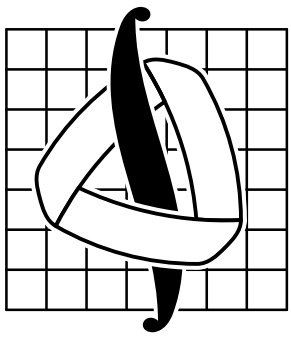
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
Механико-математический факультет



Курс лекций по высшей алгебре

Лектор — Виктор Николаевич Латышев

II курс, 3 семестр, поток математиков

Москва, 2004 г.

Оглавление

Введение

Предисловие

Автор данного документа будет признателен, если ему сообщат о замеченных в документе опечатках и неточностях. Документ не раз подвергался исправлениям, но мелкие ошибки всё ещё могут оставаться. В данной версии проведена ещё одна правка, в основном с целью улучшения читаемости.

Последняя компиляция: `8 февраля 2006 г.`
Обновления документа — на сайте `http://dmvn.mexmat.net`.
Об опечатках и неточностях пишите на `dmvn@mccme.ru`.

Список сокращений

1° Аббревиатуры: «КПАГ»=«конечно порождённая абелева группа», «САГ»=«свободная абелева группа», «КГИ»=«кольцо главных идеалов».

2° Квадратными скобками мы будем обозначать коммутаторы элементов группы и наименьшее общее кратное целых чисел. Например, $[a,b] = aba^{-1}b^{-1}$ и $[6,4,5] = 60$. К сожалению, обозначения одинаковые, но из контекста, как правило, всегда ясно, о чём идёт речь. Для полноты картины заметим, что через $[a,b]$ может обозначаться векторное произведение и коммутатор векторных полей, но в нашем тексте этих вещей не встретится.

3° Символом (a,b) мы будем обозначать наибольший общий делитель двух чисел или многочленов. Скалярное произведение, также часто обозначаемое круглыми скобками, в тексте не встретится.

4° Буквой $\mathfrak{P}$ мы будем обозначать множество простых чисел.

Литература

[1] М. Н. Вельтищев. *Конспекты лекций В. Н. Латышева по алгебре.* 2004.

[2] А. В. Домбровская. *Конспекты лекций Е. С. Голода по алгебре.* 2004.

[3] А. И. Кострикин. *Введение в алгебру. Часть III: Основные структуры.* М.: ФизМатЛит, 2001.

[4] Э. Б. Винберг. *Курс алгебры.* М.: Факториал – Пресс, 2002.

1. Теория групп

1.1. Группы

Определение. *Группой* называется непустое множество G с операцией $*\colon G\times G \longrightarrow G$, которая удовлетворяет аксиомам:

1° $(a*b)*c = a*(b*c)$ — ассоциативность операции.

2° $\exists e \in G\colon \forall a \in G$ имеем $e*a = a*e = a$ — существование нейтрального элемента.

3° $\forall a \in G \exists a^{-1}\colon a*a^{-1} = a^{-1}*a = e$ — существование обратного элемента.

Если $\forall a, b \in G$ имеет место свойство $a*b = b*a$, то группа называется *коммутативной* или *абелевой*. Знак операции, как и умножение, часто опускают, если используется мультипликативная терминология.

Нейтральный элемент группы называется *единицей*.

Легко видеть, что единица группы единственна: пусть e_1 и e_2 — две единицы группы. Тогда из свойств единицы следует, что $e_1 = e_1e_2 = e_2$, значит, $e_1 = e_2$. Обратный элемент также единствен: пусть $a^{-1}a = e$ и $b^{-1}a = e$. Тогда домножим второе равенство справа на a^{-1}, получим $b^{-1}aa^{-1} = a^{-1}$. Отсюда $b^{-1} = a^{-1}$.

Определение. *Подгруппой* H группы G называется подмножество $H \subset G$, которое относительно операции в G само является группой.

Достаточными условиями для подгруппы является её замкнутость относительно операции:

1° $a, b \in H \to ab \in H$.

2° $e \in H$.

3° $\forall a \in H$ имеем $a^{-1} \in H$.

Утверждение 1.1 (Эквивалентное определение подгруппы). *Непустое подмножество $H \subset G$ будет подгруппой в G тогда и только тогда, когда $a, b \in H \Rightarrow a^{-1}b \in H$.*

□ В одну сторону это очевидно, докажем в обратную сторону. Пусть $\forall a, b \in H$ имеем $a^{-1}b \in H$. Рассмотрим $a \in H$. Тогда $a^{-1}a = e \in H$. Тогда $\forall a \in H$ имеем $a^{-1}e = a^{-1} \in H$. Пусть теперь $a, b \in H$, тогда $a^{-1} \in H$, значит, $\left(a^{-1}\right)^{-1} b = ab \in H$, и мы видим, что все свойства подгруппы выполнены. ■

Пример 1.1.

1° $\mathcal{A}_n \subset \mathcal{S}_n$ — знакопеременная группа — подгруппа в группе подстановок.

2° $\mathbf{SO}_n \subset \mathbf{GL}_n(\mathbb{R})$ — подгруппа ортогональных матриц с определителем 1.

Определение. *Порядок* элемента $g \in G$ — число $O(g) := \min\{n\colon g^n = e\}$. По определению, элемент бесконечного порядка — элемент, не имеющий порядка.

В конечных группах все элементы имеют конечный порядок, ибо все степени одного элемента $e, g, g^2, g^3, \ldots$ не могут быть различными. Положим $n = O(g)$. Ясно, если $g^m = e$, то $n \,\big|\, m$. В самом деле, пусть $m = nq + r, r < n$. Тогда $g^m = (g^n)^q \cdot g^r = g^r = e$, что невозможно, поскольку $r < n$. Значит, $r = 0$.

1.2. Гомоморфизмы групп

Определение. *Гомоморфизм групп* $(G, *)$ и $(L, \circ)$ — отображение $\varphi\colon G \to L$, сохраняющее операцию: $\forall a, b \in$ $\in G$ имеем $\varphi(a*b) = \varphi(a) \circ \varphi(b)$.

Пусть e — единица G, а e' — единица в L. Покажем, что $\varphi(e) = e'$. В самом деле, $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$, значит, $\varphi(e)$ — нейтральный элемент в L. Покажем, что $\varphi(a^{-1}) = \varphi(a)^{-1}$. В самом деле, рассмотрим $e' = \varphi(e) =$ $= \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$, т. е. $\varphi(a^{-1})$ — обратный элемент по отношению к $\varphi(a)$.

Определение. Биективный гомоморфизм $\varphi\colon G \to L$ называется *изоморфизмом* групп. При этом говорят, что группы G и L *изоморфны*, и пишут $G \cong L$. Изоморфизм группы на себя называется *автоморфизмом*.

Определение. *Ядро* гомоморфизма φ — множество $\operatorname{Ker}\varphi := \{g \in G\colon \varphi(g) = e'\}$. *Образ* гомоморфизма — множество $\operatorname{Im}\varphi := \{x \in L\colon \exists\, g \in G\colon \varphi(g) = x\}$.

Утверждение 1.2. $\operatorname{Ker}\varphi$ *является подгруппой в* G, $\operatorname{Im}\varphi$ *является подгруппой в* L.

□ Пусть $g, h \in \operatorname{Ker}\varphi$. Тогда $\varphi(gh) = \varphi(g)\varphi(h) = e'e' = e' \Rightarrow gh \in \operatorname{Ker}\varphi$. Очевидно, $e \in \operatorname{Ker}\varphi$. Кроме того, если $g \in \operatorname{Ker}\varphi$, то $\varphi(g^{-1}) = \varphi(g)^{-1} = e'^{-1} = e' \Rightarrow g^{-1} \in \operatorname{Ker}\varphi$.

Пусть $x, y \in \operatorname{Im}\varphi$, тогда $\exists\, g, h \in G\colon x = \varphi(g), y = \varphi(h)$. Тогда $x^{-1}y = \varphi(g)^{-1}\varphi(h) = \varphi(g^{-1}h) \in \operatorname{Im}\varphi$. Используя эквивалентное определение подгруппы, получаем требуемое утверждение. ■

Определение. Инъективный гомоморфизм называется *вложением* группы G в группу L и обозначается $\varphi\colon G \hookrightarrow L$. В этом случае $G \cong \operatorname{Im}\varphi$.

Заметим, что гомоморфизм инъективен $\Leftrightarrow \operatorname{Ker}\varphi = \{e\}$. В самом деле, пусть $\operatorname{Ker}\varphi = \{e\}$. Тогда $\varphi(a) = \varphi(b) \Leftrightarrow$ $\Leftrightarrow \varphi(a^{-1}b) = e' \Leftrightarrow a^{-1}b = e \Leftrightarrow a = b$. Обратно, пусть гомоморфизм инъективен. Тогда $a \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(a) = e'$. Но $\varphi(e) = e'$, и в силу инъективности $a = e$. Значит, $\operatorname{Ker}\varphi$ содержит только e.

Пусть $\varphi\colon G \to L$ — гомоморфизм, и H — подгруппа в G. Покажем, что $K = \varphi(H)$ — подгруппа в L. Рассмотрим $x, y \in K$. Тогда $\exists\, a, b \in H\colon x = \varphi(a), y = \varphi(b)$. Тогда $xy = \varphi(a)\varphi(b) = \varphi(ab)$, значит, $xy \in K$. Поскольку $e \in H$, а $\varphi(e) = e'$, получаем, что $e' \in K$. Покажем, что $x^{-1} \in K$. Действительно, $x^{-1} = \varphi(a^{-1}) \in K$, поскольку $a^{-1} \in H$.

Определение. Сюръективный гомоморфизм называется *эпиморфизмом*.

Пусть $\varphi\colon G \to L$ — эпиморфизм, и K — подгруппа в L. Тогда $H = \varphi^{-1}(K)$ — подгруппа в G. В самом деле, пусть $x, y \in H$, тогда $\varphi(x), \varphi(y) \in K$. Рассмотрим $\varphi(x^{-1}y) = \varphi(x)^{-1}\varphi(y) \in K$. Следовательно, $x^{-1}y \in H$, значит, H — подгруппа.

Пример 2.1.

1° Пусть $n \in \mathbb{N}$. Рассмотрим $\varphi\colon (\mathbb{Z}, +) \to \mathbb{C}^*$, определённый по правилу $\varphi\colon k \mapsto \varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$. Тогда φ — гомоморфизм. Очевидно, $\operatorname{Ker}\varphi = n\mathbb{Z}$.

2° *Левый сдвиг.* Пусть G — группа. Фиксируем $g \in G$, и рассмотрим отображение $L_g\colon G \to G$, определённое по правилу $L_g\colon x \mapsto gx$. Покажем, что $L_g \in \mathcal{S}_G$, где $\mathcal{S}_G$ — группа подстановок множества G. Действительно, оно сюръективно: $L_g(g^{-1}x) = g(g^{-1}x) = x$. Кроме того, $L_g(x) = L_g(y) \Leftrightarrow gx = gy \Leftrightarrow x = y$. Значит, это инъекция. Теперь рассмотрим множество всех левых сдвигов $L_G := \{L_g\colon g \in G\}$. Это подгруппа в $\mathcal{S}_G$, поскольку произведение сдвигов на элементы g_1 и g_2 есть левый сдвиг на элемент g_1g_2, нейтральным элементом в L_G будет левый сдвиг на $e \in G$, обратным к сдвигу на g — сдвиг на g^{-1}. Таким образом, $L_G \subset \mathcal{S}_G$.

Теорема 1.3 (Кэли). *Пусть G — группа. Тогда $\exists$ инъективный гомоморфизм $G \hookrightarrow \mathcal{S}_G$.*

□ Рассмотрим $\varphi\colon G \to \mathcal{S}_G$ по правилу $\varphi\colon g \mapsto L_g$. Тогда φ — искомый гомоморфизм, ибо $\varphi(g_1g_2) = L_{g_1g_2} = L_{g_1}L_{g_2} = \varphi(g_1)\varphi(g_2)$, а его инъективность очевидна. ■

1.3. Системы порождающих

Очевидно, что если $A \subset G$ и $B \subset G$ — подгруппы, то $A \cap B$ тоже будет подгруппой G.

Определение. Фиксируем в группе G несколько элементов $A = \{a_1, \dots, a_m, \dots\}$. Подгруппой H, *порождённой* системой A, называется пересечение всех подгрупп G, содержащих A.

Изучим строение H. Ясно, что H содержит все элементы вида $a_{i_1}^{\varepsilon_1} \cdot \ldots \cdot a_{i_r}^{\varepsilon_r}$, где $\varepsilon_j = \pm 1$, а $r \in \mathbb{N}$, причём среди $i_1, \dots, i_r$ могут быть одинаковые числа. Такие произведения образуют подгруппу в G, и она является одной из подгрупп G, содержащих A. Значит, элементов, не представимых в таком виде, в H быть не может, откуда $H = \left\{a_{i_1}^{\varepsilon_1} \cdot \ldots \cdot a_{i_r}^{\varepsilon_r}\right\}$. Если $H = G$, то говорят, что A порождает G.

1.4. Циклические группы

Определение. Пусть $a \in G$ порождает группу G. Тогда G — *циклическая группа*, обозначаемая $G = \langle a \rangle$.

Теорема 1.4. *Всякая подгруппа циклической группы является циклической группой.*

□ В самом деле, пусть $G = \langle a \rangle$, и $H \subset G$. Если $H = \{e\}$, то доказывать нечего, ибо $H = \langle e \rangle$. Пусть $a^m \in H$, тогда $a^{-m} \in H$. Положим $k = \min\{m \in \mathbb{N}\colon a^m \in H\}$. Покажем, что $H = \langle a^k \rangle$. В самом деле, пусть $a^m \in H$, тогда, поделив с остатком, имеем $m = kq + r, r < k$. Тогда $a^m = \left(a^k\right)^q a^r$, следовательно, $a^r = a^m \left(a^k\right)^{-q} \in H$, поскольку каждый множитель принадлежит H. Но поскольку мы выбрали k минимальным, $r = 0$, и любой элемент из H есть некоторая степень элемента a^k. ■

Теорема 1.5. *Все бесконечные циклические группы изоморфны $(\mathbb{Z}, +)$. Все конечные циклические группы изоморфны U_n.*

□ Пусть $G = \langle a \rangle$. Возможны 2 случая.

1° $O(a) = \infty$. Тогда $G = \left\{\dots, a^{-2}, a^{-1}, e, a^1, a^2, \dots\right\}$. Все степени элемента a здесь различны, поэтому $|G| = \infty$. Рассмотрим $\varphi\colon G \to \mathbb{Z}$ по правилу $a^m \mapsto m$. Биективность отображения очевидна. Докажем сохранение операции: $\varphi(a^k a^l) = \varphi(a^{k+l}) = k + l = \varphi(a^k) + \varphi(a^l)$. Значит, φ — изоморфизм.

2° $O(a) = n$. Тогда $G = \left\{e, a^1, a^2, \dots, a^{n-1}\right\}$. В самом деле, рассмотрим $a^m = a^{nq+r} = e^q \cdot a^r = a^r$. Теперь можно построить изоморфизм $\varphi\colon G \to U_n$ по правилу $a^m \mapsto \varepsilon^m$, где $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Проверим корректность: $a^m = a^l \Rightarrow \varepsilon^m = \varepsilon^l$. Действительно, имеем $a^{m-l} = e$, значит, $n \,\big|\, (m-l)$, отсюда $\varepsilon^{m-l} = 1$, отсюда $\varepsilon^m = \varepsilon^l$. Сюръективность очевидна. Покажем инъективность. Рассмотрим $\varphi(a^m) = \varphi(a^l) \Leftrightarrow \varepsilon^m = \varepsilon^l \Leftrightarrow n \,\big|\, (m-l) \Leftrightarrow a^{m-l} = e \Leftrightarrow a^m = a^l$. Сохранение операции очевидно. Следовательно, φ — изоморфизм. ■

1.5. Разложение группы по подгруппе, теорема Лагранжа и её следствия

Определение. Пусть H — подгруппа в G. Фиксируем $a \in G$, тогда $aH = \{ah\colon h \in H\}$ — *левый смежный класс элемента a по подгруппе H*.

Аналогично определяется *правый смежный класс* Ha. Рассмотрим отображение $\varphi\colon H \to aH$ по правилу $\varphi\colon h \mapsto ah$. Сюръективность очевидна, а инъективность следует из того, что если $ah_1 = ah_2$, то, домножая слева на a^{-1}, получаем $h_1 = h_2$. Следовательно, $|H| = |aH|$.

