, но не изоморфны как модули.

§ 50. Две теоремы об изоморфизме

Естественный гомоморфизм, который отображает группу $\mathfrak{G}$ на факторгруппу $\overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{N}$, отображает каждую подгруппу $\mathfrak{H}$ из $\mathfrak{G}$ на некоторую подгруппу $\overline{\mathfrak{H}}$ из $\overline{\mathfrak{G}}$ и тоже гомоморфно. Если исходить из $\overline{\mathfrak{H}}$ и найти в $\mathfrak{G}$ всю совокупность $\mathfrak{K}$ элементов, образы которых (или смежные классы которых) принадлежат $\overline{\mathfrak{H}}$, то, вообще говоря, в $\mathfrak{K}$ окажется больше элементов, чем в $\mathfrak{H}$,

потому что вместе с каждым a из $\mathfrak{H}$ множество $\mathfrak{K}$ содержит весь смежный класс $a\mathfrak{N}$. Обозначим через $\mathfrak{H}\mathfrak{N}$ группу, которая получается из всевозможных произведений ab, где a — элемент из $\mathfrak{H}$ и b — элемент из $\mathfrak{N}$ (ср. задачу 2 из § 48); тогда $\mathfrak{K} = \mathfrak{H}\mathfrak{N}$ и $\overline{\mathfrak{H}} = \mathfrak{H}\mathfrak{N}/\mathfrak{N}$. С другой стороны, если $\mathfrak{H}$ гомоморфно отображается на $\overline{\mathfrak{H}}$, то $\overline{\mathfrak{H}}$ изоморфна факторгруппе группы $\mathfrak{H}$ по некоторой нормальной подгруппе в $\mathfrak{H}$, которая состоит из элементов группы $\mathfrak{H}$, соответствующих единичному элементу, т. е. тех элементов из $\mathfrak{H}$, которые одновременно принадлежат и $\mathfrak{N}$. Отсюда получается первая теорема об изоморфизме:

Если $\mathfrak{N}$ — нормальная подгруппа группы $\mathfrak{G}$ и $\mathfrak{H}$ — подгруппа в $\mathfrak{G}$, то пересечение $\mathfrak{H} \cap \mathfrak{N}$ является нормальной подгруппой в $\mathfrak{H}$ и [1])

$$\mathfrak{H}\mathfrak{N}/\mathfrak{N} \cong \mathfrak{H}/(\mathfrak{H} \cup \mathfrak{N}).$$

Совокупность элементов, отображающихся в $\overline{\mathfrak{H}}$, тогда и только тогда совпадает с $\mathfrak{H}$, когда группа $\mathfrak{H}$ вместе с каждым своим элементом a содержит и весь смежный класс $a\mathfrak{N}$, т. е. тогда, когда

$$\mathfrak{H} \supseteq \mathfrak{N}.$$

Эти группы $\mathfrak{H} \supseteq \mathfrak{N}$ взаимно однозначно соответствуют описанным группам $\overline{\mathfrak{H}} = \mathfrak{H}/\mathfrak{N}$ в $\overline{\mathfrak{G}}$. Вместе с тем каждая подгруппа $\overline{\mathfrak{H}}$ в $\overline{\mathfrak{G}}$ соответствует подгруппе $\mathfrak{H} \supseteq \mathfrak{N}$, состоящей из всех элементов всех содержащихся в $\mathfrak{H}$ смежных классов по подгруппе $\mathfrak{N}$. Наконец, правым и левым смежным классам по подгруппе $\overline{\mathfrak{H}}$ в $\overline{\mathfrak{G}}$ соответствуют правые и левые смежные классы по $\mathfrak{H}$ в $\mathfrak{G}$. Следовательно, если $\overline{\mathfrak{H}}$ — нормальная подгруппа в $\overline{\mathfrak{G}}$, то $\mathfrak{H}$ — нормальная подгруппа в $\mathfrak{G}$, и наоборот. Аналогичное рассуждение, с некоторыми изменениями, используется при доказательстве второй теоремы об изоморфизме:

Если $\overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{N}$ и $\overline{\mathfrak{H}}$ — нормальная подгруппа в $\overline{\mathfrak{G}}$, то соответствующая подгруппа $\mathfrak{H}$ в $\mathfrak{G}$ является нормальной и

$$\mathfrak{G}/\mathfrak{H} \cong \overline{\mathfrak{G}}/\overline{\mathfrak{H}}. \tag{1}$$

Доказательство. Если $\mathfrak{G}$ гомоморфно отображается на $\overline{\mathfrak{G}}$, а $\overline{\mathfrak{G}}$, в свою очередь, на $\overline{\mathfrak{G}}/\overline{\mathfrak{H}}$, то и $\mathfrak{G}$ гомоморфно отображается на $\overline{\mathfrak{G}}/\overline{\mathfrak{H}}$. Следовательно, группа $\overline{\mathfrak{G}}/\overline{\mathfrak{H}}$ изоморфна факторгруппе группы $\mathfrak{G}$ по нормальной подгруппе, состоящей из тех элементов группы $\mathfrak{G}$, которые при гомоморфизме $\mathfrak{G} \to \overline{\mathfrak{G}}/\overline{\mathfrak{H}}$ переходят в единичный элемент, т. е. при первом гомоморфизме $\mathfrak{G} \to \overline{\mathfrak{G}}$ эти элементы переходят в группу $\overline{\mathfrak{H}}$. Этой нормальной подгруппой и является $\mathfrak{H}$. Доказательство окончено.

---

[1]) В случае модулей нужно, конечно, вместо $\mathfrak{H}\mathfrak{N}$ писать $(\mathfrak{H}, \mathfrak{N})$.

Изоморфизм (1) можно записать и так:

$$\mathfrak{G}/\mathfrak{H} \cong (\mathfrak{G}/\mathfrak{N})/(\mathfrak{H}/\mathfrak{N}).$$

Задача 1. С помощью первой теоремы об изоморфизме показать, что факторгруппа симметрической группы $\mathfrak{S}_1$ по четвертой подгруппе $\mathfrak{B}_4$ (§ 9, задача 4) изоморфна симметрической группе $\mathfrak{S}_3$.

Задача 2. Точно так же в любой группе подстановок, в которой есть не только четные подстановки, эти последние составляют нормальную подгруппу индекса 2.

Задача 3 Точно так же факторгруппа группы движений верхней евклидовой полуплоскости по нормальной подгруппе параллельных переносов изоморфна группе поворотов вокруг некоторой точки

§ 51. Нормальные и композиционные ряды

Группа $\mathfrak{G}$ называется *простой*, если в ней нет нормальных подгрупп, отличных от нее самой и единичной подгруппы.

Примеры. Группы простого порядка просты, так как порядок подгруппы должен быть делителем порядка всей группы; следовательно, в такой группе, кроме нее самой и единичной подгруппы, вообще нет подгрупп, а потому нет и нормальных подгрупп. Позднее будет доказано, что знакопеременная группа $\mathfrak{A}_n$ при $n > 4$ проста (§ 53). Любое одномерное векторное пространство является простым, потому что каждое собственное подпространство имеет размерность нуль и состоит из одного лишь нулевого вектора.

Нормальным рядом группы $\mathfrak{G}$ называется последовательность подгрупп в $\mathfrak{G}$:

$$\{\mathfrak{G} = \mathfrak{G}_0 \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_l = \mathfrak{E}\}, \tag{1}$$

в которой для $\nu = 1, \ldots, l$ подгруппа $\mathfrak{G}_\nu$ является нормальной в $\mathfrak{G}_{\nu-1}$. Число l называется *длиной* нормального ряда. Факторгруппы $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ носят название его *факторов*. Необходимо заметить следующее: длина есть не число членов ряда (1), а число факторов $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$.

Другой нормальный ряд

$$\{\mathfrak{G} \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_m = \mathfrak{E}\} \tag{2}$$

называется *уплотнением* первого ряда, если все подгруппы $\mathfrak{G}_i$ из (1) встречаются и в (2). Например, для группы $\mathfrak{S}_4$ (§ 6) ряд

$$\{\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{B}_4 \supset \mathfrak{E}\}$$

(см. § 9, задача 4) является уплотнением ряда

$$\{\mathfrak{S}_4 \supset \mathfrak{B}_4 \supset \mathfrak{E}\}.$$

В нормальном ряде любой член может повторяться сколь угодно много раз: $\mathfrak{G}_i = \mathfrak{G}_{i+1} = \ldots = \mathfrak{G}_k$. Если этого не происходит, говорят о нормальном ряде *без повторений*. Нормальный ряд

без повторений, который без повторений нельзя уплотнить, называется *композиционным*. Например, в симметрической группе $\mathfrak{S}_3$ ряд

$$\{\mathfrak{S}_3 \supset \mathfrak{A}_3 \supset \mathfrak{E}\}$$

является композиционным, а в группе $\mathfrak{S}_4$ композиционным будет ряд

$$\{\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{B}_4 \supset \{1,\ (12)\ (34)\} \supset \mathfrak{E}\}.$$

В обоих случаях исключена возможность дальнейших уплотнений, потому что индексы последующих нормальных подгрупп в предыдущих подгруппах являются простыми числами. Однако существуют и группы, в которых все нормальные ряды обладают уплотнениями; такие группы не имеют, следовательно, композиционных рядов. Примером может служить любая бесконечная циклическая группа: если в ней задан произвольный нормальный ряд без повторений

$$\{\mathfrak{G} \supset \mathfrak{G}_1 \supset \ldots \supset \mathfrak{G}_{l-1} \supset \mathfrak{E}\},$$

и $\mathfrak{G}_{l-1}$, например, имеет индекс m, т. е. $\mathfrak{G}_{l-1} = \{a^m\}$, то между $\mathfrak{G}_{l-1}$ и $\mathfrak{E}$ всегда есть еще одна подгруппа $\{a^{2m}\}$ индекса $2m$.

Нормальный ряд является композиционным тогда и только тогда, когда между двумя любыми его членами $\mathfrak{G}_{\nu-1}$ и $\mathfrak{G}_\nu$ нельзя включить какую-либо отличную от $\mathfrak{G}_{\nu-1}$ нормальную подгруппу, или, что согласно § 50 то же самое, когда группа $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ проста. Простые факторы $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ композиционного ряда называются *композиционными*. В обоих приведенных выше композиционных рядах все композиционные факторы являются циклическими подгруппами порядков 2, 3, соответственно 2, 3, 2, 2.

Два нормальных ряда называются *изоморфными*, если все факторы $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ одного из них могут быть отображены изоморфно на переставленные в определенном порядке факторы другого. Например, в циклической группе $\{a\}$ порядка 6 ряды

$$\{\{a\},\ \{a^2\},\ \mathfrak{E}\},$$
$$\{\{a\},\ \{a^3\},\ \mathfrak{E}\}$$

изоморфны, потому что факторы первого ряда являются циклическими порядков 2, 3, а факторы второго ряда — циклическими порядков 3, 2. Для обозначения изоморфизма нормальных рядов мы будем в дальнейшем использовать знак $\cong$.

Если цепь нормальных подгрупп

$$\{\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \ldots\}$$

заканчивается нормальной подгруппой $\mathfrak{A}$ группы $\mathfrak{G}$, отличной от $\mathfrak{E}$, то говорят о *нормальном ряде группы* $\mathfrak{G}$ *над подгруппой* $\mathfrak{A}$;

такому нормальному ряду соответствует нормальный ряд

$$\{\mathfrak{G}/\mathfrak{A} \supseteq \mathfrak{G}_1/\mathfrak{A} \supseteq \ldots \supseteq \mathfrak{A}/\mathfrak{A} = \mathfrak{E}\}$$

факторгруппы $\mathfrak{G}/\mathfrak{A}$, и наоборот. Факторы второго ряда, согласно второй теореме об изоморфизме, изоморфны факторам первого.

Если нормальные ряды

$$\{\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_r = \mathfrak{E}\}$$

и

$$\{\mathfrak{G} \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_r = \mathfrak{E}\}$$

изоморфны, то для каждого уплотнения первого ряда можно найти изоморфное ему уплотнение второго. Действительно, каждые фактор $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ изоморфен вполне определенному фактору $\mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu$; тем самым каждому нормальному ряду для $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ соответствует изоморфный нормальный ряд для $\mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu$, а потому и каждому нормальному ряду группы $\mathfrak{G}_{\nu-1}$ над подгруппой $\mathfrak{G}_\nu$ соответствует изоморфный ряд подгруппы $\mathfrak{H}_{\mu-1}$ над подгруппой $\mathfrak{H}_\mu$.

Теперь мы можем доказать основную теорему о нормальных рядах, принадлежащую О. Шрайеру:

Два произвольных нормальных ряда произвольной группы $\mathfrak{G}$:

$$\{\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{G}_r = \mathfrak{E}\},$$
$$\{\mathfrak{G} \supseteq \mathfrak{H}_1 \supseteq \mathfrak{H}_2 \supseteq \ldots \supseteq \mathfrak{H}_s = \mathfrak{E}\}$$

обладают изоморфными уплотнениями:

$$\{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{E}\} \cong$$
$$\cong \{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_2 \supseteq \ldots \supseteq \mathfrak{E}\}.$$

Доказательство. Для $r=1$ или $s=1$ теорема очевидна, потому что в этом случае один из рядов имеет вид $\{\mathfrak{G} \supseteq \mathfrak{E}\}$ и, следовательно, другой является его уплотнением.

Докажем сначала эту теорему для $s=2$ индукцией по r, а потом для произвольного s индукцией по s.

Для $s=2$ второй ряд выглядит так:

$$\{\mathfrak{G} \supseteq \mathfrak{H} \supseteq \mathfrak{E}\}.$$

Положим $\mathfrak{D} = \mathfrak{G}_1 \cap \mathfrak{H}$ и $\mathfrak{P} = \mathfrak{G}_1\mathfrak{H}$; тогда $\mathfrak{P}$ и $\mathfrak{D}$ — нормальные подгруппы в $\mathfrak{G}$. Конечно, может оказаться, что $\mathfrak{P} = \mathfrak{G}$ или $\mathfrak{D} = \mathfrak{E}$. По предположению индукции, ряды длины $r-1$ и длины 2

$$\{\mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{G}_r = \mathfrak{E}\} \quad \text{и} \quad \{\mathfrak{G}_1 \supseteq \mathfrak{D} \supseteq \mathfrak{E}\}$$

обладают изоморфными уплотнениями:

$$\{\mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{E}\} \cong \{\mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{D} \supseteq \ldots \supseteq \mathfrak{E}\}. \qquad (3)$$

В силу первой теоремы об изоморфизме

$$\mathfrak{P}/\mathfrak{H} \cong \mathfrak{G}_1/\mathfrak{D} \quad \text{и} \quad \mathfrak{P}/\mathfrak{G}_1 \cong \mathfrak{H}/\mathfrak{D};$$

следовательно,

$$\{\mathfrak{P} \supseteq \mathfrak{G}_1 \supseteq \mathfrak{D} \supseteq \mathfrak{E}\} \cong \{\mathfrak{P} \supseteq \mathfrak{H} \supseteq \mathfrak{D} \supseteq \mathfrak{E}\}. \tag{4}$$

Правая часть в (3) задает уплотнение левой части из (4), для которого можно найти изоморфное уплотнение правой части:

$$\{\mathfrak{P} \supseteq \mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{D} \supseteq \ldots \supseteq \mathfrak{E}\} \cong \\ \cong \{\mathfrak{P} \supseteq \ldots \supseteq \mathfrak{H} \supseteq \mathfrak{D} \supseteq \ldots \supseteq \mathfrak{E}\}. \tag{5}$$

Из (3) и (5) следует изоморфизм

$$\{\mathfrak{G} \supseteq \mathfrak{P} \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{E}\} \cong \\ \cong \{\mathfrak{G} \supseteq \mathfrak{P} \supseteq \ldots \supseteq \mathfrak{H} \supseteq \mathfrak{D} \supseteq \ldots \supseteq \mathfrak{E}\},$$

чем и доказывается теорема для случая $s = 2$.