Теорема 1.6 (Лагранжа). *Пусть j — количество левых смежных классов по H. Тогда $|G| = |H| \cdot j$.*

□ Различные смежные классы не пересекаются. В самом деле, рассмотрим aH и bH. Пусть $g \in aH \cap bH$, значит, $g = ah_1 = bh_2$, отсюда $a = bh_2h_1^{-1}$, значит, $a \in bH$, поскольку $h_2h_1^{-1} \in H$. Но тогда $aH \subset bH$, поскольку $\forall\, h \in H$ имеем $bh_2h_1^{-1}h \in bH$. Из соображений симметрии, $bH \subset aH$. Значит, $aH = bH$. Значит, смежные классы либо не пересекаются, либо совпадают. Значит, они образуют разбиение группы G на j частей. Поскольку все смежные классы равномощны H, получаем, что $|G| = |H| \cdot j$. ■

Замечание. Точно также можно доказать, что $|G| = |H| \cdot j$, где j — количество правых смежных классов по H. Отсюда следует, что число правых и число левых смежных классов совпадает. Оно называется индексом подгруппы H и обозначается $(G : H)$.

Следствие 1.1. $|H| \,\big|\, |G|$, $(G : H) \,\big|\, |G|$, $O(a) \,\big|\, |G|$, $\forall\, a \in G$.

□ Первые два утверждения следуют из теоремы Лагранжа, а третье следует из того, что можно рассмотреть циклическую группу $\langle a \rangle$, для которой имеем $|\langle a \rangle| = O(a)$. ■

Следствие 1.2. *Если $|G| = p$, где $p \in \mathfrak{P}$, то G — циклическая группа.*

□ $\exists\, a \in G\colon O(a) = p$, поскольку порядки всех элементов не могут быть равны единице. Тогда $\langle a \rangle = G$. ■

1.6. Разложение по подгруппе. Конгруэнции. Нормальные подгруппы. Факторгруппы

Пусть H — подгруппа в G. Рассмотрим отношение $a \sim b \Leftrightarrow a^{-1}b \in H, a, b \in G$. Покажем, что $\sim$ задаёт отношение эквивалентности на G. Действительно, $a \sim a$, ибо $a^{-1}a = e \in H$. Симметричность: $b \sim a \Leftrightarrow b^{-1}a \in$ $\in H \Leftrightarrow \big(b^{-1}a\big)^{-1} \in H \Leftrightarrow a^{-1}b \in H \Leftrightarrow a \sim b$. Транзитивность: $a \sim b, b \sim c \Leftrightarrow a^{-1}b \in H, b^{-1}c \in H \Rightarrow (a^{-1}b)(b^{-1}c) \in$ $\in H \Rightarrow a^{-1}c \in H \Rightarrow a \sim c$.

Заметим, что $aH = bH \Leftrightarrow a^{-1}b \in H$. В самом деле, $b = ah \Leftrightarrow a^{-1}b = h \in H$. Следовательно, классы эквивалентности, задаваемые $\sim$, есть в точности смежные классы: $[a] = aH$.

Определение. *Конгруэнция на множестве с операцией.* Рассмотрим $(G, *)$, и пусть $\sim$ задаёт некоторое отношение эквивалентности на G. Тогда назовём $\sim$ конгруэнцией, если она согласована с операцией в G: $a \sim$ $\sim a', b \sim b' \Rightarrow a*b \sim a'*b'$. Это означает, что можно выбрать других представителей из классов эквивалентности, и это не повлияет на результат умножения.

Определение. Если $\sim$ — конгруэнция, то имеет смысл рассмотреть *факторомножество* $\big({}^{G}\!/_{\sim}, *\big)$ классов эквивалентности с операцией $*$. Поскольку $\sim$ — конгруэнция, имеем $[a] * [b] = [a * b]$, и тогда $*$ называется *естественной операцией*. Если G — группа, то для факторомножества выполняются все аксиомы группы: ассоциативность: $\big([a] * [b]\big) * [c] = [a * b] * [c] = [a * b * c] = [a] * [b * c] = [a] * \big([b] * [c]\big)$, существование нейтрального элемента: $[a]*[e] = [e]*[a] = [a]$ и существование обратного элемента: $[a]*[a^{-1}] = [e]$, следовательно, $[a^{-1}] = [a]^{-1}$. Итак, ${}^{G}\!/_{\sim}$ — *факторгруппа*.

Заметим, что разбиение на смежные классы по подгруппе не обязательно задаёт конгруэнцию. Определим класс подгрупп, факторизация по которым её задаёт.

Определение. *Нормальная подгруппа* (инвариантная подгруппа, нормальный делитель) — подгруппа H группы G, такая, что $\forall\, a \in G$ имеем $aH = Ha$. Обозначение: $H \lhd G$.

Заметим, что в абелевой группе любая подгруппа нормальна. Нормальные подгруппы существуют в любой группе: $G \lhd G, \{e\} \lhd G$.

Определение. Группа называется *простой*, если в ней нет нормальных подгрупп, кроме тривиальных.

Определение. Элементы $x, y \in G$ называются *сопряжёнными*, если $\exists\, g \in G\colon y = gxg^{-1}$. Говорят, что x сопряжён с y через g.

Покажем, что сопряжение задаёт отношение эквивалентности: $x \sim y \Leftrightarrow y = gxg^{-1}$ для некоторого $g \in G$. В самом деле, имеет место рефлексивность: $x \sim x$, ибо $x = exe^{-1}$. Докажем симметричность: $x \sim y \Rightarrow y \sim x$. Действительно, если $y = gxg^{-1}$, то $x = g^{-1}yg = \big(g^{-1}\big)\, y\, \big(g^{-1}\big)^{-1}$. Транзитивность: пусть $x \sim y, y \sim z$. Тогда $y = g_1xg_1^{-1}, z = g_2yg_2^{-1}$. Отсюда $z = (g_2g_1)x(g_2g_1)^{-1}$, значит, $x \sim z$. Таким образом, группу G можно разбить на *классы сопряжённых элементов*: $G = \bigcup K_x$, $K_x := \{y \in G\colon y \sim x\}$.

Рассмотрим *группу автоморфизмов* $\operatorname{Aut} G \subset \mathcal{S}_G$ *группы* G. Фиксируем $g \in G$. Рассмотрим отображение $I_g\colon G \to G$ по правилу $I_g\colon x \mapsto gxg^{-1}$. Покажем, что $I_g \in \operatorname{Aut} G$. В самом деле, I_g сюръективно: на x отображается элемент $g^{-1}xg$: $I_g(g^{-1}xg) = gg^{-1}xgg^{-1} = x$. Инъективность очевидна: $gxg^{-1} = gyg^{-1} \Leftrightarrow x = y$. Значит, это как минимум биекция. Покажем сохранение операции: $I_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = I_g(x)I_g(y)$. Значит, это автоморфизм.

Определение. Автоморфизмы вида I_g образуют *подгруппу внутренних автоморфизмов* $\operatorname{Int} G \subset \operatorname{Aut} G$. Покажем, что это действительно подгруппа. Имеем $\mathrm{id} = I_e \in \operatorname{Int} G$, кроме того, $(I_{g_1} \circ I_{g_2})(x) = g_1 g_2 x g_2^{-1} g_1^{-1} = (g_1 g_2) x (g_1 g_2)^{-1} = I_{g_1 g_2}(x)$. Отсюда видно, что обратным к I_g является автоморфизм $I_{g^{-1}} \in \operatorname{Int} G$. Итак, $\operatorname{Int} G$ — подгруппа.

Заметим, что $H \lhd G \Leftrightarrow gHg^{-1} = H$. Получаем эквивалентное определение: $H \lhd G$ тогда и только тогда, когда она инвариантна относительно $\operatorname{Int} G$. Следовательно, H состоит из нескольких классов сопряжённых элементов, ибо вместе с любым элементом класса сопряжённости она содержит и любой элемент этого же класса.

Теорема 1.7. *Все конгруэнции на G являются эквивалентностями, связанными с разложениями по нормальным подгруппам.*

□ **1°** Пусть $H \lhd G$, и по определению $a \sim b \Leftrightarrow a^{-1}b \in H$. Покажем, что это конгруэнция. Пусть $a \sim a', b \sim b'$. Покажем, что $ab \sim a'b'$. Имеем $a^{-1}a' \in H, b^{-1}b' \in H$. Тогда $(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = \big(b^{-1}(a^{-1}a')b\big)b^{-1}b'$. Но $a^{-1}a' \in H$ по условию, тогда в силу нормальности H имеем $b^{-1}(a^{-1}a')b \in H$. Но и $b^{-1}b' \in H$ по условию, значит, произведение этих множителей также лежит в H. Но это и означает, что $ab \sim a'b'$. Тогда ${}^{G}\!/_{\sim} = \{aH, a \in G\}$ с единицей $eH = H$, $(aH)^{-1} = a^{-1}H$, $(aH)(bH) = (ab)H$.

2° Обратно, пусть $\sim$ задаёт конгруэнцию. Покажем, что $\exists\, H \lhd G$, для которой $a \sim b \Leftrightarrow a^{-1}b \in H$. Рассмотрим $H := \{a \in G\colon a \sim e\}$. Покажем, что H — искомая нормальная подгруппа в G. Поскольку $e \sim e$, имеем $e \in H$. Пусть $a, b \in H, a \sim e, b \sim e$. По свойству конгруэнции, $ab \sim ee = e$, т. е. $ab \in H$. Далее, поскольку $a \sim e, a^{-1} \sim a^{-1}$, получаем $aa^{-1} \sim ea^{-1}$, откуда $e \sim a^{-1} \Leftrightarrow a^{-1} \in H$. Значит, H — подгруппа в G. Покажем нормальность: пусть $h \in H \Leftrightarrow h \sim e$, кроме того, $g \sim g, g^{-1} \sim g^{-1}$. Отсюда $ghg^{-1} \sim geg^{-1} = e \Rightarrow ghg^{-1} \in H$. ■

Замечание. Когда речь идёт о конгруэнции, всегда можно иметь ввиду соответствующую нормальную подгруппу. Поэтому говорят обычно не о фактормножестве по конгруэнции, а о *факторгруппе* ${}^{G}\!/_{H}$, где $H \lhd G$.

Замечание. Заметим, что отношение нормальности не является *транзитивным*, т. е. если $A \lhd B$, $B \lhd C$, то A не обязательно нормальна в C. Пример: $C = \mathcal{A}_4$, $B = \mathcal{V}_4$, $A = \{\mathrm{id}, (12)(34)\}$.

Теорема 1.8. *Пусть $H \subset G$ — подгруппа индекса 2. Тогда $H \lhd G$.*

□ Рассмотрим левые смежные классы по H. Их будет два: eH и $g_l H$, где $g_l \notin H$. Теперь рассмотрим правые смежные классы: He и Hg_r, где $g_r \notin H$. Ясно, что $eH = H = He$, но тогда $g_l H = Hg_r$, поскольку смежные классы образуют разбиение G. Но если левые и правые смежные классы совпадают, то $H \lhd G$. ■

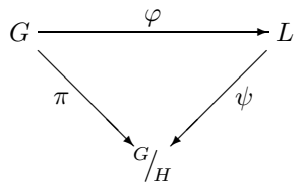
1.7. Теорема о гомоморфизме

Теорема 1.9. *Ядра гомоморфизмов, и только они, являются нормальными подгруппами.*

□ **1°** Пусть $\varphi\colon G \to L$ — гомоморфизм. Покажем, что $H = \operatorname{Ker}\varphi \lhd G$. Пусть $h \in H, g \in G$. Рассмотрим $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)e'\varphi(g)^{-1} = e'$. Значит, $ghg^{-1} \in H$, но это и означает, что $H \lhd G$.

2° Пусть $H \lhd G$. Рассмотрим естественный эпиморфизм $\pi\colon G \to {}^{G}\!/_{H}$ по правилу $\pi\colon a \mapsto aH$. Тогда $a \in \operatorname{Ker}\pi \Leftrightarrow \pi(a) = aH = H \Leftrightarrow a \in H \Rightarrow \operatorname{Ker}\pi = H$. ■

Теорема 1.10 (О гомоморфизмах групп). *Пусть $\varphi\colon G \to L$ — эпиморфизм, $H := \operatorname{Ker}\varphi$, $\pi\colon G \to {}^{G}\!/_{H}$ — естественный эпиморфизм. Тогда существует изоморфизм $\psi\colon L \to {}^{G}\!/_{H}$, для которого диаграмма* (1) *коммутативна, то есть $\pi = \psi \circ \varphi$.*



(1)

Иными словами, ${}^{G}\!/_{\operatorname{Ker}\varphi} \cong \operatorname{Im}\varphi = L$.

□ Пусть $x \in L$. Тогда $\exists\, a \in G\colon x = \varphi(a)$ в силу того, что $\operatorname{Im}\varphi = L$. Рассмотрим $\psi\colon L \to {}^{G}\!/_{H}$ по правилу $\psi\colon x \mapsto aH$, где $\varphi(a) = x$. Покажем, что ψ — искомый изоморфизм. В самом деле, проверим корректность. Пусть $x = \varphi(a) = \varphi(b), a, b \in G$. Тогда $\varphi(a) = \varphi(b) \Leftrightarrow \varphi(a^{-1}b) = e_L$, где e_L — единица в L. Отсюда $a^{-1}b \in \operatorname{Ker}\varphi = H$, значит, $aH = bH$. Значит, ψ переведёт $\varphi(a)$ и $\varphi(b)$ в один и тот же смежный класс. Тем самым корректность доказана.

Покажем, что ψ — биекция. Сюръективность сразу следует из определения ψ: достаточно взять такой x, что $x = \varphi(a)$. Проверим инъективность: $\psi\big(\varphi(a)\big) = \psi\big(\varphi(b)\big) \Leftrightarrow aH = bH \Leftrightarrow a^{-1}b \in H \Leftrightarrow \varphi(a^{-1}b) = e_L \Leftrightarrow \varphi(a) = \varphi(b)$.

Покажем, что ψ сохраняет операцию: $\psi\big(\varphi(a)\varphi(b)\big) = \psi\big(\varphi(ab)\big) = (ab)H = aH \cdot bH = \psi\big(\varphi(a)\big) \cdot \psi\big(\varphi(b)\big)$. Здесь свойство $(ab)H = aH \cdot bH$ следует из того, что $H = \operatorname{Ker}\varphi$, и, следовательно, задаёт конгруэнцию.

Проверим коммутативность. Пусть $a \in G$. Тогда $\pi(a) = aH$. Но $(\psi \circ \varphi)(a) = aH$ по определению ψ. ■

1.8. Теорема о соответствии групп при эпиморфизме

Говоря о гомоморфизмах, мы уже показали, что прообраз подгруппы при эпиморфизме есть подгруппа.

Теорема 1.11 (О соответствии). *Пусть $\varphi\colon G \to L$ — эпиморфизм групп. Положим $H := \operatorname{Ker}\varphi \lhd G$. Назовём $A \subset G$ выделенной подгруппой, если $H \subset A$. Тогда сопоставление θ выделенной подгруппе $A \subset G$ её образа $\varphi(A)$ определяет биекцию между выделенными подгруппами в G и всеми подгруппами L. При этом соответствующие подгруппы одновременно нормальны и факторгруппы по ним изоморфны.*

□ **1°** Покажем, что θ биективно. Сюръективность очевидна, ибо для любой подгруппы $U \subset L$ имеем $e_L \in U$, следовательно, $H \subset \varphi^{-1}(U) = A$, откуда заключаем, что A — выделенная подгруппа. Докажем инъективность. Пусть $A, B \subset G$ — выделенные подгруппы, и $\varphi(A) = \varphi(B)$. Покажем, что $A = B$. Рассмотрим произвольное $a \in A$. Тогда в силу совпадения образов, $\exists\, b \in B\colon \varphi(a) = \varphi(b)$. Отсюда $\varphi(b^{-1}a) = e_L \Leftrightarrow b^{-1}a \in \operatorname{Ker}\varphi = H$, значит, $a = bh$, но поскольку $H \subset B$, получаем $bh \in B$, т. е. $a \in B$. Следовательно, $A \subset B$. По симметричным соображениям $B \subset A$. Значит, $A = B$.

2° Пусть A — выделенная подгруппа в G. Покажем, что $A \lhd G \Leftrightarrow \varphi(A) \lhd L$. В самом деле, пусть $A \lhd G$. Тогда $\forall\, g \in G$ имеем $gAg^{-1} \in A$. Применим φ к этому тождеству, получим $\varphi(g)\varphi(A)\varphi(g)^{-1} = \varphi(A)$. Но поскольку φ — эпиморфизм, то когда g пробегает G, $\varphi(g)$ пробегает всю L. Отсюда следует нормальность $\varphi(A)$ в L. Обратно, пусть $M \lhd L$, предположим, что $A := \varphi^{-1}(M)$ не является нормальной в G. Значит, $\exists\, g \in G$, $x \in A\colon gxg^{-1} \notin A$. Тогда $\varphi(gxg^{-1}) \notin M$, следовательно, $\varphi(g)\varphi(x)\varphi(g)^{-1} \notin M$. Но это уже противоречит тому, что $M \lhd L$, поскольку $\varphi(x) \in M$. Тем самым одновременная нормальность доказана.

3° Докажем изоморфность факторгрупп, соответствующих нормальным подгруппам. Пусть $A \lhd G$ — выделенная подгруппа, и $U := \varphi(A)$. Рассмотрим отображение $\psi\colon G \to {}^{L}\!/_{U}$, определённое по правилу $g \mapsto \varphi(g)U$. Докажем, что это эпиморфизм. Сюръективность очевидна: когда g бегает по G, $\varphi(g)$ бегает по всей L, значит, любой смежный класс накроется. Проверим сохранение операции: $\psi(g_1g_2) = \varphi(g_1g_2)U = \big(\varphi(g_1)\varphi(g_2)\big)U = \varphi(g_1)U \cdot \varphi(g_2)U = \psi(g_1)\cdot\psi(g_2)$ по свойствам естественной операции. Теперь найдём ядро: $g \in \operatorname{Ker}\psi \Leftrightarrow \psi(g) = \varphi(g)U = U \Leftrightarrow \varphi(g) \in U \Leftrightarrow g \in A$. Отсюда следует, что $A = \operatorname{Ker}\psi$. По теореме о гомоморфизме получаем ${}^{G}\!/_{A} \cong {}^{L}\!/_{U}$. ■

Теорема 1.12. *Пусть $L \lhd K \lhd G$ и $L \lhd G$. Тогда ${}^{G/L}\!/_{K/L} \cong {}^{G}\!/_{K}$.*

□ Рассмотрим естественный эпиморфизм $\varphi\colon G \to {}^{G}\!/_{L}$. Имеем $\operatorname{Ker}\varphi = L$. Тогда $\varphi(K) = {}^{K}\!/_{L}$. Применим теорему о соответствии к φ, тогда получим $K \overset{\theta}{\longleftrightarrow} {}^{K}\!/_{L}$. Отсюда ${}^{K}\!/_{L} \lhd {}^{G}\!/_{L}$. По теореме о соответствии, факторгруппы по соответствующим нормальным подгруппам изоморфны, поэтому ${}^{G}\!/_{K} \cong {}^{G/L}\!/_{K/L}$. ■

2. Поля и кольца

2.1. Кольца. Гомоморфизмы колец. Факторкольца

Определение. *Кольцом* называется непустое множество R с двумя операциями, сложением и умножением: $(R, +, \cdot)$. При этом по сложению кольцо — абелева группа, по умножению выполнена левая и правая дистрибутивность: $a(b+c) = ab + ac, (a+b)c = ac + bc$. *Ассоциативное* кольцо — кольцо с ассоциативным умножением, *коммутативное* кольцо — кольцо с коммутативным умножением, *кольцо с единицей* — кольцо, в котором есть нейтральный по умножению элемент.

Определение. *Гомоморфизм* колец R и Q — отображение $\varphi\colon R \to Q$, сохраняющее обе операции. Поскольку это, в частности, гомоморфизмы их аддитивных групп, имеем $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$. Гомоморфизм не обязан сохранять единицу кольца, даже если она есть.

Определение. *Конгруэнция* кольца — отношение эквивалентности $\sim$, согласованное с операциями: $a \sim b, a' \sim b' \Rightarrow a + a' \sim b + b', aa' \sim bb'$.

Естественные операции в кольцах обладают свойствами:
1° $[a] + [b] = [a+b]$,
2° $[a][b] = [ab]$,
3° $[c]\big([a] + [b]\big) = [c][a+b] = [c(a+b)] = [ca+cb] = [ca] + [cb] = [c][a] + [c][b]$,
4° $\big([a] + [b]\big)[c] = [a][c] + [b][c]$ (доказывается аналогично).

Определение. *Идеалом* кольца R называется подгруппа $(I, +) \subset (R, +)$, выдерживающая левое и правое умножение на элементы кольца: $\forall\, a \in R$ имеем $aI \subset I, Ia \subset I$. Если I выдерживает только левое умножение, он называется *левым* идеалом. Аналогично определяется *правый* идеал.

В кольцах идеалы играют роль нормальных подгрупп, и обозначение такое же: $I \lhd R$. Поскольку кольцо по сложению является абелевой группой, можно определить эквивалентность $a \sim b \Leftrightarrow a - b \in I$. Тогда это будет конгруэнция относительно сложения. Покажем, что это будет конгруэнцией и по умножению. Пусть $a \sim a', b \sim b'$.

Рассмотрим $ab - a'b' = (ab - ab') + (ab' - a'b') = a(b - b') + (a - a')b' \in I$, поскольку $a - a' \in I, b - b' \in I$. Но $ab - a'b' \in I \Leftrightarrow ab \sim a'b'$.

Определение. Определим теперь *факторкольцо* по идеалу I: это факторгруппа ${}^{A}\!/_{I}$ с операцией умножения $(a + I)(b + I) = ab + I$.

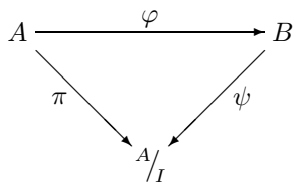
Определение. *Ядром* гомоморфизма колец $\varphi\colon R \to Q$ называется множество $\operatorname{Ker}\varphi = \{x \in R\colon \varphi(x) = 0\}$.

Теорема 2.1. *Ядра гомоморфизмов, и только они, являются идеалами кольца.*

□ **1°** Пусть $\varphi\colon R \to Q$ — гомоморфизм колец, обозначим $I := \operatorname{Ker}\varphi$. Пусть $x \in I, a \in R$. Проверим, что I выдерживает умножение: $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \cdot 0 = 0$, значит, $ax \in I$. Аналогично, $xa \in I$. Кроме того, из теоремы о ядре гомоморфизма групп следует, что $(I, +) \subset (R, +)$. Значит, $I \lhd R$.

2° Обратно, пусть $I \lhd R$. Рассмотрим естественный эпиморфизм $\pi\colon R \to {}^{R}\!/_{I}$, тогда $\operatorname{Ker}\pi = I$. ■

Теорема 2.2 (О гомоморфизмах колец). *Пусть $\varphi\colon A \to B$ — эпиморфизм, $I := \operatorname{Ker}\varphi$, $\pi\colon A \to {}^{A}\!/_{I}$ — естественный эпиморфизм. Тогда существует изоморфизм $\psi\colon B \to {}^{A}\!/_{I}$, для которого диаграмма* (1) *коммутативна, то есть $\pi = \psi \circ \varphi$.*



(1)

□ Поскольку все участвующие в теореме кольца являются абелевыми группами, для аддитивных групп существование ψ доказано. Покажем, что ψ будет изоморфизмом колец. Нам надо проверить только сохранение умножения. Рассмотрим $x, y \in A$, тогда $\varphi(x), \varphi(y) \in B$. Рассмотрим $\psi\big(\varphi(x)\varphi(y)\big) = \psi\big(\varphi(xy)\big) = (xy) + I = (x + I)(y + I) = \psi\big(\varphi(x)\big)\psi\big(\varphi(y)\big)$, что и требуется. ■

Заметим, что тривиальные идеалы в кольцах есть всегда. Таково всё кольцо и нулевое подкольцо. Покажем, что в полях все идеалы тривиальны. Действительно, если $x \in I$, где $x \neq 0$, то $1 \in I$, поскольку $x^{-1}x \in I$. А если в идеале есть единица, то там содержится и всё поле, поскольку идеал выдерживает умножение на любой элемент поля.

Определение. Рассмотрим коммутативное кольцо A. Зафиксируем систему элементов $\{x_1, \ldots, x_r\}, x_i \in A$. Рассмотрим множество $I := \{a_1x_1 + \ldots + a_rx_r \mid a_i \in A\}$. Очевидно, что $I \lhd A$, поскольку оно замкнуто относительно сложения и операции умножения на элементы кольца. Такой идеал называется *порождённым* элементами $x_1, \ldots, x_r$ и обозначается $(x_1, \ldots, x_r) \lhd A$. Идеал, порождённый одним элементом, называется *главным*. Кольцо, в котором каждый идеал главный, называется *кольцом главных идеалов*.

Теорема 2.3. *Пусть K — поле. Тогда $K[x]$ — КГИ.*

□ Рассмотрим ненулевой идеал $I \lhd K[x]$. Выберем в I ненулевой многочлен минимальной степени и обозначим его через d. Покажем, что $I = (d)$. В самом деле, пусть $f \in I$. Допустим, что $d \nmid f$. Поделим f на d с остатком: $f = dq + r$. Тогда $r = f - dq$, откуда $r \in I$. Действительно, $f \in I$, $dq \in I$, значит, их разность тоже лежит в идеале. Но $\deg r < \deg d$, а это противоречит тому, что мы брали d минимальной степени. Значит, $d \mid f$, откуда $I = (d)$. ■

Из этой теоремы следует, что идеал в $K[x]$ содержит единственный ненулевой многочлен минимальной степени со старшим коэффициентом 1. Кроме того, если $K[x]$ заменить на $\mathbb{Z}$, а «степень» — на «модуль», то мы получим доказательство теоремы о том, что $\mathbb{Z}$ — кольцо главных идеалов.

Задача 2.1. *Докажите, что $K[x_1, \ldots, x_n], n \geqslant 2$ и $\mathbb{Z}[x]$ не являются КГИ.*

Теорема 2.4 (Об инъективности). *Пусть $\varphi\colon F \to L$ — гомоморфизм полей. Тогда либо $\varphi \equiv 0$, либо φ инъективен.*

□ Поскольку $\operatorname{Ker}\varphi \lhd F$, а в полях нетривиальных идеалов нет, получаем, что либо $\operatorname{Ker}\varphi = 0$, и тогда φ инъективен; либо $\operatorname{Ker}\varphi = F$, и $\varphi \equiv 0$.

2.2. Факторкольца многочленов. Алгебраические расширения. Поля разложения многочленов

Рассмотрим факторкольцо $A = {}^{K[x]}\!/_{(d)}$, где $d = a_nx^n + \ldots + a_0, n > 0$. Рассмотрим эпиморфизм $\varphi\colon K[x] \to A$, определённый по правилу $\varphi\colon f \mapsto f + I$. Кроме того, поскольку $K \hookrightarrow K[x]$, можно рассмотреть и ограничение этого эпиморфизма $\varphi\Big|_{K}\colon K \to A$. Введём обозначение для смежных классов по идеалу: $\overline{f} = f + I$. Для элементов поля K имеем $\varphi(\alpha+\beta) = (\alpha+\beta)+I = \varphi(\alpha)+\varphi(\beta)$ и $\varphi(\alpha\beta) = (\alpha\beta)+I = \varphi(\alpha)\varphi(\beta)$. Тогда $\overline{K} = \{\overline{\alpha} = \alpha + I\colon \alpha \in K\} \cong$ $\cong K$. Значит, по теореме об инъективности, $K \hookrightarrow A$, и тогда A будет линейным пространством над полем K.

Заметим, что каждый смежный класс порождается многочленом степени меньше n: поделив на d с остатком, получаем $\overline{f} = f + I = r + (qd + I) = r + I$. Отсюда $\dim_K A = n$. Базисом будут степени $\overline{x}$ до $n-1$ включительно: $\overline{1}, \ldots, \overline{x}^{n-1}$. Через них всё выражается, докажем линейную независимость: если бы $\overline{\alpha_{n-1}x^{n-1} + \ldots + \alpha_0} = \overline{0} = 0 + I \in I$, то это противоречило бы тому, что в I нет многочленов степени ниже n, кроме нулевого. Заметим, что здесь мы воспользовались свойствами естественных операций. Отсюда следует, что $\alpha_i = 0$.

Теорема 2.5. *Факторкольцо $A = {}^{K[x]}\!/_{(d)}$ является полем тогда и только тогда, когда d неприводим.*

□ В самом деле, если $d = d_1 d_2$, и $\deg d_1, \deg d_2 < n$, то $\overline{d}_1, \overline{d}_2 \neq \overline{0}$. Но $\overline{d}_1\overline{d}_2 = \overline{d} = \overline{0}$. Значит, тут есть делители нуля, и A не может быть полем. Пусть d неприводим, тогда пусть $\overline{f} \neq \overline{0}$, значит, $d \nmid f$. Поскольку d неприводим, получаем, что $(d, f) = 1$, а отсюда по формуле «$fu + gv$» имеем $\overline{f}\overline{u} + \overline{d}\overline{v} = \overline{1}$. Но $\overline{d} = \overline{0}$, отсюда $\overline{f}\overline{u} = \overline{1}$, и мы нашли обратный элемент к ненулевому многочлену $\overline{f}$. Значит, это поле. ■

Определение. Пусть K — подполе F, тогда F называют *расширением* поля K. Пусть p — неприводимый над K многочлен. Тогда ${}^{K[x]}\!/_{(p)}$ называют *простым алгебраическим расширением поля K*. Также можно рассмотреть *простое трансцендентное расширение* $K \hookrightarrow K(x)$ с помощью *поля рациональных функций* над K, но мы не будем этого делать.

Неприводимый над K многочлен p имеет корни в ${}^{K[x]}\!/_{(p)}$. Действительно, $p(\overline{x}) = \alpha_n\overline{x}^n + \ldots + \alpha_0 = \overline{p(x)} = \overline{0}$.

Теорема 2.6 (О вложении). *Пусть F — расширение поля K, содержащее корень θ неприводимого над K многочлена $p \in K[x]$. Тогда существует вложение ${}^{K[x]}\!/_{(p)} \hookrightarrow F$.*

□ Рассмотрим отображение $\varphi\colon K[x] \to F$ по правилу $\varphi\colon f(x) \mapsto f(\theta)$. Это, очевидно, гомоморфизм. Ясно, что $\operatorname{Ker}\varphi$ есть множество всех многочленов из $K[x]$, имеющих корень θ, в частности, $p \in \operatorname{Ker}\varphi$. Заметим, что $\operatorname{Ker}\varphi$ — главный идеал, порождённый некоторым многочленом d. Значит, $p = d \cdot g$, но p — неприводим, значит, $p \sim d$. Тогда можно считать, что $\operatorname{Ker}\varphi = (p)$, и применив теорему о гомоморфизме колец, получаем требуемое. Заметим, что мы таким образом построили минимальное подполе, содержащее корень неприводимого многочлена p. Это вытекает из соображений размерности: не существует собственного подполя, содержащего корень θ с размерностью, равной размерности данного поля. ■

Замечание. Расширение поля K, полученное присоединением корня θ неприводимого над K многочлена, обозначается $K(\theta)$.

Пример 2.1. Построим поле $\mathbb{C}$. Возьмём многочлен p второй степени с отрицательным дискриминантом, и в качестве θ рассмотрим какой-нибудь его корень. Мы знаем, что $\dim_{\mathbb{R}}\mathbb{C} = 2$. Имеем $\varphi(1) = 1, \varphi(x) = \theta$. Поскольку 1 и θ линейно независимы, $\mathbb{C} = \langle 1, \theta\rangle$. Тогда ${}^{\mathbb{R}[x]}\!/_{(p)} \cong \mathbb{C}$.

Пусть $K \subset F, K \subset L$. Пусть $\varphi\colon F \to L$ — изоморфизм полей. φ называется *изоморфизмом над K*, если $\forall\, \alpha \in K$ имеем $\varphi(\alpha) = \alpha$, т. е. поле K при таком изоморфизме неподвижно.

Пусть $f \in K[x]$. Многочлен f может не разлагаться на линейные множители над K, если $n = \deg f > 1$. Наша цель — построить поле, в котором он разложится на линейные множители. Рассмотрим L_1 — простое алгебраическое расширение K, содержащее корень θ_1 многочлена f. L_1 строится очевидным образом: надо профакторизовать $K[x]$ по любому неприводимому множителю f, тогда это будет поле, содержащее корень данного неприводимого множителя. Итак, $f = (x-\theta_1)g \in L_1[x]$, причём $\deg g = n-1$. Значит, можно рассмотреть простое алгебраическое расширение L_2 для g, там будет ещё один корень θ_2, и так далее. Поскольку степень многочлена уменьшается на 1 при каждом расширении, не более, чем за n расширений мы придём к полю L_r, над которым f разлагается на линейные множители.

Определение. Теперь рассмотрим пересечение всех подполей, содержащих корни θ_i. Оно тоже разлагает многочлен f на линейные множители, и кроме того обладает свойством минимальности, т. е. не существует промежуточного подполя, над которым f разлагается на линейные множители. Такое поле называется *полем разложения* многочлена f.