В случае произвольного s согласно доказанному мы можем так уплотнить ряд $\{\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \ldots\}$, чтобы он стал изоморфным некоторому уплотнению ряда $\{\mathfrak{G} \supseteq \mathfrak{H}_1 \supseteq \mathfrak{E}\}$:

$$\{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{E}\} \cong \\ \cong \{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{E}\}. \tag{6}$$

Входящий в правую часть отрезок ряда $\{\mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{E}\}$ и ряд $\{\mathfrak{H}_1 \supseteq \mathfrak{H}_2 \supseteq \ldots \supseteq \mathfrak{H}_s = \mathfrak{E}\}$ согласно предположению индукции обладают изоморфными уплотнениями:

$$\{\mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{E}\} \cong \{\mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_2 \supseteq \ldots \supseteq \mathfrak{E}\}. \tag{7}$$

Левая часть в (7) дает некоторое уплотнение правой части в (6), для которого можно найти изоморфное уплотнение левой части в (6). Следовательно,

$$\{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{E}\} \\ \cong \{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{E}\} \\ [\text{ввиду } (7)] \cong \{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_2 \supseteq \ldots \supseteq \mathfrak{E}\}.$$

Тем самым теорема полностью доказана [1]).

Если в двух изоморфных рядах вычеркнуть все повторения, то останутся изоморфные ряды. Следовательно, в основной теореме уплотнения, о которых идет речь, можно считать уплотнениями без повторений.

Из основной теоремы о нормальных рядах немедленно получаются две следующие теоремы о группах, обладающих композиционными рядами.

1. Теорема Жордана—Гёльдера. *Любые два композиционных ряда одной и той же группы $\mathfrak{G}$ изоморфны.*

---

[1]) Другое доказательство предложено в работе Цассенхауз (Zassenhaus H.). — Abh. math. Sem Hamburg, 1934, **10**, S. 106.

Действительно, эти ряды совпадают со своими уплотнениями без повторений.

2. *Если $\mathfrak{G}$ обладает композиционным рядом, то каждый ее нормальный ряд можно уплотнить до композиционного. В частности, через каждую нормальную подгруппу проходит некоторый композиционный ряд.*

Группа называется *разрешимой*, если у нее есть нормальный ряд, в котором все факторы абелевы. (Примеры: группы $\mathfrak{S}_3$ и $\mathfrak{S}_4$ — см. выше.)

Из основной теоремы следует, что у разрешимой группы любой нормальный ряд уплотняется до нормального ряда с абелевыми факторами. В частности, если такая группа обладает композиционным рядом, то все факторы последнего — абелевы группы.

Задача 1. Всякая конечная группа обладает композиционным рядом

Задача 2. Построить все композиционные ряды циклической группы порядка 20.

Задача 3. Абелева группа (без операторов) является простой лишь тогда, когда она циклична и имеет простой порядок.

Задача 4. В любом композиционном ряде конечной разрешимой группы композиционные факторы цикличны и имеют простой порядок.

§ 52. Группы порядка p^n

Под *центром* группы $\mathfrak{G}$ или кольца $\mathfrak{R}$ подразумевается множество таких элементов z этой группы или этого кольца, которые перестановочны со всеми элементами:

$$zg = gz \text{ для всех } g \text{ из } \mathfrak{G} \text{ или } \mathfrak{R}.$$

Центр группы $\mathfrak{G}$ является группой и даже нормальной подгруппой в $\mathfrak{G}$. Центром кольца является подкольцо.

Пусть p — простое число, n — натуральное число и $\mathfrak{G}$ — некоторая группа порядка p^n. Покажем, что центр группы $\mathfrak{G}$ не может состоять только из единичного элемента.

Рассмотрим разбиение группы $\mathfrak{G}$ на классы сопряженных элементов (§ 9, задача 7). Чему равно число элементов в одном таком классе?

Пусть a — произвольный групповой элемент. Два элемента bab^{-1} и cac^{-1}, сопряженные с a, равны тогда и только тогда, когда произведение $b^{-1}c$ перестановочно с a:

$$\text{из } bab^{-1} = cac^{-1} \text{ следует } a(b^{-1}c) = (b^{-1}c)a.$$

Групповые элементы, перестановочные с a, составляют некоторую подгруппу $\mathfrak{H}$, называемую *нормализатором элемента* a. Если $b^{-1}c$ принадлежит группе $\mathfrak{H}$, то c лежит в смежном классе $b\mathfrak{H}$. Обратно: если c лежит в $b\mathfrak{H}$, то можно положить $c = bh$ и тогда

$$cac^{-1} = bha(bh)^{-1} = bahh^{-1}b^{-1} = bab^{-1}.$$

Таким образом, каждому смежному классу $b\mathfrak{H}$ соответствует некоторый сопряженный элемент bab^{-1}, и наоборот. Число различных элементов, сопряженных с элементом a, равно числу смежных классов, т. е. равно индексу группы $\mathfrak{H}$ в группе $\mathfrak{G}$. Индекс всегда является делителем порядка группы. В частности, если a — элемент центра, то $\mathfrak{H}=\mathfrak{E}$ и класс состоит из одного лишь элемента a. Во всех остальных случаях число элементов класса больше единицы.

Пусть теперь $\mathfrak{G}$ — некоторая *p-группа*, т. е. группа порядка p^n. Тогда число элементов в любом классе равно делителю числа p^n, т. е. является степенью числа p. Порядок группы $\mathfrak{G}$ равен сумме мощностей отдельных классов, т. е. сумме некоторых степеней числа p:

$$p^h = 1 + p^i + p^j + \ldots + p^m. \tag{1}$$

Если бы единица была единственным элементом центра, то в сумме справа участвовало бы лишь одно слагаемое 1, а все остальные делились бы на p. Тогда левая часть в (1) делилась бы на p, а правая — нет, что невозможно. Следовательно, *центр любой p-группы не может состоять из одного единичного элемента.*

Может оказаться так, что центр $\mathfrak{Z}_1$ является всей группой, тогда группа $\mathfrak{G}$ абелева. В противном же случае можно построить факторгруппу $\overline{\mathfrak{G}}=\mathfrak{G}/\mathfrak{Z}_1$. Она вновь является p-группой и, следовательно, обладает неединичным центром $\overline{\mathfrak{Z}}=\mathfrak{Z}_2/\mathfrak{Z}_1$. Продолжая таким образом, мы получим возрастающую последовательность центров

$$\mathfrak{E} \subset \mathfrak{Z}_1 \subset \mathfrak{Z}_2 \subset \ldots$$

Так как каждый ее член имеет больший порядок, чем предыдущий, последовательность должна закончиться через некоторое конечное число членов равенством $\mathfrak{Z}_n=\mathfrak{G}$. Факторгруппы $\mathfrak{Z}_k/\mathfrak{Z}_{k-1}$ все абелевы; поэтому:

Каждая группа порядка p^n разрешима.