Теорема 2.7. *Все поля разложения многочлена $f \in K[x]$ изоморфны между собой над K.*

□ Будем вести доказательство индукцией по $n = \deg f \geqslant 1$. Для $n = 1$ доказывать нечего, ибо поле разложения просто совпадает с K. Пусть утверждение теоремы верно для всех многочленов степени меньше n над любым полем. Покажем, что и для n это справедливо. Пусть E и E' — поля разложения $f \in K[x]$. Выберем неприводимый множитель p многочлена f, и пусть $\theta \in E\colon p(\theta) = 0$ и $\theta' \in E'\colon p(\theta') = 0$. Тогда по теореме о вложении получаем $L := K(\theta) = {}^{K[x]}\!/_{(p)} \hookrightarrow E$ и $L' := K(\theta') = {}^{K[x]}\!/_{(p)} \hookrightarrow E'$. Тогда ясно, что $L \cong L'$ над K. Отождествим в силу этого изоморфизма поля L и L', а также корни θ и θ'. Поэтому далее можно считать, что $L \subset E, L \subset E'$. Заметим, что многочлен f представим над L как $f = (x-\theta)g$, где $\deg g = n-1, g \in L[x]$. Покажем, что E и E' есть поля разложения g. Действительно, если f разлагается над E на линейные множители, то и g разлагается. Однако, если бы существовало промежуточное подполе F над которым g разлагается, и $L \subset F \subsetneq E$, то F было бы полем разложения f, что невозможно. Аналогично устанавливаем, что E' есть поле разложения g. По предположению индукции имеем $E \cong E'$ над L. Поскольку $K \subset L$, тем более имеет место изоморфизм $E \cong E'$

над K. ■

2.3. Алгебраические элементы. Алгебраическая замкнутость

Теорема 2.8 (О простых подполях). *Пусть K — поле. Если* $\operatorname{char} K = 0$, *то* $\mathbb{Q} \hookrightarrow K$. *Если* $\operatorname{char} K \neq 0$, *то* $F_p \hookrightarrow K$.

□ Пусть $\operatorname{char} K = 0$. Рассмотрим $\varphi\colon \mathbb{Q} \to K$, определённое по правилу $\varphi\colon \frac{m}{n} \mapsto (m \cdot 1)(n \cdot 1)^{-1}$. Очевидно, φ сохраняет операцию. Но φ инъективно по теореме об инъективности. Пусть $\operatorname{char} K = p$, тогда $p \in \mathfrak{P}$. Пусть $\varphi\colon \mathbb{Z} \to K$ — гомоморфизм, где $\varphi\colon m \mapsto m{\cdot}1$. Имеем: $m \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(m) = me = 0 \Leftrightarrow p \,\big|\, m$. Значит, $\operatorname{Ker}\varphi = (p) \lhd \mathbb{Z}$. Отсюда по теореме о гомоморфизмах колец $F_p = {}^{\mathbb{Z}}\!/_{(p)} \hookrightarrow K$. ■

Определение. Пусть F — простое алгебраическое расширение поля K. Обозначим через $[F : K]$ *размерность* $\dim_K F$, которая, по доказанному выше, есть степень неприводимого многочлена, по которому мы проводили факторизацию.

Определение. Элемент $\alpha \in F$ называется *алгебраическим над* K, если $\exists\, f \in K[x]\colon f(\alpha) = 0$.

Если $[F : K] < \infty$, то все элементы F алгебраические. В самом деле, пусть $m := [F : K]$. Рассмотрим $\alpha \in F$ и пусть $n > m$. Рассмотрим элементы $e, \alpha, \alpha^2, \ldots, \alpha^n$. Они будут линейно зависимы, значит, найдётся нетривиальная линейная комбинация $c_0 e + c_1\alpha + \ldots + c_n\alpha^n = 0$. Тогда $c_0, \ldots, c_n$ и будут коэффициентами искомого многочлена, имеющего корень α.

Теорема 2.9 (О размерности короткой башни полей). *Пусть $K \subset L \subset F$ — короткая башня полей, и* $[F : L] < \infty$ *и* $[L : K] < \infty$. *Тогда* $[F : K] = [F : L] \cdot [L : K]$.

□ В самом деле, пусть $x_1, \ldots, x_m$ — базис L над K, а $y_1, \ldots, y_n$ — базис F над L. Докажем, что $\mathcal{B} = \{x_i y_j\}$ будет базисом F над K, откуда и будет следовать утверждение теоремы. Покажем, что через $\mathcal{B}$ выражается любой элемент F. В самом деле, пусть $z \in F$, тогда $z = \beta_1 y_1 + \ldots + \beta_n y_n$, где $\beta_j \in L$. Отсюда $\beta_j = \alpha_{1j}x_1 + {} + \ldots + \alpha_{mj}x_m$. Значит, если мы подставим β_j в выражение для z, получим $z = \sum\limits_{j=1}^{n}\sum\limits_{i=1}^{m} \alpha_{ij}x_i y_j$, и выразимость доказана. Теперь докажем линейную независимость. Пусть $0 = \sum c_{ij}x_i y_j = \sum\bigl(\sum c_{ij}x_i\bigr)y_j = 0$. Но поскольку $c_{ij} \in K$, получаем, что $r_j := \sum c_{ij}x_i \in L$, значит, поскольку $\{y_j\}$ — базис, получаем, что $r_j = 0$, $\forall\, j$. Но так как $\{x_i\}$ — базис, получаем, что при каждом j имеем $c_{ij} = 0$, $\forall\, i$. Итак, все $c_{ij} = 0$, значит, только тривиальные линейные комбинации векторов $\mathcal{B}$ могут быть равны 0. Значит, $\mathcal{B}$ — базис. ■

Следствие 2.1. *Пусть E — поле разложения многочлена $f \in K[x]$. Тогда* $[E : K] < \infty$.

□ Как было показано ранее, если p — неприводим, то ${}^{K[x]}\!/_{(p)}$ — поле размерности $\deg p$ над K, поэтому, как следует из алгоритма построения поля разложения, его размерность над K по предыдущей теореме будет конечна, ибо мы расширяем поле не более $\deg f$ раз. ■

Определение. Пусть F — алгебраически замкнутое расширение поля K. Напомним, что *алгебраическая замкнутость* поля означает, что любой многочлен положительной степени над этим полем имеет в нём корни. Пусть $\overline{K}$ — множество корней в F многочленов из $K[x]$. $\overline{K}$ называется *алгебраическим замыканием* поля K.

Теорема 2.10. *Множество $\overline{K}$ является алгебраически замкнутым подполем F.*

□ Покажем, что $\overline{K}$ — подполе. Пусть $f_1, f_2 \in K[x]$ и $f_1(\alpha_1) = 0, f_2(\alpha_2) = 0$, где $\alpha_i \in \overline{K}$. Возьмём $f := f_1 f_2$, тогда α_i — его корни. Пусть $E \hookrightarrow F$ — поле разложения f. E — поле, значит, $\alpha_1\alpha_2, \alpha_1^{-1}, \alpha_1 + \alpha_2 \in E$. Так как $[E : K] < \infty$, все элементы E алгебраичны над K, значит, все они лежат в $\overline{K}$.

Покажем, что $\overline{K}$ алгебраически замкнуто. Рассмотрим $f = c_n x^n + \ldots + c_0 \in \overline{K}[x]$. Расширим поле K, присоединив к нему все c_i, получим поле E. Тогда $E \hookrightarrow F$ и $[E : K] < \infty$. Теперь можно утверждать, что $f \in E[x]$. В силу алгебраической замкнутости F, $\exists\, \theta \in F\colon f(\theta) = 0$. Пусть $E(\theta) \hookrightarrow F$ — расширение, полученное присоединением корня θ. Тогда $[E(\theta) : E] < \infty$. По теореме о короткой башне полей имеем $[E(\theta) : K] < \infty$, откуда все элементы $E(\theta)$ алгебраичны над K. Значит, θ есть корень некоторого многочлена из $K[x]$ и потому $\theta \in \overline{K}$. ■

Пример 3.1. Рассмотрим $\mathbb{C} \supset \mathbb{Q}$. Рассмотрим подполе *алгебраических чисел* $\overline{\mathbb{Q}}$. Остальные числа $\mathbb{C} \setminus \overline{\mathbb{Q}}$ называются *трансцендентными*. Заметим, что множество трансцендентных чисел имеет мощность континуум, в то время как $\bigl|\overline{\mathbb{Q}}\bigr| = \aleph_0$.

2.4. Конечные поля

Пусть F_q — конечное поле порядка q. Очевидно, $\operatorname{char} F_q = p \in \mathfrak{P}$. Мы знаем, что $F_p \hookrightarrow F_q$ и $[F_q : F_p] < \infty$ в силу конечности полей. Пусть $y \in F_q$, тогда $\exists!$ разложение вида $y = c_1x_1 + \ldots + c_nx_n$, где $c_i \in F_p$. Тогда мощность F_q будет равна количеству строк вида $(c_1, \ldots, c_n)$, а их, очевидно, будет p^n штук, отсюда $|F_q| = p^n$.

Пусть $x, y \in F_q$. Покажем, что $(x+y)^p = x^p + y^p$. В самом деле, имеем $(x+y)^p = \sum\limits_0^p \binom{p}{i} x^i y^{p-i}$. Но так как $p \,\big|\, \binom{p}{i}$ при $i \neq 0, i \neq p$, то для таких i в поле характеристики p будем иметь $\binom{p}{i} = 0$. Тогда $(x+y)^p = x^p + y^p$.

Имеем $|F_q^*| = p^n - 1$. По теореме Лагранжа имеем для $a \in F_q^*$ соотношение $a^{p^n-1} = 1$. Тогда $a^{p^n} = a$. Рассмотрим $f(x) = x^{p^n} - x \in F_p[x]$. Тогда любой элемент F_q является его корнем. Но у него не может быть больше p^n корней по теореме Безу, поэтому F_q — поле разложения этого многочлена. Отсюда следует единственность с точностью до изоморфизма поля из p^n элементов, поскольку все они будут изоморфны как поля разложения некоторого многочлена.

Теперь докажем, что такие поля существуют. Рассмотрим $p \in \mathfrak{P}$ и $n \in \mathbb{N}$. Пусть $f = x^{p^n} - x \in F_p[x]$. Рассмотрим формальную производную этого многочлена: получим $f' = p^n x^{p^n-1} - 1 = -1$ в $F_p[x]$. Значит, у него нет кратных корней. Пусть E — поле разложения f. Покажем, что все корни f образуют подполе $\mu \subset E$. Пусть $f(\alpha) = 0, f(\beta) = 0$. Имеем $\alpha^{p^n} = \alpha$ и $\beta^{p^n} = \beta$. Рассмотрим $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$. Отсюда $f(\alpha+\beta) = 0$. Совершенно аналогично показывается, что произведение корней $\alpha\beta$ и α^{-1} также лежат в подполе μ. Тогда, поскольку E — минимальное поле, над которым f разложим на линейные множители, получаем, что $E = \mu$. Отсюда $|E| = p^n$.

Теорема 2.11. *Инъекция $F_{p^n} \hookrightarrow F_{p^m}$ существует $\Leftrightarrow n \,\big|\, m$.*

□ Пусть инъекция существует. Тогда положим $r := [F_{p^m} : F_{p^n}]$. По теореме о размерности короткой башни полей $F_p \subset F_{p^n} \subset F_{p^m}$ получаем $nr = m$, что и требуется.

Обратно, пусть $m = nr$. Имеем $p^m - 1 = p^{nr} - 1 = (p^n)^r - 1 = (p^n - 1)t$. Имеем также $x^{p^m} - x = \left(x^{p^m-1} - 1\right) x = x\left(x^{(p^n-1)t} - 1\right) = x\left(x^{p^n-1} - 1\right) g(x)$, где вид g нас не интересует. Отсюда $x^{p^m} - x = (x^{p^n} - x) g(x)$. Значит, все корни многочлена $x^{p^n} - x$ являются корнями многочлена $x^{p^m} - x$. Из этого следует вложение. ■

Теорема 2.12. *Пусть $a, b \in G, ab = ba, \langle a \rangle_m \cap \langle b \rangle_n = \{e\}$. Тогда $O(ab) = [m, n]$.*

□ Имеем $(ab)^s = e \Leftrightarrow a^s b^s = e \Leftrightarrow a^s = b^{-s}$. Но $a^s \in \langle a \rangle$, а $b^{-s} \in \langle b \rangle$, значит, поскольку пересечение только по единице, получаем $a^s = e, b^{-s} = e$. Значит, $m \,\big|\, s, n \,\big|\, s$, откуда $[m, n] \,\big|\, s$. Поэтому $O(ab) = [m, n]$. В случае, если $(m, n) = 1$, получаем, что $O(ab) = mn$. ■

Определение. Пусть $n = p^s \cdot k$, причём $(k, p) = 1$ и $p \in \mathfrak{P}$. Тогда p^s называется *примарным делителем* числа n по p.

Теорема 2.13. *Мультипликативная группа конечного поля является циклической.*

□ Пусть F_q — поле порядка q, значит, $|F_q^*| = q - 1$. Рассмотрим элемент a максимального порядка в F_q^*: $O(a) = n$. Покажем, что $F_q^* = \langle a \rangle_n$. Допустим противное, именно, $\exists b\colon b \notin \langle a \rangle$. Рассмотрим произвольное $p \in \mathfrak{P}$ среди делителей n. Возьмём примарный по p делитель: $n = p^s k$. Рассмотрим $m := O(b)$. Представим m в виде $m = p^t r$, и покажем, что $s \geqslant t$. В самом деле, допустим, $s < t$. Тогда рассмотрим $\left\langle a^{p^s} \right\rangle_k \cap \langle b^r \rangle_{p^t} = \{e\}$, поскольку по теореме Лагранжа порядок элемента из пересечения делит и k, и p^t, а они взаимно просты. Тогда по предыдущей теореме получаем, что $O\left(a^{p^s} \cdot b^r\right) = kp^t > kp^s = n$. Этого не может быть, ведь мы выбрали элемент максимального порядка. Значит, получаем, что $m \,\big|\, n$, ибо число p можно было брать любым. Тогда получаем, что уравнение $x^n = 1$ имеет $n + 1$ корень: n корней из $\langle a \rangle_n$ и ещё корень b. Такого не бывает, значит, $\langle a \rangle_n = F_q^*$. ■

Теорема 2.14. *Над конечным полем F_q, где $q = p^m$ и $\operatorname{char} F_q = p$, существуют неприводимые многочлены любой степени.*

□ Найдём многочлен степени n над полем F_q. Рассмотрим поле F_r, где $r = q^n$. Такое поле существует, ибо $r = p^{mn}$. Так как $m \,\big|\, mn$, существует вложение $F_q \hookrightarrow F_r$, причём $\dim_{F_q} F_r = n$. По предыдущей теореме $F_r^* = \langle \theta \rangle_{r-1}$. Рассмотрим отображение $\varphi\colon F_q[x] \to F_r$ по правилу $\varphi\colon f \mapsto f(\theta)$. Поскольку $\varphi(0) = 0$, а $\varphi(x^k) = \theta^k$, получаем, что φ — эпиморфизм. По теореме о гомоморфизмах колец имеем $F_q[x]/\operatorname{Ker}\varphi \cong F_r$. Заметим, что $\operatorname{Ker}\varphi$ — главный идеал, порождённый некоторым неприводимым многочленом d. Действительно, если бы он был приводим, фактор по нему не был бы полем. Поскольку $\dim_{F_q} F_r = n$, получаем, что $\deg d = n$, и многочлен найден. ■

3. Конечнопорождённые абелевы группы

3.1. Прямые произведения групп

3.1.1. Внутренние произведения

Определение. *Произведением* подмножеств $A_1, \ldots, A_m$ группы G назовём множество

$$A_1 \cdot \ldots \cdot A_m := \{a_1 \cdot \ldots \cdot a_m \mid a_i \in A_i\}.$$

Пусть $A, B \subset G$. Скажем, что A и B *коммутируют как подмножества*, если $AB = BA$. Подмножества A и B *коммутируют поэлементно*, если $\forall\, a \in A$, $\forall\, b \in B$ имеем $ab = ba$.

Очевидно, если подмножества коммутируют поэлементно, то они коммутируют и как подмножества.

Задача 3.1. *Приведите пример двух коммутирующих подмножеств, не коммутирующих поэлементно.*

Пусть A, B — подгруппы G.

Задача 3.2. *Приведите пример, когда AB не будет подгруппой G.*

Заметим, что если $B \lhd G$, то $AB = BA$. В самом деле, рассмотрим $a \in A, b \in B$. Тогда $ab = (aba^{-1})a \in BA$, поскольку в силу нормальности B имеем $aba^{-1} \in B$. Значит, $AB \subset BA$. Аналогично, $BA \subset AB$. Значит, $AB = BA$.