§ 53. Прямые произведения

Группа $\mathfrak{G}$ называется *прямым произведением* подгрупп $\mathfrak{A}$ и $\mathfrak{B}$, если выполнены следующие условия:

А1. $\mathfrak{A}$ и $\mathfrak{B}$ — нормальные подгруппы в $\mathfrak{G}$;

А2. $\mathfrak{G}=\mathfrak{A}\mathfrak{B}$;

А3. $\mathfrak{A}\cap\mathfrak{B}=\mathfrak{E}$.

Эквивалентными этому являются требования:

Б1. Каждый элемент группы $\mathfrak{G}$ является произведением

$$g=ab, \quad a\in\mathfrak{A}, \quad b\in\mathfrak{B}. \tag{1}$$

Б2. Множители a и b однозначно определяются элементом g.

Б3. Каждый элемент подгруппы $\mathfrak{A}$ перестановочен с каждым элементом подгруппы $\mathfrak{B}$.

Из условий А *следуют условия* Б. Действительно, Б1 следует из А2. Условие Б2 получается так: если

$$g = a_1 b_1 = a_2 b_2,$$

то

$$a_2^{-1} a_1 = b_2 b_1^{-1};$$

элемент $a_2^{-1} a_1$ должен принадлежать как $\mathfrak{A}$, так и $\mathfrak{B}$, а потому в силу А3 он оказывается равным единице; следовательно,

$$a_1 = a_2, \quad b_1 = b_2$$

и установлена единственность представления (1). Условие Б3 следует из того, что $aba^{-1}b^{-1}$ в силу А1 принадлежит как $\mathfrak{A}$, так и $\mathfrak{B}$, а потому в силу А3 этот элемент равен единичному.

Из условий Б *следуют условия* А. То, что подгруппа $\mathfrak{A}$ является нормальной, получается так:

$$g\mathfrak{A}g^{-1} = ab\mathfrak{A}b^{-1}a^{-1} = a\mathfrak{A}a^{-1} = \mathfrak{A} \text{ [в силу Б3].}$$

Условие А2 следует из Б1. Условие А3 получается так: если c — элемент пересечения $\mathfrak{A} \cap \mathfrak{B}$, то c представляется двумя способами как произведение некоторого элемента из $\mathfrak{A}$ и некоторого элемента из $\mathfrak{B}$:

$$c = 1 \cdot c = c \cdot 1.$$

В силу единственности [Б2] должно выполняться равенство $c = 1$. Условие А3 получено.

Произведение $\mathfrak{A}\mathfrak{B}$, когда оно является прямым, будет обозначаться через $\mathfrak{A} \times \mathfrak{B}$. В случае аддитивных групп (модулей) пишут $(\mathfrak{A}, \mathfrak{B})$ для обозначения суммы и $\mathfrak{A} + \mathfrak{B}$ — для обозначения прямой суммы.

Если известно строение групп $\mathfrak{A}$ и $\mathfrak{B}$, то известно строение и группы $\mathfrak{G}$, потому что любые два элемента $g_1 = a_1 b_1$ и $g_2 = a_2 b_2$ перемножаются путем умножения сомножителей:

$$g_1 g_2 = a_1 a_2 \cdot b_1 b_2.$$

Группа $\mathfrak{G}$ называется *прямым произведением нескольких своих подгрупп* $\mathfrak{G} = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \ldots \times \mathfrak{A}_n$, если выполнены следующие условия:

А′1. Все $\mathfrak{A}_\nu$ являются нормальными подгруппами в $\mathfrak{G}$.

А′2. $\mathfrak{A}_1 \mathfrak{A}_2 \ldots \mathfrak{A}_n = \mathfrak{G}$.

А′3. $(\mathfrak{A}_1 \mathfrak{A}_2 \ldots \mathfrak{A}_{\nu-1}) \cap \mathfrak{A}_\nu = \mathfrak{E}$ $(\nu = 2, 3, \ldots, n)$.

Если эти условия выполнены, то группы $\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1}$ являются нормальными подгруппами и в их произведении $\mathfrak{A}_1 \mathfrak{A}_2 \ldots \mathfrak{A}_{n-1}$, так что это произведение согласно тому же определению является прямым. Далее, $\mathfrak{A}_1 \mathfrak{A}_2 \ldots \mathfrak{A}_{n-1}$, как произведение нормальных под-

групп, вновь является нормальной подгруппой в $\mathfrak{G}$ и

$$(\mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{n-1}) \cap \mathfrak{A}_n = \mathfrak{E}.$$

Следовательно,

$$\mathfrak{G} = (\mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{n-1}) \times \mathfrak{A}_n = \mathfrak{B}_n \times \mathfrak{A}_n, \tag{2}$$

где

$$\mathfrak{B}_n = \mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{n-1} = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \ldots \times \mathfrak{A}_{n-1}.$$

С помощью (2) прямые произведения можно определять рекуррентно. Если к произведению $\mathfrak{G} = \mathfrak{B}_n \times \mathfrak{A}_n$ применить определение Б, то индукцией по n получится:

Б′. *Каждый элемент g группы $\mathfrak{G}$ однозначно представим как произведение*

$$g = a_1a_2 \ldots a_n \quad (a_\nu \in \mathfrak{A}_\nu),$$

и каждый элемент из $\mathfrak{A}_\mu$ перестановочен с каждым элементом из $\mathfrak{A}_\nu$ $(\mu \neq \nu)$.

Из Б′ в свою очередь, следуют условия А′. Действительно, положим

$$\mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{\nu-1}\mathfrak{A}_{n+1} \ldots \mathfrak{A}_n = \mathfrak{B}_\nu;$$

тогда из Б′ для произвольного ν получается

$$\mathfrak{G} = \mathfrak{A}_\nu \times \mathfrak{B}_\nu; \tag{3}$$

следовательно, каждая подгруппа $\mathfrak{A}_\nu$ является нормальной в $\mathfrak{G}$ и

$$\mathfrak{A}_\nu \cap \mathfrak{B}_\nu = \mathfrak{E}.$$

Последнее утверждение содержит нечто большее, чем условие А′3.

Из (3) согласно первой теореме об изоморфизме следует, что

$$\mathfrak{G}/\mathfrak{A}_\nu \cong \mathfrak{B}_\nu; \quad \mathfrak{G}/\mathfrak{B}_\nu \cong \mathfrak{A}_\nu.$$

Группы

$$\left.\begin{aligned} \mathfrak{G} &= \mathfrak{A}_1 \times \mathfrak{A}_2 \times \ldots \times \mathfrak{A}_n, \\ \mathfrak{G}_1 &= \mathfrak{A}_1 \times \mathfrak{A}_2 \times \ldots \times \mathfrak{A}_{n-1}, \\ &\ldots\ldots\ldots\ldots\ldots \\ \mathfrak{G}_{n-1} &= \mathfrak{A}_1, \\ \mathfrak{G}_n &= \mathfrak{E} \end{aligned}\right\} \tag{4}$$

составляют нормальный ряд группы $\mathfrak{G}$ с факторами $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu \cong \mathfrak{A}_{n-\nu+1}$. Если группы $\mathfrak{A}_\nu$ обладают композиционными рядами, то и $\mathfrak{G}$ обладает композиционным рядом, длина которого является суммой длин отдельных факторов.

Задача 1. Если $\mathfrak{G} = \mathfrak{A} \times \mathfrak{B}$, $\mathfrak{G}'$ — подгруппа в $\mathfrak{A}$ и $\mathfrak{G}' \supseteq \mathfrak{A}$, то $\mathfrak{G}' = \mathfrak{A} \times \mathfrak{B}'$, где $\mathfrak{B}'$ обозначает пересечение $\mathfrak{G}'$ и $\mathfrak{B}$.