Теорема 3.1. *Если подгруппы $H_i \subset G$ попарно коммутируют, то $H := H_1 \cdot \ldots \cdot H_m$ — подгруппа в G, не зависящая от порядка сомножителей. Если подгруппа H_i коммутирует поэлементно со всеми остальными множителями H_j, то $H_i \lhd H$.*

□ Докажем, что H — подгруппа в G. Доказывать будем индукцией по m. При $m = 1$ доказывать нечего. Пусть $m = 2$, тогда $A, B \subset G$. Рассмотрим $a_1b_1, a_2b_2 \in AB$. Имеем $(a_1b_1)^{-1}(a_2b_2) = \underbrace{b_1^{-1}a_1^{-1}a_2}_{a_3b_3}\, b_2 \in AB$. Значит, AB — подгруппа. Докажем шаг индукции: пусть $m \geqslant 3$ и $H = \underbrace{H_1 \cdot \ldots \cdot H_{m-1}}_{L} H_m$. По предположению индукции L — подгруппа, поскольку там $m - 1$ множитель. Кроме того, поскольку H_i попарно коммутируют, получаем $LH_m = H_mL$, и тогда LH_m — подгруппа, поскольку здесь тоже меньше, чем m сомножителей. Итак, H — подгруппа в G.

Пусть имеет место поэлементное коммутирование. Покажем, что $H_i \lhd H$. В самом деле, пусть $h \in H$. Тогда $h = h_1 \cdot \ldots \cdot h_i \cdot \ldots \cdot h_m$. Далее $\widehat{h_i}$ обозначает пропуск соответствующего множителя. Имеем $hH_i = (h_1 \cdot \ldots \cdot h_i \cdot \ldots \cdot h_m)H_i = \{$ в силу поэлементного коммутирования $\} = (h_1 \cdot \ldots \cdot \widehat{h_i} \cdot \ldots \cdot h_m)(h_iH_i) = (h_1 \cdot \ldots \cdot \widehat{h_i} \cdot \ldots \cdot h_m)H_i = \{$ в силу поэлементного коммутирования, H_i можно протащить через произведение $\} = H_i(h_1 \cdot \ldots \cdot \widehat{h_i} \cdot \ldots \cdot h_m) = (H_ih_i)(h_1 \cdot \ldots \cdot \widehat{h_i} \cdot \ldots \cdot h_m) = H_i(h_1 \cdot \ldots \cdot h_i \cdot \ldots \cdot h_m) = H_ih$, а, значит, левый смежный класс совпадает с правым. ■

Следствие 3.1. *Если все $H_i \lhd G$, то $H = H_1 \cdot \ldots \cdot H_m \lhd G$.*

□ Поскольку нормальные подгруппы заведомо коммутируют как подмножества, получаем, что H — подгруппа в G. Рассмотрим $g \in G$, тогда $gHg^{-1} = g(H_1 \cdot \ldots \cdot H_m)g^{-1} = (gH_1g^{-1}) \cdot \ldots \cdot (gH_mg^{-1}) = H_1 \cdot \ldots \cdot H_m = H \Rightarrow H \lhd G$, ибо нормальные подгруппы инвариантны относительно внутренних автоморфизмов. ■

Определение. Произведение подгрупп $H_i \subset G$ называется *прямым*, если H_i коммутируют между собой поэлементно и $\forall\, h \in H = H_1 \cdot \ldots \cdot H_m$ существует единственный набор $(h_1, \ldots, h_m)$: $h = h_1 \cdot \ldots \cdot h_m, h_i \in H_i$. Заметим, что в силу поэлементного коммутирования имеем $H_i \lhd H$.

Обозначения: $H = H_1 \times \ldots \times H_m$ для мультипликативной терминологии, $H = H_1 \oplus \ldots \oplus H_m$ — для аддитивной.

Теорема 3.2 (О прямом произведении). *Пусть $H_i \lhd G$. Тогда $H = H_1 \times \ldots \times H_m \Leftrightarrow \forall\, i$ имеем $H_i \cap (H_1 \cdot \ldots \cdot \widehat{H_i} \cdot \ldots \cdot H_m) = \{e\}$.*

□ Пусть $H = H_1 \times \ldots \times H_m$. Тогда $M := H_i \cap (H_1 \cdot \ldots \cdot \widehat{H_i} \cdot \ldots \cdot H_m)$. Рассмотрим $x \in M$. С одной стороны, поскольку $x \in H_i$, получаем $x = e \cdot \ldots \cdot \underset{i}{x} \cdot \ldots \cdot e$. С другой стороны, $x = h_1 \cdot \ldots \cdot \underset{i}{e} \cdot \ldots \cdot h_m$. Но представление x в виде произведения множителей из H_j единственно, значит, $x = e$. Следовательно, $M = \{e\}$.

Обратно, пусть пересечение тривиально. Рассмотрим коммутатор $[h_i, h_j] = h_ih_jh_i^{-1}h_j^{-1}$. Имеем $h_ih_jh_i^{-1} \in H_j$ в силу нормальности H_j. Но $h_jh_i^{-1}h_j^{-1} \in H_i$ в силу нормальности H_i. Значит, $[h_i, h_j] \in H_i \cap H_j = \{e\}$. Следовательно, $h_ih_j = h_jh_i$, и мы доказали поэлементное коммутирование. Теперь докажем единственность разложения. Пусть $x \in H = h_1 \cdot \ldots \cdot h_i \cdot \ldots \cdot h_m = h'_1 \cdot \ldots \cdot h'_i \cdot \ldots \cdot h'_m$. Тогда, пользуясь коммутированием, получаем $h_i(h_1 \cdot \ldots \cdot \widehat{h_i} \cdot \ldots \cdot h_m) = h'_i(h'_1 \cdot \ldots \cdot \widehat{h'_i} \cdot \ldots \cdot h'_m)$. Далее, $h_i(h'_i)^{-1} = (h'_1 \cdot \ldots \cdot \widehat{h'_i} \cdot \ldots \cdot h'_m)(h_m^{-1} \cdot \ldots \cdot \widehat{h_i^{-1}} \cdot \ldots \cdot h_1^{-1})$. Теперь, поскольку $h'_mh_m^{-1} \in H_m$, он коммутирует с элементами других подгрупп, поэтому этот множитель можно переставить в «хвост» произведения. Теперь, поскольку $h'_{m-1}h_{m-1}^{-1} \in H_{m-1}$, его тоже можно переставить на предпоследнее место. Так будем переставлять их, пока не получим $h_i(h'_i)^{-1} = (h'_1h_1^{-1}) \cdot \ldots \cdot (\widehat{h'_ih_i^{-1}}) \cdot \ldots \cdot (h'_mh_m^{-1})$. Но поскольку пересечение подгрупп единичное, получаем $h_i(h'_i)^{-1} = \{e\}$. Значит, $h_i = h'_i$, и мы доказали единственность разложения. ■

3.1.2. Внешние произведения

Определение. Пусть $G_1, \ldots, G_m$ — группы. Рассмотрим обычное декартово произведение $G := G_1 \times \ldots \times G_m$ и определим на нём операцию покомпонентного умножения: $(g_1, \ldots, g_m) \cdot (g'_1, \ldots, g'_m) := (g_1g'_1, \ldots, g_mg'_m)$. Очевидно, это будет группой с единицей в виде строки единиц групп G_i. В этом случае G называется *прямым произведением групп* $G_1, \ldots, G_m$ и обозначается так же, как и внутреннее произведение.

Рассмотрим $\widetilde{G_i} := \{\widetilde{g_i} = (e_1, \ldots, g_i, \ldots, e_m), g_i \in G_i\}$. Очевидно что $\widetilde{G_i}$ образуют подгруппы в G. Осуществим канонический изоморфизм $G_i \to \widetilde{G_i}$ по правилу $g_i \mapsto \widetilde{g_i}$. Тогда можно мысленно отождествить G_i и $\widetilde{G_i}$. Тогда $G_i \hookrightarrow G$. Заметим, что $G = \widetilde{G_1} \times \ldots \times \widetilde{G_m}$. В самом деле, элементы между собой коммутируют, разложение единственно, а пересечение, очевидно, единичное.

Теорема 3.3 (О факторизации по прямым множителям). *Пусть $G = G_1 \times \ldots \times G_m$. Пусть $H_i \lhd G_i$. Рассмотрим $H = H_1 \times \ldots \times H_m$. Тогда $H \lhd G$ и ${}^{G}\!/_{H} \cong {}^{G_1}\!/_{H_1} \times \ldots \times {}^{G_m}\!/_{H_m}$.*

□ Рассмотрим отображение $\varphi\colon G \to {}^{G_1}\!/_{H_1} \times \ldots \times {}^{G_m}\!/_{H_m}$, определённое по правилу

$$\varphi\colon g = (g_1, \ldots, g_m) \mapsto (g_1 H_1, \ldots, g_m H_m).$$

Оно сохраняет операцию: $\varphi(gg') = \big((g_1 g_1')H_1, \ldots, (g_m g_m')H_m\big) = (g_1 H_1, \ldots, g_m H_m)\cdot(g_1' H_1, \ldots, g_m' H_m) = \varphi(g)\varphi(g')$. Сюръективность φ очевидна, ибо на любую строку смежных классов отображается строка их представителей. Поэтому φ — эпиморфизм. Далее, $g \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(g) = (g_1 H_1, \ldots, g_m H_m) = (H_1, \ldots, H_m) \Leftrightarrow g_i \in H_i$. Отсюда $\operatorname{Ker}\varphi = H$, и, факторизуя по H, по теореме о гомоморфизме групп получаем требуемое. ■

3.2. Конечнопорождённые абелевы группы

Определение. Пусть G — абелева группа. Мы будем придерживаться аддитивной терминологии для абелевых групп. Говорят, что G *порождается* системой $g_1, \ldots, g_m$, если $\forall\, g \in G$ имеем $g = n_1 g_1 + \ldots + n_m g_m$, где $n_i \in \mathbb{Z}$. Тогда G называют *конечнопорождённой абелевой группой.*

Определение. Система порождающих $x_1, \ldots, x_m$ группы G называется *базой* (*базисом*), если она «линейно независима» над $\mathbb{Z}$, т. е. только тривиальные целочисленные линейные комбинации базисных векторов могут быть равны 0. Очевидно, если $x_1, \ldots, x_m$ — база, то представление любого элемента группы через базисные вектора единственно. В самом деле, если бы их было два, то можно вычесть одно из другого и получить нетривиальную, но равную нулю линейную комбинацию.

Определение. КПАГ G называется *свободной*, если она обладает базой. Заметим, что далеко не каждая абелева группа свободна. Например, конечная ненулевая абелева группа имеет конечное число порождающих, но никогда не бывает свободной, поскольку там все элементы имеют конечный порядок, значит, для любого ненулевого базисного вектора x найдётся $n \in \mathbb{N}$: $nx = 0$, значит, система даже из одного базисного вектора будет линейно зависимой.

Рассмотрим группу $G = \langle x_1 \rangle_\infty \oplus \ldots \oplus \langle x_m \rangle_\infty \cong \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{m} \hookrightarrow \mathbb{Q}^m$. Заметим, что если существует нетривиальная линейная зависимость над $\mathbb{Q}$, то она есть и над $\mathbb{Z}$. Достаточно все дроби домножить на их общий знаменатель.

Теорема 3.4. *Все базы САГ G имеют одинаковое количество элементов.*

□ Пусть $\mathcal{X} = \{x_1, \ldots, x_m\}$ и $\mathcal{Y} = \{y_1, \ldots, y_n\}$ — две различные базы. Допустим, что $m \neq n$, и для определённости $m > n$. Тогда, поскольку каждый вектор x_i выражается через вектора базы $\mathcal{Y}$, получаем $(x_1, \ldots, x_m) = (y_1, \ldots, y_n)C$, где C — целочисленная матрица, в которой n строк и m столбцов. Но по основной лемме о линейной зависимости столбцы C линейно зависимы над $\mathbb{Q}$ (ведь мы доказывали эту лемму для произвольного поля). Значит, как уже было сказано, имеет место и нетривиальная линейная зависимость между векторами $\mathcal{X}$ над $\mathbb{Z}$, а это невозможно. ■

Определение. Число векторов базиса САГ называется её *рангом.* Из теоремы следует, что определение корректно. По определению, нулевая группа считается *свободной абелевой группой ранга* 0.

Пусть G — САГ с базисом $x_1, \ldots, x_m$. Произвольное отображение векторов базиса в элементы некоторой абелевой группы L продолжается естественным образом до гомоморфизма. Действительно, пусть $\varphi\colon G \to L$, причём $\varphi(x_i) = a_i$. Имеем $\varphi(n_1 x_1 + \ldots + n_m x_m) = n_1 a_1 + \ldots + n_m a_m$, причём отображение задано корректно благодаря единственности разложения элемента G по базису.

Теорема 3.5. *Всякая КПАГ L с m порождающими изоморфна некоторому фактору САГ G ранга m.*

□ Пусть G — САГ с базисом $x_1, \ldots, x_m$, а $L = \langle a_1, \ldots, a_m \rangle$. Как было сказано выше, корректно задан гомоморфизм $\varphi\colon G \to L$, при котором $x_i \mapsto a_i$. Поскольку $a_1, \ldots, a_m$ порождают G, этот гомоморфизм будет сюръективен, ведь мы перебираем все строки вида $(n_1, \ldots, n_m)$. Тогда по теореме о гомоморфизме групп получаем ${}^{G}\!/_{\operatorname{Ker}\varphi} \cong L$. ■

Теорема 3.6 (О согласованных базах). *Пусть G — САГ ранга m и H — ненулевая подгруппа в G. Тогда H — САГ ранга $l \leqslant m$, причём существуют согласованные базы $\mathcal{X} = \{x_1, \ldots, x_m\}$ группы G и $\mathcal{Y} = \{y_1, \ldots, y_l\}$ группы H, такие, что $y_i = n_i x_i$.*

□ Будем вести индукцию по рангу m САГ. При $m = 1$ доказывать нечего: $G \cong \mathbb{Z} = \langle 1 \rangle_\infty$, а поскольку любая подгруппа $H \subset \mathbb{Z}$ имеет строение $n\mathbb{Z}$, то для неё базисом будет вектор $y_1 = n \cdot 1$.

1° Рассмотрим $h = a_1x_1 + \ldots + a_mx_m$, для которого $a_1 \in \mathbb{N}$ реализует минимально возможный коэффициент по всем a_i и по всем возможным базам группы G.

2° Рассмотрим другой элемент $h' = a'_1x_1 + \ldots + a'_mx_m \in H$. Докажем, что $a_1 \,\big|\, a'_1$. В самом деле, допустим, что это не так, поделим с остатком: $a'_1 = a_1q + r$. Рассмотрим элемент $h' - qh = rx_1 + \ldots$. Но этого не может быть, поскольку мы договорились, что a_1 реализует минимум среди коэффициентов. Значит, $r = 0$, и тогда $a_1 \,\big|\, a'_1$.

3° Покажем, что $a_1 \,\big|\, a_i, i = 1, \ldots, m$. Допустим, что $a_i = a_1q + r$. Перейдём к новой базе $\{x_1 + qx_i, x_2, \ldots, x_m\}$ и положим $x'_1 := x_1 + qx_i$. Ясно, что целочисленные элементарные преобразования не нарушают линейной независимости. Но тогда в этой базе $h = a_1x'_1 + \ldots + rx_i + \ldots$. Этого тоже не может быть, поскольку мы договорились, что a_1 реализует минимум по всем возможным базам G.

4° Теперь мы точно знаем, что $a_i = a_1q_i, i = 2, \ldots, m$. Выберем новый первый вектор для базы G, а остальные оставим без изменения: $x'_1 = x_1 + q_2x_2 + \ldots + q_mx_m$. В новой базе имеем $h = a_1x'_1$. Пусть $H_1 := \langle h \rangle_\infty$, $G_0 := \langle x_2 \rangle_\infty \oplus$ $\oplus \ldots \oplus \langle x_m \rangle_\infty$. Рассмотрим $H_0 := H \cap G_0$. Очевидно, $H_1 \cap H_0 = \{0\}$. Заметим, что $H = H_1 \oplus H_0$. В самом деле, покажем, что $\forall\, h' \in H$ представим в виде суммы элементов из H_1 и H_0. Пусть $h' = a'_1x'_1 + \ldots$. Тогда по доказанному имеем $a_1 \,\big|\, a'_1$, т. е. $a'_1 = a_1q_1$. Рассмотрим $h' - q_1h = 0 \cdot x'_1 + \cdots = h'' \in H_0$, поскольку оставшаяся часть будет некоторой линейной комбинацией $x_2, \ldots, x_m$. Следовательно, $h' = q_1h_1 + h''$, и представимость доказана.