Задача 2. Любая циклическая группа порядка $n = rs$ с $(r, s) = 1$ является прямым произведением своих подгрупп порядков s и r.

Задача 3. Конечная циклическая группа является прямым произведением своих подгрупп, порядки которых являются наибольшими возможными степенями простых чисел.

Группа $\mathfrak{G}$ называется *вполне приводимой*, если она является прямым произведением простых групп. В этом случае соответствующий нормальный ряд (4) является композиционным рядом. Согласно теореме Жордана — Гёльдера композиционные факторы $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu \cong \mathfrak{A}_{n-\nu+1}$ определены однозначно с точностью до изоморфизма и порядка следования.

Теорема. *В любой вполне приводимой группе $\mathfrak{G}$ каждая нормальная подгруппа является прямым сомножителем, т. е. для каждой нормальной подгруппы $\mathfrak{H}$ существует разложение $\mathfrak{G} = \mathfrak{H} \times \mathfrak{B}$.*

Доказательство. Из $\mathfrak{G} = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \ldots \times \mathfrak{A}_n$ следует, что

$$\mathfrak{G} = \mathfrak{H} \cdot \mathfrak{G} = \mathfrak{H} \cdot \mathfrak{A}_1 \cdot \mathfrak{A}_2 \cdot \ldots \cdot \mathfrak{A}_n. \tag{5}$$

С каждым из сомножителей $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ можно проделать следующую операцию: множитель либо зачеркивается, либо предшествующий ему знак $\cdot$ заменяется на знак $\times$ прямого произведения. Действительно, пересечение рассматриваемой группы $\mathfrak{A}_k$ с произведением $\Pi = \mathfrak{H} \cdot \mathfrak{A}_1 \cdot \ldots \cdot \mathfrak{A}_{k-1}$ является нормальной подгруппой в $\mathfrak{A}_k$, поэтому оно равно либо $\mathfrak{A}_k$, либо $\mathfrak{E}$. В первом случае $\Pi \cap \mathfrak{A}_k = \mathfrak{A}_k$ и $\mathfrak{A}_k \subseteq \Pi$, т. е. множитель $\mathfrak{A}_k$ в произведении $\Pi\mathfrak{A}_k$ исчезает. Во втором случае произведение $\Pi \cdot \mathfrak{A}_k$ является прямым: $\Pi \cdot \mathfrak{A}_k = \Pi \times \mathfrak{A}_k$.

Согласно доказанному выше произведение (5) после вычеркивания ненужных групп $\mathfrak{A}$ приобретает форму прямого произведения:

$$\mathfrak{G} = \mathfrak{H} \times \mathfrak{A}_i \times \mathfrak{A}_j \times \ldots \times \mathfrak{A}_k.$$

Отсюда следует требуемое.

§ 54. Групповые характеры

Пусть $\mathfrak{G}$ — некоторая группа и K — некоторое поле. Под *характером* группы $\mathfrak{G}$ в поле K понимается любое гомоморфное отображение группы $\mathfrak{G}$ в мультипликативную группу поля K. Другими словами: характер σ группы $\mathfrak{G}$ в поле K — это некоторая функция элементов из $\mathfrak{G}$ со значениями в поле K, отличными от нуля, обладающая следующим свойством:

$$\sigma(xy) = \sigma(x)\,\sigma(y). \tag{1}$$

Из (1), как обычно, следует, что

$$\sigma(x_1 \ldots x_n) = \sigma(x_1) \ldots \sigma(x_n),$$
$$\sigma(x^n) = \sigma(x)^n,$$
$$\sigma(e) = 1,$$
$$\sigma(x^{-1}) = \sigma(x)^{-1}.$$

Если σ и τ — характеры, то с помощью равенства

$$\sigma\tau(x) = \sigma(x)\tau(x)$$

определяется произведение отображений $\sigma\tau$; оно тоже является характером. Относительно такого умножения характеры группы $\mathfrak{G}$ в поле K образуют абелеву группу $\mathfrak{G}'$, *группу характеров группы* $\mathfrak{G}$ *в поле* K.

Теорема о независимости. *Различные характеры* $\sigma_1, \ldots, \sigma_n$ *группы* $\mathfrak{G}$ *в поле* K *всегда линейно независимы, т. е. если в поле* K *выполняется равенство*

$$c_1\sigma_1(x) + \ldots + c_n\sigma_n(x) = 0 \tag{2}$$

для всех x *из* $\mathfrak{G}$, *то все коэффициенты* c_i *равны нулю.*

Доказательство. (По книге: Артин (Artin E.). Galoissche Theorie. — Leipzig, 1959, S. 28.) Для $n=1$ из $c_1\sigma_1(x)=0$ сразу следует, что $c_1=0$. Следовательно, можно начать индукцию по n и предположить, что утверждение справедливо для $n-1$ характеров.

Заменим в (2) элемент x на ax, где a — промзвольный элемент группы $\mathfrak{G}$; тогда получится равенство

$$c_1\sigma_1(a)\sigma_1(x) + \ldots + c_n\sigma_n(a)\sigma_n(x) = 0. \tag{3}$$

Вычтем отсюда равенство (2), умноженное на $\sigma_n(a)$:

$$c_1\{\sigma_1(a) - \sigma_n(a)\}\sigma_1(x) + \ldots$$
$$\ldots + c_{n-1}\{\sigma_{n-1}(a) - \sigma_n(a)\}\sigma_{n-1}(x) = 0. \tag{4}$$

Согласно индуктивному предположению характеры $\sigma_1, \ldots, \sigma_{n-1}$ линейно независимы; следовательно, все коэффициенты в (4) должны быть нулевыми:

$$c_i\{\sigma_i(a) - \sigma_n(a)\} = 0 \quad \text{для} \quad i = 1, \ldots, n-1. \tag{5}$$

Так как σ_i и σ_n — различные характеры, для каждого фиксированного i можно так выбрать элемент a, чтобы было

$$\sigma_i(a) \neq \sigma_n(a).$$

Тогда из (5) следует, что

$$c_i = 0 \text{ для } i = 1, \ldots, n-1.$$

Подставим это в (2); тогда окажется, что $c_n = 0$, чем и доказывается требуемое.

Следствие. *Если* $\sigma_1, \ldots, \sigma_n$ — *различные изоморфные отображения поля* K' *в поле* K, *то все они линейно независимы.* Действительно, можно рассматривать $\sigma_1, \ldots, \sigma_n$ как характеры мультипликативной группы поля K' в поле K.

Особенно важны характеры абелевых групп.

Пример 1. Пусть $\mathfrak{G}$ — циклическая группа порядка n. Опишем характеры группы $\mathfrak{G}$ в поле K.

Если a — образующий элемент группы $\mathfrak{G}$ и χ — произвольный характер, то положим

$$\chi(a) = \zeta. \tag{6}$$

Произвольный элемент из $\mathfrak{G}$ является некоторой степенью

$$x = a^z \quad (z = 0,\ 1,\ \ldots,\ n-1).$$

Из (6) следует, что

$$\chi(x) = \chi(a^z) = \zeta^z. \tag{7}$$

Далее, $a^n = e$; следовательно, $\chi(a^n) = \zeta^n = 1$, а потому ζ — корень n-й степени из единицы. Обратно, каждому корню n-й степени из единицы ζ в поле K соответствует некоторый характер χ, определяемый равенством (7).

Согласно задаче 4 из § 42 корни n-й степени из единицы образуют в поле K циклическую группу, порядок n' которой является делителем числа n. Следовательно, характеры χ образуют циклическую группу порядка n', где $n' \mid n$.

Предположим, что K содержит все корни n-й степени из единицы и n не делится на характеристику поля K; тогда $n' = n$ и, следовательно, группа характеров $\mathfrak{G}'$ группы $\mathfrak{G}$ изоморфна самой группе $\mathfrak{G}$. Пусть, скажем, η — примитивный корень n-й степени из единицы в поле K. Тогда равенство

$$\sigma(a^z) = \eta^z$$

определяет характер σ и все характеры χ_k являются степенями характера σ:

$$\chi_k = \sigma^k \quad (k = 0,\ 1,\ \ldots,\ n-1).$$

Следовательно,

$$\chi_k(a^z) = \eta^{kz}. \tag{8}$$

При фиксированном k характер χ_k можно рассматривать как функцию от z, а при фиксированном z — как функцию от k. Так получаются все характеры из $\mathfrak{G}'$. *Следовательно, опять группа характеров $\mathfrak{G}'$ изоморфна группе $\mathfrak{G}$.*

В конце § 42 было доказано, что

$$1 + \zeta + \ldots + \zeta^{n-1} = \begin{cases} n & \text{при } \zeta = 1, \\ 0 & \text{при } \zeta \neq 1 \end{cases}$$

для любого корня n-й степени из единицы ζ. Отсюда в силу (8) следует, что

$$\sum_k \chi_k(a^z) = \begin{cases} n, & z = 0, \\ 0, & z \neq 0, \end{cases} \tag{9}$$

и

$$\sum_z \chi_k(a^z) = \begin{cases} n, & k = 0, \\ 0, & k \neq 0, \end{cases} \tag{10}$$

или, записывая иначе,

$$\sum_{\chi} \chi(x) = \begin{cases} n, & x = e, \\ 0, & x \neq e, \end{cases} \tag{11}$$

$$\sum_{x} \chi(x) = \begin{cases} n, & \chi = 1, \\ 0, & \chi \neq 1. \end{cases} \tag{12}$$

Из (11) следует, если x заменить на xy, что

$$\sum_{\chi} \chi(x)\chi(y) = \begin{cases} n, & \text{если } y = x^{-1}, \\ 0 & \text{в остальных случаях.} \end{cases} \tag{13}$$

Точно так же из (12) следует:

$$\sum_{x} \chi'(x)\chi(x) = \begin{cases} n, & \text{если } \chi' = \chi^{-1}, \\ 0 & \text{в остальных случаях.} \end{cases} \tag{14}$$

Введем матрицу A с элементами

$$a_{zk} = \chi_k(a^z) \qquad (z,\ k = 0,\ 1,\ \ldots,\ n-1) \tag{15}$$

и матрицу B с элементами

$$b_{kz} = \frac{1}{n}\chi_k(a^{-z}); \tag{16}$$

тогда равенство (13) можно записать в виде

$$AB = 1,$$

а равенство (14) — в виде

$$BA = 1.$$

Оба равенства говорят о том, что B — обратная матрица для матрицы A.

Функции $f(x)$, которые отображают группу $\mathfrak{G}$ в поле K, определяются n значениями

$$f(e),\ f(a),\ f(a^2),\ \ldots,\ f(a^{n-1})$$

и, следовательно, образуют n-мерное векторное пространство над K. Согласно теореме о независимости n характеров $\chi_k(x)$ линейно независимы. Следовательно, каждую функцию $f(x)$ можно выразить через $\chi_k(x)$:

$$f(x) = \sum_{k} c_k\chi_k(x). \tag{17}$$

Положим $f(x) = f(a^z) = g(z)$; тогда вместо (17) можно записать

$$g(z) = \sum_{k} c_k a_{zk} = \sum_{k} c_k \eta^{kz}. \tag{18}$$

Решение этой системы уравнений с учетом того, что матрица B —

обратная для A, выглядит так:

$$c_k = \sum_z b_{kz} g(z) = \frac{1}{n} \sum_z \eta^{-kz} g(z). \tag{19}$$

В частности, возьмем в качестве K поле комплексных чисел и положим

$$\eta = e^{\frac{2\pi i}{n}};$$

тогда (18) превратится в конечный ряд Фурье

$$g(z) = \sum_{k=0}^{n-1} c_k e^{2\pi i \frac{k}{n} z}, \tag{20}$$

где

$$c_k = \frac{1}{n} \sum_{z=0}^{n-1} e^{-2\pi i \frac{k}{n} z} g(z). \tag{21}$$

Пример 2. Пусть $\mathfrak{G}$ — прямое произведение циклических групп $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_r$ порядков $n_1, \ldots, n_r$. Будет предполагаться, что наименьшее общее кратное v порядков $n_1, \ldots, n_r$ не делится на характеристику поля K, а само поле K содержит корни v-й степени из единицы. Определим все характеры группы $\mathfrak{G}$ в поле K.

Пусть $a_1, \ldots, a_r$ — порождающие элементы групп $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_r$ и η_i $(i = 1, \ldots, r)$ — примитивный корень n_i-й степени из единицы. Если χ — произвольный характер группы $\mathfrak{G}$, то $\chi(a_i)$ для каждого i является корнем n_i-й степени из единицы и

$$\chi(a_i) = \eta_i^{k_i}.$$

Каждый элемент x из $\mathfrak{G}$ однозначно представляется в виде

$$x = a_1^{z_1} a_2^{z_2} \ldots a_r^{z_r}$$

и

$$\chi(x) = \chi(a_1)^{z_1} \ldots \chi(a_r)^{z_r} = \eta_1^{k_1 z_1} \eta_2^{k_2 z_2} \ldots \eta_r^{k_r z_r}.$$

В качестве k_i можно взять любое из чисел $0, 1, \ldots, n_i - 1$; следовательно, имеется $n = n_1 \ldots n_r$ характеров. Выберем одно из k_i равным 1, а все остальные равными 0; в результате получится характер σ_i. Произвольный характер представляется в виде

$$\chi_{k_1, \ldots, k_r} = \sigma_1^{k_1} \sigma_2^{k_2} \ldots \sigma_r^{k_r}.$$

Группа характеров $\mathfrak{G}'$ является, следовательно, прямым произведением циклических групп порядков $n_1, \ldots, n_r$, т. е. изоморфна группе $\mathfrak{G}$. Вновь оказалось так, что $\mathfrak{G}'$ и $\mathfrak{G}$ изоморфны.

Точно так же, как раньше, доказываются равенства (11) и (12) и из них выводятся (13)—(19). В равенстве (15) нужно, конечно, вместо a^z писать

$$a_1^{z_1} \ldots a_r^{z_r},$$

а в (18) вместо η^{kz} —

$$\eta_1^{k_1 z_1} \ldots \eta_r^{k_r z_r}.$$

Позднее мы докажем основную теорему об абелевых группах, которая утверждает, что любая абелева группа с конечным множеством порождающих элементов, в частности, любая конечная абелева группа, является прямым произведением циклических групп. Следовательно, доказанные выше формулы выполняются в любой конечной абелевой группе.

Теория характеров может быть перенесена и на бесконечные абелевы группы. Двойственность между $\mathfrak{G}$ и $\mathfrak{G}'$ является важным вспомогательным средством в изучении бесконечных абелевых групп. См. Понтрягин Л. С. — Ann. of Math. 1934, 35, p. 361, и ван Кампен (van Kampen E. R.). — Ann. of Math., 1935, 36, p. 448.