5° Вспомним, что мы ведём индукцию по рангу G. Имеем $\operatorname{rk} G_0 = m - 1$, и поскольку $H_0 \subset G_0$ — САГ, и по предположению индукции её ранг не превосходит $m - 1$, и существуют согласованные базы $x'_2, \ldots, x'_m$ группы G_0 и $y_2, \ldots, y_l$ группы H_0, и эти базы согласованы числами $n_2, \ldots, n_m$. В силу того, что $H = \langle h \rangle_\infty \oplus H_0$, откуда $\operatorname{rk} H = l$. Мы знаем, что $h = a_1x'_1$. Значит, чтобы получить согласованные базы для G и H, достаточно взять x'_1 и уже выбранную базу G_0, а для H взять y_1 и уже выбранную базу H_0. При этом $n_1 := a_1$. ■

Следствие 3.2. *Всякая КПАГ является прямой суммой циклических подгрупп (конечных и бесконечных).*

□ Пусть L — КПАГ. Тогда $L \cong {}^{G}\!/_{H}$, где G — САГ некоторого ранга, и $H \subset G$ — подгруппа. Выберем согласованные базы в G и H, и пусть $x_1, \ldots, x_m$ — база G, а $y_1, \ldots, y_l$ — база H, причём $y_i = n_ix_i$. Тогда $G = \langle x_1 \rangle_\infty \oplus \ldots \oplus \langle x_l \rangle_\infty \oplus \langle x_{l+1} \rangle_\infty \oplus \ldots \oplus \langle x_m \rangle_\infty$, а H можно представить в виде $H = \langle n_1x_1 \rangle_\infty \oplus \ldots \oplus \langle n_lx_l \rangle_\infty \oplus$ $\oplus \langle 0 \rangle_1 \oplus \ldots \oplus \langle 0 \rangle_1$. Тогда можно профакторизовать по прямым слагаемым, и получим ${}^{G}\!/_{H} \cong {}^{\langle x_1 \rangle}\!/_{\langle n_1x_1 \rangle} \oplus \ldots \oplus$ $\oplus\, {}^{\langle x_l \rangle}\!/_{\langle n_lx_l \rangle} \oplus {}^{\langle x_{l+1} \rangle}\!/_{\langle 0 \rangle} \oplus \ldots \oplus {}^{\langle x_m \rangle}\!/_{\langle 0 \rangle}$. Но поскольку ${}^{\langle x_i \rangle}\!/_{\langle n_ix_i \rangle} \cong {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$, а ${}^{\langle x_i \rangle}\!/_{\langle 0 \rangle} \cong \mathbb{Z}$, получаем, что $L \cong {}^{G}\!/_{H} \cong \mathbb{Z}_{n_1} \oplus$ $\oplus \ldots \oplus \mathbb{Z}_{n_l} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$, что и требуется. ■

3.3. Разложение на примарные циклические группы

Опишем способ вычисления порядка элемента прямого произведения групп. Пусть $G = G_1 \times \ldots \times G_m$, причём G не обязательно абелева. Имеем $g = g_1 \cdot \ldots \cdot g_m$. Тогда $O(g) = \big[O(g_1), \ldots, O(g_m)\big]$. В самом деле, пусть $g^s = \big\{$ поскольку элементы из различных сомножителей коммутируют между собой $\big\} = g_1^s \cdot \ldots \cdot g_m^s = e \cdot \ldots \cdot e$. Значит, имеем $O(g_i) \,\big|\, s$, отсюда следует наше утверждение. В частности, если порядки элементов взаимно просты, их наименьшее общее кратное совпадает с их произведением.

Определение. Группа называется *прямо не разложимой*, если она не представляется в виде прямого произведения.

Покажем, что $\mathbb{Z}$ прямо не разложима. В самом деле, любая подгруппа $\mathbb{Z}$ имеет вид $n\mathbb{Z}$. Следовательно, любые две подгруппы $\mathbb{Z}$, скажем, $n\mathbb{Z}$ и $m\mathbb{Z}$, содержат в своём пересечении подгруппу $mn\mathbb{Z}$, поэтому сумма никаких двух подгрупп не может быть прямой.

Определение. Если группа G имеет порядок p^n, где $p \in \mathfrak{P}$, то она называется *p-группой*.

3° Циклическая p-группа прямо не разложима. В самом деле, допустим, что имеет место нетривиальное представление $G = \langle a \rangle_{p^n} = \langle a_1 \rangle_{p^s} \oplus \langle a_2 \rangle_{p^t}$. Здесь из соображений порядков подгрупп имеем $p^n = p^s \cdot p^t$. Рассмотрим $b = b_1 + b_2 \in G$, где $b_1 \in \langle a_1 \rangle_{p^s}$, а $b_2 \in \langle a_2 \rangle_{p^t}$. Тогда имеем $O(b_1) \,\big|\, p^s, O(b_2) \,\big|\, p^t$, откуда $O(b) = [p^s, p^t] = p^{\max\{s,t\}}$. Но мы же договорились, что $s, t > 0$. Значит, в G нет элементов порядка p^n, ибо $O(b) < p^n$. Противоречие.

4° Пусть G — конечная циклическая группа, и $|G| \neq p^n, p \in \mathfrak{P}$. Тогда G разлагается в прямую сумму. Действительно, пусть $G = \langle a \rangle_n$, $n = st, (s,t) = 1$. Тогда $G = \langle ta \rangle_s \oplus \langle sa \rangle_t$. Сумма действительно прямая, ибо пересечение явно нулевое, в силу взаимной простоты s и t, а $O(ta + sa) = [s,t] = st = n$. Значит, количество элементов $\langle ta \rangle_s \oplus \langle sa \rangle_t$ совпадает с $n = |G|$. Значит, G действительно разлагается в прямую сумму.

Следствие 3.3. *Любую конечную циклическую группу можно разложить в прямую сумму примарных циклических.*

□ Будем разлагать, пока не останутся только примарные слагаемые. Рано или поздно мы остановимся. ■

3.4. Инварианты групп

Определение. *Инвариантом* группы G назовём любой объект, который никак не зависит от примарного разложения этой группы. Мы извлечём единственность разложения на примарные и бесконечные циклические группы из инвариантов.

Определение. Во всякой абелевой группе G множество элементов конечного порядка образует подгруппу, называемую *подгруппой кручения* и обозначаемую $\operatorname{Tor} G$. То, что это подгруппа, легко проверяется.

По определению, $\operatorname{Tor} G$ — инвариант G. Не менее очевидно, что в примарном разложении подгруппе $\operatorname{Tor} G$ соответствуют все прямые слагаемые конечного порядка. Значит, $G = L \oplus \operatorname{Tor} G$, где L — САГ. На основании этого мы сейчас докажем, что число бесконечных слагаемых разложения инвариантно. Заметим для начала, что если $C = A \times \ldots \times B$, то ${}^{C}\!/_{B} \cong A$, что тривиально выводится из теоремы о факторизации по прямым множителям. В нашем случае имеем ${}^{G}\!/_{\operatorname{Tor} G} \cong L$. Но тогда $\operatorname{rk} L$ — инвариант, ибо ${}^{G}\!/_{\operatorname{Tor} G}$ — инвариант. А ранг L в точности равен количеству бесконечных слагаемых в разложении.

Значит, нам остаётся доказать, что разложение $\operatorname{Tor} G$ единственно. Выделим из разложения $\operatorname{Tor} G$ *примарные компоненты* — слагаемые порядка p_i^s, где $p_i \in \mathfrak{P}$, и обозначим их G_{p_i}. Ясно, что p-примарная компонента есть прямая сумма p-примарных циклических подгрупп, порядки которых суть степени p, и потому инвариантна. Таким образом, нам осталось доказать, что каждая p-примарная компонента разложима единственным образом.

Теорема 3.7 (О единственности). *Разложение p-примарной компоненты единственно.*

□ Пусть $|G| = p^k$ и $G = \langle c_1 \rangle_{p^{k_1}} \oplus \ldots \oplus \langle c_r \rangle_{p^{k_r}}$, причём $\sum k_i = k$. Будем вести индукцию по k, и докажем, что набор $k_1, \ldots, k_r$ не зависит от разложения. При $k = 1$ доказывать нечего, ибо в группе порядка p нетривиальных подгрупп нет. Пусть $k > 1$. Рассмотрим гомоморфизм $\varphi\colon G \to G$, определённый по правилу $\varphi\colon g \mapsto pg$. Положим $pG := \varphi(G)$. Легко видеть, что $pG = \langle pc_1 \rangle_{p^{k_1-1}} \oplus \ldots \oplus \langle pc_r \rangle_{p^{k_r-1}}$. При этом обратятся в нули ровно те слагаемые, для которых $k_i = 1$. Ясно, что pG — инвариант, и, кроме того, к pG применимо предположение индукции, ибо $|pG| < |G|$. Значит, набор не обратившихся в нули k_i инвариантен, поскольку инвариантен набор $\{k_i - 1\colon k_i > 1\}$. Но и количество ушедших в нули слагаемых инвариантно, поскольку оно определяется из соотношения $k_1 + \ldots + k_r = k$ однозначно. ■

4. Действия. Разрешимые группы. Теоремы Силова

4.1. Действие группы на множестве

Определение. Говорят, что группа G *действует на множестве* $\mathcal{M}$, если задан гомоморфизм $\rho\colon G \to \mathcal{S}_{\mathcal{M}}$, где $\mathcal{S}_{\mathcal{M}}$ — группа подстановок множества $\mathcal{M}$. Обозначение: $gx = \rho(g)(x) \in \mathcal{M}$. Само действие принято обозначать либо $G\colon \mathcal{M}$, либо тройкой $(G, \rho, \mathcal{M})$.

Рассмотрим очевидные свойства действия:

1° $\forall\, g_1, g_2 \in G$, $\forall\, x \in \mathcal{M}$ имеем $(g_1 g_2)x = g_1(g_2 x)$, что следует из определения операции в $\mathcal{S}_{\mathcal{M}}$.

2° $\forall\, x \in \mathcal{M}$ имеем $ex = x$, поскольку $\rho(e) = \mathrm{id}_{\mathcal{M}}$.

Определение. *Стабилизатором (стационарной подгруппой)* элемента $x \in \mathcal{M}$ называется множество $\operatorname{St} x = \{g\colon gx = x\}$. Покажем, что это действительно подгруппа. Пусть $g_1, g_2 \in \operatorname{St} x$. Тогда $(g_1 g_2)x = g_1(g_2 x) = g_1 x = x$, поэтому $g_1 g_2 \in \operatorname{St} x$. Поскольку $ex = x$, получаем $e \in \operatorname{St} x$. Далее, пусть $g \in \operatorname{St} x$, тогда $gx = x \Leftrightarrow g^{-1}(gx) = g^{-1}x \Leftrightarrow (g^{-1}g)x = g^{-1}x \Leftrightarrow x = g^{-1}x$, а это и означает, что $g^{-1} \in \operatorname{St} x$. Итак, $\operatorname{St} x$ — подгруппа в G.

Определение. *Орбитой* элемента $x \in \mathcal{M}$ называется множество $\operatorname{Orb} x = Gx = \{gx\colon g \in G\}$.

Покажем, что орбита порождается любым своим элементом, иными словами, если $x, y \in \operatorname{Orb} x$, то $\operatorname{Orb} x = \operatorname{Orb} y$. В самом деле, поскольку $y \in \operatorname{Orb} x$, имеем $gx = y$. Но ясно, что $\operatorname{Orb} gx = \operatorname{Orb} x$, ибо $\operatorname{Orb} gx = \{hgx, h \in G\}$, а когда h бегает по G, то и hg бегает по G, поэтому $\operatorname{Orb} y$ ничем не отличается от $\operatorname{Orb} x$.

Следовательно, орбиты образуют разбиение множества $\mathcal{M}$. В самом деле, если орбиты пересекаются, то они совпадают. Действительно, если $z \in \operatorname{Orb} x \cap \operatorname{Orb} y$, то $\operatorname{Orb} x = \operatorname{Orb} z = \operatorname{Orb} y$. Кроме того, сам элемент всегда лежит на своей орбите, поскольку $ex = x$.

Покажем, что стабилизаторы элементов одной и той же орбиты сопряжены. Рассмотрим $\operatorname{St} x, \operatorname{St} y$, причём $y = gx$. Рассмотрим $a \in G$ и посмотрим, когда $a \in \operatorname{St} gx$. Имеем $a(gx) = gx \Leftrightarrow (g^{-1}ag)x = x \Leftrightarrow g^{-1}ag \in \operatorname{St} x$. Положим $h = g^{-1}ag$, тогда $a = ghg^{-1} \in g(\operatorname{St} x)g^{-1}$, что и требовалось доказать.

Покажем, что $|\operatorname{Orb} x| = (G : \operatorname{St} x)$, если $|G| < \infty, |\mathcal{M}| < \infty$. В самом деле, если элементы орбиты совпадают, т. е. $g_1 x = g_2 x \Leftrightarrow (g_1^{-1}g_2)x = x \Leftrightarrow g_1^{-1}g_2 \in \operatorname{St} x$, откуда $g_1 \operatorname{St} x = g_2 \operatorname{St} x$, т. е. смежные классы по стабилизатору совпадают. Следовательно, если мы будем брать разные элементы из орбиты, то им будут соответствовать разные смежные классы. А их количество как раз и есть $(G : \operatorname{St} x)$.

Пример 1.1. Пусть $H \subset G$ — подгруппа, $\mathcal{M} := G$, а действовать на $\mathcal{M}$ будем левыми сдвигами: $\rho(g) = L_g$. Тогда $\operatorname{Orb} g = Hg$.

Пример 1.2. Группа G действует на себе сопряжениями: $I_g x = gxg^{-1}$. Рассмотрим орбиты при сопряжении: $\operatorname{Orb} x = \{gxg^{-1}\colon g \in G\} = K_x$ — класс сопряжённости элемента x. Отсюда следует, что классы сопряжённости не пересекаются. При таком действии стабилизатор называется *централизатором* и обозначается $\mathcal{N}_x$. Заметим, что $\mathcal{N}_x$ содержит в себе все элементы группы, коммутирующие с x.

Определение. Множество элементов, коммутирующих со всеми элементами группы, называется *центром* и обозначается $\mathcal{Z}(G)$.

Ясно, что центр — абелева группа. Центр нормален в G. Действительно, пусть $z \in \mathcal{Z}(G)$. Тогда $gzg^{-1} = gg^{-1}z = z$, т. е. элементы центра неподвижны при сопряжении. Следовательно $\mathcal{Z}(G)$ состоит из неподвижных элементов и потому инвариантна относительно внутренних автоморфизмов. Значит, $\mathcal{Z}(G) \lhd G$.

Пример 1.3. Группа действует на множестве своих подгрупп сопряжениями: пусть $H \subset G$, тогда $I_g H = gHg^{-1} = H^g$. Рассмотрим стабилизатор $\operatorname{St} H = \{g \in G\colon gHg^{-1} = H \Leftrightarrow Hg = gH\}$. Такие стабилизаторы называются *нормализаторами* и обозначаются $\mathcal{N}_H$. Очевидно, $H \lhd \mathcal{N}_H$. Таким образом, нормализатор подгруппы есть максимальная подгруппа, в которой нормальна подгруппа H группы G. Обозначим через K_H орбиты этого действия. Они называются классами сопряжённых подгрупп. По доказанному выше имеем $|K_H| = (G : \mathcal{N}_H)$.

4.2. Разрешимые группы

Теорема 4.1. *Пусть A — подгруппа в G, а $B \lhd G$. Тогда ${}^{AB}\!/_{B} \cong {}^{A}\!/_{A\cap B}$.*

□ Мы уже знаем, что AB — подгруппа в G. Поскольку $B \lhd G$, тем более $B \lhd AB$. Далее, рассмотрим отображение $\varphi\colon A \to {}^{AB}\!/_{B}$, определённое по правилу $\varphi\colon a \to aB$. Покажем, что φ — эпиморфизм. $(ab)B = a(bB) = aB$, поэтому на каждый смежный класс что-то отобразится. Сохранение операции: $\varphi(a_1a_2) = (a_1a_2)B = (a_1B)(a_2B) = \varphi(a_1)\varphi(a_2)$. Рассмотрим его ядро: $a \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(a) = aB = B \Leftrightarrow a \in B$, откуда $a \in A \cap B$. Итак, φ — эпиморфизм. Осталось профакторизовать по его ядру и получить требуемое утверждение. ■

Теорема 4.2. *Пусть $B \lhd G$, а B и ${}^{G}\!/_{B}$ являются p-группами, $p \in \mathfrak{P}$. Тогда G — тоже p-группа.*

□ Пусть $|B| = p^n$, а $\left|{}^{G}\!/_{H}\right| = p^k$. Тогда имеем $|G| = |B| \cdot \left|{}^{G}\!/_{B}\right| = p^n \cdot p^k = p^{n+k}$. ■

Определение. Назовём *коммутатором* элементов $a, b \in G$ элемент $[a, b] = aba^{-1}b^{-1}$.