§ 55. Простота знакопеременной группы

В § 51 мы видели, что симметрические группы $\mathfrak{S}_3$ и $\mathfrak{S}_4$ разрешимы. В противоположность этому, все последующие симметрические группы $\mathfrak{S}_n$ разрешимыми не являются. Правда, в них всегда есть нормальная подгруппа индекса 2 — знакопеременная группа $\mathfrak{A}_n$; однако композиционный ряд каждой из них переходит от $\mathfrak{A}_n$ сразу к $\mathfrak{E}$, в соответствии со следующей теоремой:

Теорема. *Знакопеременная группа $\mathfrak{A}_n$ $(n > 4)$ проста.*

Нам понадобится

Лемма. *Если нормальная подгруппа $\mathfrak{N}$ группы $\mathfrak{A}_n$ $(n > 2)$ содержит цикл из трех элементов, то $\mathfrak{N} = \mathfrak{A}_n$.*

Доказательство леммы. Пусть $\mathfrak{N}$ содержит цикл $(1\ 2\ 3)$. Тогда в $\mathfrak{N}$ должен содержаться и квадрат этого цикла $(2\ 1\ 3)$ и все трансформированные из этого цикла элементы:

$$\sigma \cdot (2\ 1\ 3) \cdot \sigma^{-1} \qquad (\sigma \in \mathfrak{A}_n).$$

Возьмем $\sigma = (1\ 2)(3\ k)$, где $k > 3$; тогда

$$\sigma \cdot (2\ 1\ 3) \cdot \sigma^{-1} = (1\ 2\ k).$$

Таким образом, подгруппа $\mathfrak{N}$ содержит все циклы вида $(1\ 2\ k)$. Но такие циклы порождают всю группу $\mathfrak{A}_n$ (§ 10, задача 4). Следовательно, $\mathfrak{N} = \mathfrak{A}_n$.

Доказательство теоремы. Пусть $\mathfrak{N}$ — произвольная отличная от $\mathfrak{E}$ нормальная подгруппа в $\mathfrak{A}_n$. Мы должны доказать, что $\mathfrak{N} = \mathfrak{A}_n$.

Выберем в $\mathfrak{N}$ подстановку τ, которая, будучи отличной от 1, оставляет неподвижными наибольшее возможное количество чисел из тех, на которые действуют подстановки из данной симметрической группы. Покажем, что τ переставляет в точности три числа, а остальные не сдвигает с места.

Сначала предположим, что τ переставляет в точности 4 элемента. Тогда τ является произведением двух транспозиций, потому что просто нет другого способа построить четную подстановку, которая переставляет в точности 4 элемента. Следовательно, пусть

$$\tau = (1\ 2)(3\ 4).$$

По условию $n > 4$, поэтому подстановку τ можно трансформировать с помощью подстановки $\sigma = (3\ 4\ 5)$ и получить

$$\tau_1 = \sigma\tau\sigma^{-1} = (1\ 2)(4\ 5).$$

Произведение $\tau\tau_1$ является тройным циклом $(3\ 4\ 5)$ и, следовательно, переставляет меньше чисел, чем τ, что противоречит выбору τ.

Предположим далее, что τ переставляет более 4 чисел. Вновь запишем τ в виде произведения циклов, причем начнем с наиболее длинного; например,

$$\tau = (1\ 2\ 3\ 4\ \ldots)\ldots,$$

или, если самый длинный цикл состоит из трех чисел,

$$\tau = (1\ 2\ 3)(4\ 5\ \ldots)\ldots,$$

или, если в подстановку входят лишь двойные циклы,

$$\tau = (1\ 2)(3\ 4)(5\ 6)\ldots$$

Трансформируем τ с помощью подстановки

$$\sigma = (2\ 3\ 4);$$

получим подстановку

$$\tau_1 = \sigma\tau\sigma^{-1},$$

которая в каждом из трех названных случаев имеет такой вид:

$$\tau_1 = (1\ 3\ 4\ 2\ \ldots)\ldots,$$
$$\tau_1 = (1\ 3\ 4)(2\ 5\ \ldots)\ldots,$$
$$\tau_1 = (1\ 3)(4\ 2)(5\ 6)\ldots$$

Во всех этих случаях $\tau_1 \neq \tau$, так что $\tau^{-1}\tau_1 \neq 1$. Подстановка $\tau^{-1}\tau_1$ в первом и третьем случаях оставляет неподвижными все числа $k > 4$, потому что для них $\tau_1 k = \tau k$. Во втором же случае

$$\tau = (1\ 2\ 3)(4\ 5\ \ldots)$$

и $\tau^{-1}\tau_1$ оставляет неподвижным все числа, кроме 1, 2, 3, 4 и 5;

таким образом, эта подстановка переставляет лишь пять чисел, в то время как τ переставляет более пяти чисел.

Таким образом, во всех случаях подстановка $\tau\,{}^1\tau_1$ переставляет меньше чисел, чем τ, что противоречит выбору τ. Следовательно, подстановка τ может переставлять лишь три числа. Но тогда τ является тройным циклом и, согласно лемме, $\mathfrak{N}=\mathfrak{A}_n$. Теорема полностью доказана.

Задача. Доказать, что для $n\neq 4$ знакопеременная группа $\mathfrak{A}_n$ является единственной нормальной подгруппой группы $\mathfrak{S}_n$, отличной от самой этой группы и от $\mathfrak{E}$.

§ 56. Транзитивность и примитивность

Группа подстановок некоторого множества $\mathfrak{M}$ называется *транзитивной над* $\mathfrak{M}$, если некоторый элемент a из $\mathfrak{M}$ с помощью подстановок из этой группы может быть переведен во все элементы x из $\mathfrak{M}$.

Если выполнено это условие, то для любых двух элементов x, y существует подстановка из группы, которая переводит x в y, потому что из

$$\rho a=x,\ \sigma a=y$$

следует, что

$$(\sigma\rho^{-1})\,x=y.$$

Следовательно, в вопросе о транзитивности безразлично, какой исходный элемент выбирается в качестве a.

Если группа $\mathfrak{G}$ не является транзитивной над $\mathfrak{M}$ (*интранзитивная группа*), то множество $\mathfrak{M}$ распадается на *области транзитивности*, т. е. на такие подмножества, которые группа переводит в себя и на которых она является транзитивной. В основе разбиения на такие подмножества лежит следующее отношение: два элемента a, b из $\mathfrak{M}$ тогда и только тогда включаются в одно подмножество, когда в $\mathfrak{G}$ существует элемент σ, переводящий a в b.

Это отношение, во-первых, рефлексивно, во-вторых, симметрично, в-третьих, транзитивно, потому что:

1) $\sigma a=a$ для $\sigma=1$;

2) из $\sigma a=b$ следует $\sigma^{-1}b=a$;

3) из $\sigma a=b$, $\tau b=c$ следует, что $(\tau\sigma)\,a=c$.

Следовательно, этим условием определяется разбиение множества $\mathfrak{M}$ на классы.

Если группа $\mathfrak{G}$ транзитивна над $\mathfrak{M}$ и $\mathfrak{G}_a$ — подгруппа, состоящая из элементов группы $\mathfrak{G}$, оставляющих неподвижным элемент a из $\mathfrak{M}$, то каждый левый смежный класс $\tau\mathfrak{G}_a$ по подгруппе $\mathfrak{G}_a$ переводит элемент a в однозначно определенный элемент τa. Таким образом, левым смежным классам взаимно однозначно соответствуют элементы множества $\mathfrak{M}$. Следовательно, число смежных классов (индекс группы $\mathfrak{G}_a$) равно числу элементов множества $\mathfrak{M}$.