Очевидны свойства: $[a, b] = e \Leftrightarrow ab = ba$ и $[a, b]^{-1} = [b, a]$.

Определение. Рассмотрим подгруппу $G' \subset G$, порождённую всеми коммутаторами элементов G. Ввиду второго свойства коммутатора любой элемент G' есть произведение нескольких коммутаторов. Такая подгруппа называется *коммутантом* группы G. Индуктивно определяются *коммутанты высших порядков*: пусть $G^{(k)}$ — коммутант k-ого порядка, тогда $G^{(k+1)} = \big(G^{(k)}\big)'$. Группа G называется *разрешимой*, если $\exists\, m \in \mathbb{N}\colon G^{(m)} = \{e\}$.

Теорема 4.3. *Пусть $\varphi\colon G \to L$ — гомоморфизм групп. Тогда $\varphi\big(G^{(i)}\big) \subset L^{(i)}$.*

□ Доказывать будем по индукции. При $i = 1$ это верно, поскольку произведение коммутаторов переходит в произведение коммутаторов: $\varphi\big([a, b][c, d]\big) = \varphi\big([a, b]\big)\varphi\big([c, d]\big) = \big[\varphi(a), \varphi(b)\big]\big[\varphi(c), \varphi(d)\big]$, и потому всё, что порождено коммутаторами элементов из G, при гомоморфизме окажется в L', и база индукции доказана. Пусть теперь $\varphi\big(G^{(i)}\big) \subset L^{(i)}$. Мы уже знаем, что $\varphi\left(\big(G^{(i)}\big)'\right) \in \big(L^{(i)}\big)'$. Но это и означает, что $\varphi\big(G^{(i+1)}\big) \subset L^{(i+1)}$. ■

Теорема 4.4. *Пусть $p \in \mathfrak{P}$. Центр p-группы нетривиален.*

□ Имеем $|G| = p^n$. Рассмотрим разбиение G на классы сопряжённых элементов: $G = \bigcup K_a$. Заметим, что если $a \in \mathcal{Z}(G)$, то его класс сопряжённости состоит только из самого элемента a. Имеем $|K_a| = (G : \mathcal{N}_a)$. Если $a \notin \mathcal{Z}(G)$, то $\mathcal{N}_a \neq G$, но тогда по теореме Лагранжа p делит $|K_a|$. Имеем тогда: $|G| = p^n = |\mathcal{Z}(G)| + \sum |K_a|$. Отсюда следует, что p делит $|\mathcal{Z}(G)|$. Но это означает, что центр нетривиален. ■

Теорема 4.5. *Пусть $p \in \mathfrak{P}$. Тогда p-группа разрешима.*

□ В самом деле, будем вести индукцию по n, где n — степень множителя p в $|G|$. При $n = 1$ утверждение очевидно, ибо тогда $|G| = p$ и она циклическая, а потому абелева. Пусть $n \geqslant 2$, тогда $\mathcal{Z}(G) \neq \{e\}$. Рассмотрим $\overline{G} := {}^{G}\!/_{\mathcal{Z}(G)}$, тогда $|\overline{G}| = p^{n-1}$ и она разрешима по индуктивному предположению, т. е. $\overline{G}^{(m)} = \{\overline{e}\}$. Рассмотрим естественный эпиморфизм $\varphi\colon G \to \overline{G}$. Поскольку гомоморфный образ коммутанта содержится в коммутанте фактора, получаем, что $\varphi\big(G^{(m)}\big) = \{\overline{e}\}$, откуда $G^{(m)} \subset \operatorname{Ker}\varphi = \mathcal{Z}(G)$. Отсюда $G^{(m+1)} = \{e\}$, поскольку $\mathcal{Z}(G)$ — абелева. ■

Теорема 4.6. *Пусть G — неабелева группа. Тогда ${}^{G}\!/_{\mathcal{Z}(G)}$ не может быть циклическим.*

□ Допустим, что $\overline{G} = {}^{G}\!/_{\mathcal{Z}(G)}$ является циклической. Тогда пусть $\overline{a} = a\mathcal{Z}(G)$ — порождающий элемент в $\overline{G}$. Рассмотрим разбиение G на смежные классы. Пусть $x, y \in G$. Каждый из них лежит в каком-то из смежных классов, которые в силу цикличности фактора можно записать как $\mathcal{Z}(G), \ldots, a^{k-1}\mathcal{Z}(G)$, где $k = O(\overline{a}) = |\overline{G}|$. Следовательно, имеют место равенства $x = a^t z_1$ и $y = a^s z_2$, где $z_i \in \mathcal{Z}(G)$. Тогда $xy = a^t z_1 a^s z_2 = \{$ поскольку z_i

коммутируют со всеми элементами группы $\} = a^{t+s}z_2z_1 = a^sz_2a^tz_1 = yx$, и мы получили, что любые 2 элемента группы коммутируют между собой, т. е. G — абелева. Это невозможно по условию. Значит, фактор не может быть циклическим. ■

Следствие 4.1. *Группа $|G| = p^2$, где $p \in \mathfrak{P}$, является абелевой.*

□ Имеем: $\mathcal{Z}(G)$ нетривиален. Допустим, что G — не абелева, тогда $\mathcal{Z}(G) \neq G$. По теореме Лагранжа $|\mathcal{Z}(G)| = p$, и потому порядок фактора по центру тоже равен p. Но все группы порядка p — циклические, а, как мы знаем, фактор по центру неабелевой группы не может быть циклическим. Противоречие, значит, G — абелева. ■

4.3. Теоремы Силова

Определение. Рассмотрим группу $|G| = p^nm$, причём $p \in \mathfrak{P}$ и взят примарный по p делитель. Если $H \subset G$ и $|H| = p^n$, то такая подгруппа называется *силовской* p-подгруппой. Мы будем обозначать силовскую подгруппу символом $\mathcal{P}$ и в рассуждениях всегда будем подразумевать, что это p-подгруппа.

Теорема 4.7 (Первая теорема Силова). *Силовская p-подгруппа существует.*

□ Итак, пусть $|G| = p^nm$, где $p \in \mathfrak{P}$, причём взят примарный по p делитель. Докажем теорему индукцией по порядку G. При $|G| = p$ доказывать нечего. Пусть $|G| > p$, и для групп меньшего порядка всё доказано. Возможны два случая.

1° Пусть $p \,\big|\, |\mathcal{Z}(G)|$. Отсюда $\mathcal{Z}(G)$ нетривиален. Рассмотрим $\langle a\rangle_p \subset \mathcal{Z}(G)$. Такая есть, поскольку $\mathcal{Z}(G)$ абелева, и к ней применима теорема о разложении на примарные циклические. Тогда, поскольку элементы центра коммутируют со всеми элементами группы, получаем $\langle a\rangle_p \lhd G$. Рассмотрим $\overline{G} := {}^{G}\!/_{\langle a\rangle_p}$, причём тогда $|\overline{G}| = p^{n-1}m$.

Рассмотрим канонический эпиморфизм $\varphi\colon G \to \overline{G}$, тогда по предположению индукции $\exists\, L \subset \overline{G}$ — силовская p-подгруппа, поскольку порядок фактора меньше порядка группы. Кроме того, имеем $|L| = p^{n-1}$. Рассмотрим $\mathcal{P} := \varphi^{-1}(L) \subset G$, тогда, поскольку $L = \overline{H} = {}^{H}\!/_{\langle a\rangle_p}$, получаем $|\mathcal{P}| = p\cdot p^{n-1} = p^n$. Значит, $\mathcal{P}$ — искомая силовская подгруппа.

2° Пусть $p \nmid |\mathcal{Z}(G)|$. Тогда рассмотрим разбиение G на классы сопряжённости: $p^nm = |\mathcal{Z}(G)| + \sum |K_a|$. Из соображений делимости, найдётся нетривиальный смежный класс K_a, порядок которого не делится на p. Отсюда, поскольку $|K_a| = (G : \mathcal{N}_a)$ и $|G| = p^nm = (G : \mathcal{N}_a)\cdot|\mathcal{N}_a|$, получаем, что $p \nmid (G : \mathcal{N}_a)$, откуда $p^n \,\big|\, |\mathcal{N}_a|$. Поскольку $|\mathcal{N}_a| < |G|$, по предположению индукции $\exists\, \mathcal{P} \subset \mathcal{N}_a\colon |\mathcal{P}| = p^n$. Она и будет искомой силовской подгруппой в G. ■

Теорема 4.8 (Вторая и третья теоремы Силова). *Всякая p-подгруппа группы G содержится в некоторой силовской p-подгруппе. Все силовские p-подгруппы сопряжены.*

□ Пусть $H \subset G$ — какая либо p-подгруппа. Рассмотрим действие H на фактормножестве ${}^{G}\!/_{\mathcal{P}}$ левыми сдвигами. Так как число элементов любой нетривиальной орбиты обязано делиться на p, а $p \nmid \left|{}^{G}\!/_{\mathcal{P}}\right|$, то такое действие должно иметь неподвижные точки. Пусть $g\mathcal{P}$ — такая неподвижная точка, то есть для $\forall\, h \in H$ имеем $h\cdot ga = hga = ga'$, где $a, a' \in \mathcal{P}$. Тогда $h = g\underbrace{a'a^{-1}}_{\in\mathcal{P}}g^{-1}$, а отсюда ясно, что $\forall\, h \in H$ имеем $h \subset g\mathcal{P}g^{-1}$. Тем самым доказано первое утверждение. Теперь, пусть H — силовская p-подгруппа. По доказанному имеем $H \subset g\mathcal{P}g^{-1}$, но $|H| = |g\mathcal{P}g^{-1}| = |\mathcal{P}|$, откуда $H = g\mathcal{P}g^{-1}$. ■

Теорема 4.9 (Последняя теорема Силова). *Число силовских p-подгрупп сравнимо с 1 по модулю p.*

□ По предыдущей теореме, множество всех силовских подгрупп есть $X = \left\{g\mathcal{P}g^{-1}\colon g \in G\right\}$. Рассмотрим действие $(\mathcal{P}, I, X)$. Покажем, что единственной неподвижной точкой при таком действии будет сама $\mathcal{P}$. В самом деле, пусть $H \in X$ — неподвижная точка. Это означает, что $\mathcal{P} \subset \mathcal{N}_H$. Действительно, если при сопряжении элементами из $\mathcal{P}$ подгруппа H остаётся на месте, это означает, что $\operatorname{St} H$ содержит $\mathcal{P}$. Но стабилизатор при сопряжении — это и есть нормализатор. Но поскольку $H \subset \mathcal{N}_H$, мы нашли две силовские подгруппы в группе $\mathcal{N}_H$, а они сопряжены по предыдущей теореме. Но $H \lhd \mathcal{N}_H$, откуда $H = \mathcal{P}$. Далее, поскольку порядки всех нетривиальных орбит кратны p, получаем, что $|X| \equiv 1 \mod p$. ■

5. Элементы теории представлений

5.1. Линейные представления групп

Определение. Пусть G — группа, V — векторное пространство над полем K. *Линейным представлением* ρ группы G называется гомоморфизм вида $\rho\colon G \to \operatorname{Aut} V$, где $\operatorname{Aut} V$ — группа невырожденных линейных операторов на V. Заметим, что $\operatorname{Aut} V \subset \mathcal{S}_V$, и таким образом, представление — частный случай действия

(G, ρ, V). Пространство V называется *несущим пространством* линейного представления. Мы будем изучать конечномерные векторные пространства. Пусть $\dim V = n$, тогда n называется *размерностью* представления.

Определение. Пусть $U \subset V$ — подпространство. U называется *G-инвариантным*, если U инвариантно относительно всех операторов $\rho(g), g \in G$.

Такое свойство U позволяет рассмотреть ограничение нашего представления ρ на U, поскольку $\forall\, g \in G$ получаем $\rho(g)\Big|_U : U \to U$ — корректно определённый линейный оператор. Тогда $\rho\Big|_U$ называется подпредставлением. Очевидно, что любое представление имеет тривиальные G-инвариантные подпространства: нулевое и само пространство V.

Определение. Если у представления есть нетривиальные подпредставления, то оно называется *приводимым*. Если же все подпредставления тривиальны, то оно называется *неприводимым*.

Определение. Пусть даны два представления (G, ρ, V) и (G, τ, U). Естественно, что V и U рассматриваются над одним и тем же полем K. Линейное отображение $\varphi\colon V \to U$ называется *гомоморфизмом представлений* ρ и τ, если оно согласовано с действием группы: $\forall\, x \in V, \forall\, g \in G$ имеем $\varphi\left(\rho(g)x\right) = \tau(g)\varphi(x)$. На языке операторов: $\forall\, g \in G$ имеем $\varphi \circ \rho(g) = \tau(g) \circ \varphi$. Если φ — изоморфизм линейных пространств V и U, то φ называют *изоморфизмом* представлений. Гомоморфизм представлений обычно обозначается так: $\varphi\colon \rho \to \tau$.

Со всяким линейным представлением группы связано её *матричное представление*, если зафиксировать в V базис. Тогда получаем сквозной гомоморфизм $G \xrightarrow{\rho} \operatorname{Aut} V \to \mathbf{GL}_n(K)$. Недостатком матричных представлений является их зависимость от базиса. Из курса линейной алгебры следует, что если зафиксировать два базиса, то матрицы одного и того же линейного оператора $\rho(g)$ будут связаны равенством $B_{\rho(g)} = CA_{\rho(g)}C^{-1}$, где C — матрица перехода от одного базиса к другому. Такие матричные представления называются эквивалентными. Заметим, что очень похожее по виду соотношение получается, если записать по-другому операторное равенство: $\forall\, g \in G$ имеем $\tau(g) = \varphi \circ \rho(g)\varphi^{-1}$.

Определение. Пусть представление (G, ρ, V) имеет два G-инвариантных подпространства U и W, причём $V = U \oplus W$. Тогда имеет смысл разложить наше представление в *прямую сумму*: $\rho = \rho_U \oplus \rho_W$. Представление, разлагающееся в прямую сумму неприводимых, называется *вполне приводимым*.

На языке матриц существование G-инвариантного подпространства U означает, что матрицы $\rho(g)$ имеют вид $\left(\begin{array}{c|c} * & * \\ \hline 0 & * \end{array}\right)$, причём первый блок матрицы соответствует подпространству U. Аналогично, если $\rho = \rho_U \oplus \rho_W$, то матрицы $\rho(g)$ имеют вид $\left(\begin{array}{c|c} * & 0 \\ \hline 0 & * \end{array}\right)$.

Определение. Представление называется *точным*, если $\operatorname{Ker}\rho = \{e\}$, т. е. ρ инъективно. Тогда $G \hookrightarrow \operatorname{Aut} V$.

Теорема 5.1. *Пусть $\varphi\colon \rho \to \tau$ — гомоморфизм представлений с несущими пространствами V и U соответственно. Тогда $\operatorname{Im}\varphi$ и $\operatorname{Ker}\varphi$ являются G-инвариантными подпространствами.*

□ Пусть $x \in V$, тогда $\varphi(x) \in \operatorname{Im}\varphi$. Из согласованности действий следует, что $\tau(g)\varphi(x) = \varphi\left(\rho(g)x\right) \in \operatorname{Im}\varphi$, а это означает, что $\operatorname{Im}\varphi$ является G-инвариантным. Пусть теперь $x \in \operatorname{Ker}\varphi$, то есть $\varphi(x) = 0$. Тогда $\varphi\left(\rho(g)x\right) = = \tau(g)\varphi(x) = \tau(g)0 = 0$, значит, $\rho(g)x \in \operatorname{Ker}\varphi$, а это означает, что $\operatorname{Ker}\varphi$ является G-инвариантным. ■

Теорема 5.2 (Лемма Шура). *Пусть φ — гомоморфизм неприводимых представлений с несущими пространствами V и U. Тогда либо $\varphi = 0$, либо φ есть изоморфизм линейных пространств V и U.*

□ Пусть $\varphi \neq 0$. Тогда $\operatorname{Im}\varphi$ есть ненулевое G-инвариантное подпространство. Но в U нет нетривиальных G-инвариантных подпространств. Значит, $\operatorname{Im}\varphi = U$. Иначе говоря, φ сюръективно. Далее, поскольку $\operatorname{Ker}\varphi \neq V$, получаем, что $\operatorname{Ker}\varphi = 0$, ибо в V тоже нет нетривиальных G-инвариантных подпространств. Следовательно, φ инъективно. Но тогда φ биективно, а это и означает, что φ — изоморфизм линейных пространств V и U. ■

5.2. Теорема Машке

Определение. Пусть $\Phi\colon V \to V$ — линейный оператор. Если $\Phi^2 = \Phi$, то такой оператор называется *проектором*.