Группа тех элементов из $\mathfrak{G}$, которые оставляют инвариантными элемент τa, задается равенством

$$\mathfrak{G}_{\tau a} = \tau \mathfrak{G}_a \tau^{-1}.$$

Транзитивная группа подстановок некоторого множества $\mathfrak{M}$ называется *импримитивной*, если $\mathfrak{M}$ разбивается по меньшей мере на два непересекающихся подмножества $\mathfrak{M}_1$, $\mathfrak{M}_2$, ..., из которых хотя бы в одном содержится более одного элемента, причем элементы группы переводят каждое $\mathfrak{M}_\mu$ в некоторое $\mathfrak{M}_\nu$. Множества $\mathfrak{M}_1$, $\mathfrak{M}_2$, ... называются *областями импримитивности*. Если же разбиение

$$\mathfrak{M} = \mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \ldots$$

только что указанного вида невозможно, то группа называется *примитивной*.

Примеры. Четверная группа Клейна импримитивна с областями импримитивности

$$\{1,\ 2\},\ \{3,\ 4\}.$$

(Впрочем, возможны еще два разбиения на области импримитивности.) Наоборот, полная группа подстановок (и, равным образом, знакопеременная группа) на n символах обязательно является примитивной, потому что для каждого разложения множества $\mathfrak{M}$ на подмножества, например,

$$\mathfrak{M} = \{1,\ 2,\ \ldots,\ k\} \cup \{\ldots\} \cup \ \ldots\ (1 < k < n),$$

существует подстановка, которая переводит $\{1,\ 2,\ \ldots,\ k\}$ в $\{1,\ 2,\ \ldots,\ k-1,\ k+1\}$, т. е. в множество, имеющее с $\{1,\ 2,\ \ldots, k\}$ общие элементы и не совпадающее с ним.

При любом разбиении $\mathfrak{M} = \{\mathfrak{M}_1,\ \ldots,\ \mathfrak{M}_r\}$ с описанным выше свойством, в котором, следовательно, группа $\mathfrak{G}$ переставляет множества $\mathfrak{M}_\nu$ между собой, для каждого ν существует подстановка, принадлежащая группе, которая переводит $\mathfrak{M}_1$ в $\mathfrak{M}_\nu$. Действительно, нужно лишь на основе транзитивности найти такую подстановку, которая произвольно взятый элемент из $\mathfrak{M}_1$ переводит в какой-нибудь элемент из $\mathfrak{M}_\nu$; тогда эта подстановка будет переводить $\mathfrak{M}_1$ в $\mathfrak{M}_\nu$. Отсюда, в частности, следует, что множества $\mathfrak{M}_1$, $\mathfrak{M}_2$, ... состоят из одного и того же числа элементов.

Для произвольной транзитивной группы подстановок $\mathfrak{G}$ некоторого множества $\mathfrak{M}$ выполняется следующая теорема:

Пусть $\mathfrak{g}$ — подгруппа, состоящая из тех элементов группы $\mathfrak{G}$, которые оставляют неподвижным некоторый элемент a множества $\mathfrak{M}$. Если группа $\mathfrak{G}$ импримитивна, то существует подгруппа $\mathfrak{h}$, отличная от $\mathfrak{G}$ и от $\mathfrak{g}$, для которой

$$\mathfrak{g} \subset \mathfrak{h} \subset \mathfrak{G},$$

и обратно, если существует подгруппа $\mathfrak{h}$, удовлетворяющая этим включениям, то $\mathfrak{G}$ импримитивна. Группа $\mathfrak{h}$ оставляет неподвижной одну из областей импримитивности $\mathfrak{M}_1$, а левые смежные классы по $\mathfrak{h}$ переводят $\mathfrak{M}_1$ в те или иные области $\mathfrak{M}_\nu$.

Доказательство. Пусть сначала группа $\mathfrak{G}$ импримитивна и $\mathfrak{M}=\{\mathfrak{M}_1, \mathfrak{M}_2, \ldots\}$ — ее разложение на области импримитивности. Пусть a — некоторый элемент области $\mathfrak{M}_1$. Пусть $\mathfrak{h}$ — подгруппа элементов группы $\mathfrak{G}$, оставляющих инвариантным множество $\mathfrak{M}_1$. Согласно сделанному выше замечанию группа $\mathfrak{h}$ содержит все подстановки из $\mathfrak{G}$, переводящие a в себя или в какой-нибудь другой элемент подмножества $\mathfrak{M}_1$; отсюда следует, что $\mathfrak{g}\subset\mathfrak{h}$ и $\mathfrak{h}\neq\mathfrak{g}$. Но в группе $\mathfrak{G}$ существует подстановка, которая переводит $\mathfrak{M}_1$, скажем, в $\mathfrak{M}_2$; поэтому $\mathfrak{h}\neq\mathfrak{G}$. Если τ переводит систему $\mathfrak{M}_1$ в $\mathfrak{M}_\nu$, то и весь смежный класс $\tau\mathfrak{h}$ переводит $\mathfrak{M}_1$ в $\mathfrak{M}_\nu$.

Обратно, пусть $\mathfrak{g}$—группа, отличная от $\mathfrak{G}$ и от $\mathfrak{h}$, и пусть

$$\mathfrak{g}\subset\mathfrak{h}\subset\mathfrak{G}.$$

Группа $\mathfrak{G}$ распадается на смежные классы $\tau\mathfrak{h}$ и каждый из этих смежных классов распадается на смежные классы $\sigma\mathfrak{g}$. Последние смежные классы переводят элемент a в некоторые элементы σa; следовательно, если их собрать в смежные классы $\tau\mathfrak{h}$, то элементы σa составят по меньшей мере два непересекающихся множества $\mathfrak{M}_1, \mathfrak{M}_2, \ldots$, каждое из которых состоит по меньшей мере из двух элементов. Множества $\mathfrak{M}_\nu$ определяются, таким образом, условием

$$\mathfrak{M}_\nu=\tau\mathfrak{h}a. \tag{1}$$

Каждая новая подстановка σ переводит $\mathfrak{M}_\nu=\tau\mathfrak{h}a$ в $\sigma\tau\mathfrak{h}a$, т. е. опять-таки в некоторое множество того же вида, чем и доказывается импримитивность группы $\mathfrak{G}$. Обозначим через $\mathfrak{M}_1$ множество, получающееся в соответствии с (1) при $\tau=1$; тогда $\mathfrak{h}$ (в силу $\mathfrak{h}\mathfrak{M}_1=\mathfrak{h}\mathfrak{h}a=\mathfrak{h}a=\mathfrak{M}_1$) оставляет область импримитивности $\mathfrak{M}_1$ неподвижной, а смежные классы $\tau\mathfrak{h}$ переводят $\mathfrak{M}_1$ в остальные области импримитивности $\mathfrak{M}_\nu$ (в силу $\tau\mathfrak{h}\mathfrak{M}_1=\tau\mathfrak{h}\mathfrak{h}a=\tau\mathfrak{h}a$).

Задача 1. Если число элементов множества $\mathfrak{M}$ простое, то каждая транзитивная группа на $\mathfrak{M}$ примитивна.

Задача 2. Определенная выше группа $\mathfrak{h}$ транзитивна на $\mathfrak{M}_1$.

Задача 3. Пусть множество $\mathfrak{M}$ разлагается на три области импримитивности, в каждой из которых по два элемента. Пусть порядок группы $\mathfrak{g}$ равен 12. Чему равен:

а) индекс группы $\mathfrak{h}$ в группе $\mathfrak{G}$;

б) индекс группы $\mathfrak{g}$ в группе $\mathfrak{h}$;

в) порядок группы $\mathfrak{g}$?

Задача 4. Порядок транзитивной группы подстановок конечного множества объектов делится на число этих объектов.

Замечание. Число переставляемых объектов называется *степенью* группы подстановок.