Теорема 5.3. *Пусть Φ — проектор. Тогда $V = \operatorname{Im}\Phi \oplus \operatorname{Ker}\Phi$.*

□ Пусть $x \in V$. Рассмотрим тождество $x = \underbrace{\Phi x}_{\in \operatorname{Im}} + \underbrace{x - \Phi x}_{\in \operatorname{Ker}}$. В самом деле, поскольку Φ — проектор, имеем $\Phi(x - \Phi x) = \Phi x - \Phi^2 x = \Phi x - \Phi x = 0$. Значит, действительно $x - \Phi x \in \operatorname{Ker}\Phi$. Однако $\operatorname{Ker}\Phi \cap \operatorname{Im}\Phi = 0$. Но это и означает, что $V = \operatorname{Im}\Phi \oplus \operatorname{Ker}\Phi$. ■

Говорят, что Φ *проектирует* $\operatorname{Im}\Phi$ *параллельно* $\operatorname{Ker}\Phi$.

Теорема 5.4. *Пусть G — конечная группа, а K — поле нулевой характеристики или $\operatorname{char} K \nmid |G|$. Тогда всякое подпредставление выделяется прямым слагаемым.*

□ Рассмотрим произвольное подпредставление $(G, \rho_U, U) \subset (G, \rho, V)$. Из общей теории линейной алгебры следует, что всегда можно выбрать $W \subset V$ так, чтобы $V = U \oplus W$. В нашем случае U было и остаётся G-инвариантным, а вот W — не обязательно. Покажем, что его можно «подправить» таким образом, чтобы ρ_U выделилось в качестве прямого слагаемого.

Пусть $\Theta\colon V \to U$ задаёт проекцию на U, то есть $\Theta x = u + w \mapsto u$. Рассмотрим линейный оператор

$$\Phi = \frac{1}{|G|} \sum_{g \in G} \rho(g) \Theta \rho(g)^{-1}.$$

Покажем, что Φ согласован с действием G. В самом деле, пусть $h \in G$, а $x \in V$. Тогда

$$\rho(h)\Phi x = \frac{1}{|G|} \sum_{g \in G} \rho(h)\rho(g)\Theta\rho(g)^{-1}x = \frac{1}{|G|} \sum_{g \in G} \rho(h)\rho(g)\Theta\rho(g)^{-1}\rho(h)^{-1}\rho(h)x =$$

$$= \underbrace{\frac{1}{|G|} \sum_{g \in G} \rho(hg)\Theta\rho(hg)^{-1}}_{\Phi} \rho(h)x = \Phi\rho(h)x,$$

поскольку когда g бегает по g, то hg тоже бегает по всей G. Иначе говоря, $\Phi\colon \rho \to \rho$ — гомоморфизм представлений.

Покажем, что $\operatorname{Im}\Phi \subset U$. Действительно, возьмём $x \in V$, тогда

$$\Phi x = \frac{1}{|G|} \sum_{g \in G} \rho(g) \underbrace{\Theta\rho(g)^{-1}x}_{\in U} \in U$$

в силу того, что Θ — проекция на U, а $\rho(g)$ вектора из U переводит в вектора из U, поскольку U есть G-инвариантное подпространство.

Наконец, заметим, что если $u \in U$, то $\Phi u = u$. Действительно, $\Phi u = \frac{1}{|G|} \sum\limits_{g \in G} \rho(g)\Theta\rho(g)^{-1}u = \{$ в силу G-инвариантности U имеем $\rho(g)^{-1}u \in U$, а потому $\Theta\rho(g)^{-1}u = \rho(g)^{-1}u$, следовательно $\} = \frac{1}{|G|} \sum\limits_{g \in G} \rho(g)\rho(g)^{-1}u =$ $= \frac{|G|}{|G|}u = u$.

Заметим, что наша конструкция работает благодаря тому, что по условию теоремы в поле K число $|G| \neq 0$. Мы доказали, что Φ является проектором, а потому $V = \operatorname{Im}\Phi \oplus \operatorname{Ker}\Phi$. Но, как мы знаем, $\operatorname{Im}\Phi$ и $\operatorname{Ker}\Phi$ являются G-инвариантными подпространствами. ■

Теорема 5.5 (Машке). *Пусть $|G| < \infty$. Если $\operatorname{char} K = 0$ или $\operatorname{char} K \nmid |G|$, то любое её представление вполне приводимо.*

□ Рассмотрим произвольное представление. Если оно неприводимо, то доказывать нечего. Если оно приводимо, то оно разлагается в прямую сумму подпредставлений: $(G, \rho, V) = (G, \rho_U, U) \oplus (G, \rho_W, W)$. Если они приводимы, то их можно разлагать дальше. Поскольку $\dim U, \dim W < \dim V$, процесс разложения когда-то остановится. ■

5.3. Линейные представления абелевых групп

Пусть K — алгебраически замкнутое поле.

Теорема 5.6. *Пусть $\Phi = \{\varphi_i\}$ — множество попарно коммутирующих линейных операторов на $V(K)$, причём $\dim V < \infty$. Тогда в V существует общий собственный вектор для всех этих операторов.*

□ Будем вести индукцию по $n = \dim V$. При $n = 1$ доказывать нечего. Пусть теперь $n > 1$, и наше утверждение верно для пространств меньшей размерности. Если все φ_i являются гомотетиями, то доказывать нечего, ибо любой вектор $x \neq 0$ будет искомым. Если же это не так, то $\exists\, \varphi \in \Phi$, не являющийся гомотетией. Поскольку K алгебраически замкнуто, у φ есть собственные векторы. Пусть λ — одно из собственных значений φ, а V_λ — подпространство, отвечающее этому собственному значению. Тогда $V_\lambda \neq V$ в силу негомотетичности оператора φ и $\dim V_\lambda < n$.

Мы знаем, что $V_\lambda = \operatorname{Ker}(\varphi - \lambda\mathcal{E})$. Докажем, что V_λ инвариантно относительно всех операторов из Φ. В самом деле, пусть $x \in V_\lambda \Leftrightarrow (\varphi - \lambda\mathcal{E})x = 0$. Пусть $\psi \in \Phi$. Заметим, что $\lambda\mathcal{E}$ коммутирует с любым оператором. Тогда $(\varphi - \lambda\mathcal{E})\psi x = \psi(\varphi - \lambda\mathcal{E})x = \psi 0 = 0$, откуда $\psi x \in V_\lambda$. Тогда по предположению индукции, $\exists\, x \in V_\lambda$ — собственный для всех операторов из Φ, и вектор найден. ■

Теорема 5.7. *Всякое неприводимое представление абелевой группы над алгебраически замкнутым полем одномерно.*

□ Поскольку G — абелева, получаем, что операторы из $\operatorname{Im}\rho$ попарно коммутируют. По предыдущей теореме, $\exists\, x \in V$, собственный для операторов из $\operatorname{Im}\rho$. Тогда $U = \langle x\rangle$, очевидно, является G-инвариантным. Но ρ неприводимо, а потому $U = V$, то есть $\dim V = 1$. ■

Следствие 5.1. *В условиях теоремы Машке любое представление абелевой группы над алгебраически замкнутым полем разлагается в прямую сумму одномерных представлений.*

Зафиксируем базис V. Одномерные представления представляют собой гомоморфизмы вида $\rho\colon G \to K^*$.

Лемма 5.8. *Пусть $G = G_1 \times \ldots \times G_m$ и L — абелевы группы. Пусть $\varphi_i\colon G_i \to L$ — гомоморфизмы прямых множителей. Тогда отображение $\varphi\colon G \to L$, определённое по правилу $\varphi\colon g = g_1 \cdot \ldots \cdot g_m \mapsto \varphi_1(g_1)\cdot\ldots\cdot\varphi_m(g_m)$ — гомоморфизм, и наоборот, если задан гомоморфизм $\varphi\colon G \to L$, то он индуцирует φ_i.*

□ Имеем $\varphi(gg') = \varphi_1(g_1g_1')\cdot\ldots\cdot\varphi_m(g_mg_m') = \{\ L \text{ абелева }\} = \big(\varphi_1(g_1)\cdot\ldots\cdot\varphi_m(g_m)\big)\cdot\big(\varphi_1(g_1')\cdot\ldots\cdot\varphi_m(g_m')\big) = \varphi(g)\varphi(g')$. Обратно, пусть $\varphi\colon G \to L$ — гомоморфизм, а $\varphi_i = \varphi\Big|_{G_i}$. Тогда из свойств гомоморфизма и свойств ограничений следует, что $\varphi(g) = \varphi(g_1)\cdot\ldots\cdot\varphi(g_m) = \varphi_1(g_1)\cdot\ldots\cdot\varphi_m(g_m)$. ■

Рассмотрим все неприводимые представления G в $\mathbb{C}^*$, где G — КПАГ. Как мы знаем, наша группа разлагается в прямое произведение (нам будет удобна мультипликативная терминология): $G = \langle x_1\rangle_\infty \times \ldots \times \langle x_r\rangle_\infty \times \ldots \times \langle a_1\rangle_{n_1} \times \ldots \times \langle a_s\rangle_{n_s}$. В данном случае неважно, являются ли конечные прямые множители примарными или нет. Нам необходимо изучить гомоморфизмы вида $\varphi\colon G \to \mathbb{C}^*$. По лемме, необходимо изучить ограничения φ на каждое из слагаемых. Поэтому можно считать, что теперь группа G состоит всего из одного прямого множителя. Возможны два случая.

1° Пусть G — САГ ранга 1, т. е. $G = \langle x\rangle_\infty$. Поскольку φ — гомоморфизм, достаточно задать образ порождающей: пусть $\varphi(x) = c \in \mathbb{C}^*$. Тогда $\varphi(x^k) = \varphi(x)^k = c^k$, т. е. $\varphi\colon x^m \mapsto c^m$, и других возможностей нет.

2° Пусть $G = \langle a\rangle_n \cong U_n$. Мы знаем, что φ определяется образом одного порождающего элемента. Пусть $\varphi(a) = \varepsilon \in \mathbb{C}^*$, тогда $\varphi(a^m) = \varepsilon^m$. Имеем $\varphi(a^n) = \varphi(e) = 1$, откуда $\varepsilon^n = 1$. Таким образом, ε должен быть некоторым корнем n-ой степени из 1, т. е. $\varepsilon \in U_n$. Обратно, если $\varepsilon \in U_n$, то отображение, заданное по правилу $\varphi\colon a \mapsto \varepsilon$, продолжается до гомоморфизма по правилу $a^m \mapsto \varepsilon^m$. Здесь, конечно, надо проверить корректность данного отображения: если $a^k = a^l$, то $\varphi(a^k) \overset{?}{=} \varphi(a^l)$. Но мы не первый раз сталкиваемся с такого рода гомоморфизмами: подобную проверку мы уже проводили, когда доказывали изоморфизм $\langle a\rangle_n \cong U_n$ в первой главе.

Итак, если $G = \langle x_1\rangle_\infty \times \ldots \times \langle x_r\rangle_\infty \times \ldots \times \langle a_1\rangle_{n_1} \times \ldots \times \langle a_s\rangle_{n_s}$. Тогда гомоморфизмы $\varphi\colon G \to \mathbb{C}^*$ определяются по правилу $\varphi\colon g = x_1^{k_1}\cdot\ldots\cdot x_r^{k_r}\cdot a_1^{l_1}\cdot\ldots\cdot a_s^{l_s} \mapsto c_1^{k_1}\cdot\ldots\cdot c_r^{k_r}\cdot\varepsilon_1^{l_1}\cdot\ldots\cdot\varepsilon_s^{l_s}$, где $c_i \in \mathbb{C}^*$, а $\varepsilon_i \in U_{n_i}$, и других нет.

5.4. Регулярные представления групп

Определение. Пусть K — поле, а $|G| = n$. Приступим к изготовлению групповой алгебры KG. Пусть $G = \{g_1, \ldots, g_n\}$, тогда $KG := \left\{\sum_{i=1}^n \alpha_i g_i\right\}$, где $\alpha_i \in K$. Определим сложение и умножение на скаляры: пусть $x = \sum\alpha_i g_i, y = \sum\beta_i g_i, \lambda \in K$, тогда $x + y := \sum(\alpha_i + \beta_i)g_i$ и $\lambda x := \sum(\lambda\alpha_i)g_i$. Можно отождествить $1\cdot g_i \leftrightarrow g_i$, и тогда $G \hookrightarrow KG$. Из определения следует, что базисом в KG будут элементы группы, отсюда $\dim KG = n$. Можно ввести умножение элементов в KG: его достаточно задать на базисных векторах, но их мы умеем перемножать, поскольку это просто элементы группы G. Тогда это будет ассоциативная алгебра с единицей над K. Построенное пространство KG называется *групповой алгеброй* над K.

Определение. Рассмотрим представление (G, Λ, KG), называемое *регулярным*. Пусть $g \in G$, Определим линейные операторы $\Lambda\colon KG \to KG$ по правилу $\Lambda(g) = L_g$, т. е. это левый сдвиг на элемент g. Таким образом, $\Lambda(g)$ будет как-то переставлять базисные вектора. Следовательно, он невырожден, поскольку базис переходит в базис.

Рассмотрим регулярное представление (G, Λ, KG) и другое представление $\big(G, \rho, V(K)\big)$. Фиксируем $x \in V$. Рассмотрим $\varphi_x\colon KG \to V$, действующее по правилу $\varphi_x\colon \sum\alpha_i g_i \mapsto \sum\alpha_i\rho(g_i)x$. Несложно показать, что φ_x является линейным отображением $KG \to V$. Покажем, что φ_x задаёт гомоморфизм представлений $\Lambda \to \rho$. В самом деле, проверим согласованность с действием: $\varphi_x\big(\Lambda(g)\sum\alpha_i g_i\big) = \varphi_x\big(\sum\alpha_i gg_i\big) = \sum\alpha_i\rho(gg_i)x = \rho(g)\big(\sum\alpha_i\rho(g_i)x\big) = \rho(g)\varphi_x\big(\sum\alpha_i g_i\big)$, и таким образом, операция действительно согласована. Далее, имеем $\varphi_x(e) = \rho(e)x = \mathrm{id}\, x = x$. Таким образом,

Покажем, что никаких других гомоморфизмов $\Lambda \to \rho$ не существует. Именно, если $\varphi\colon \Lambda \to \rho$ — гомоморфизм представлений, то φ совпадает с некоторым φ_x. В самом деле, пусть $x := \varphi(e)$. Тогда для базисных векторов имеем $\varphi(g) = \varphi(ge) = \varphi\big(\Lambda(g)e\big) = \rho(g)\varphi(e) = \rho(g)x = \varphi_x(g)$.

Теорема 5.9 (Универсальное свойство регулярного представления). *В условиях теоремы Машке всякое неприводимое представление G изоморфно некоторому подпредставлению регулярного представления.*

□ Рассмотрим регулярное представление (G, Λ, KG). По теореме Машке оно разложимо в прямую сумму

неприводимых представлений: $\Lambda = \bigoplus\limits_{i=1}^{m} \rho_i$. Тогда $KG = \bigoplus\limits_{i=1}^{m} V_i$, где V_i являются G-инвариантными подпространствами. Рассмотрим произвольное неприводимое представление $(G, \rho, V(K))$. Пусть $x \in V$ — ненулевой вектор. Рассмотрим $\varphi_x \colon \Lambda \to \rho$, а это отображение, как мы знаем, есть гомоморфизм представлений. Оно ненулевое, поскольку $\varphi_x(e) = x$. Имеем $\operatorname{Im}\varphi_x \neq 0$. Но $\operatorname{Im}\varphi_x$ есть G-инвариантное подпространство. По лемме Шура получаем $\operatorname{Im}\varphi_x = V$. Рассмотрим ограничение $\varphi_x\Big|_{V_i} : \rho_i \to \rho$. По лемме Шура получаем, что это либо нулевое отображение, либо изоморфизм. Но поскольку φ_x ненулевое, значит, $\exists\, i \colon \rho_i \cong \rho$. В самом деле, в силу неприводимости ρ, оно не может быть изоморфно прямой сумме нескольких ρ_i, но кому-то из них — обязательно. ■

Следствие 5.2. *В условиях теоремы Машке группа обладает конечным числом различных неприводимых представлений.*

□ Любое неприводимое представление оказалось изоморфно некоторому подпредставлению регулярного представления, а их конечное число. ■

6. Замечания и приложения большой теории

6.1. Лирическое отступление о цикличности конечной подгруппы K^*

Определение. *Экспонента* группы G — число $d := \min\big\{k \in \mathbb{N} \colon \forall\, x \in G\, x^k = e\big\}$. Обозначение: $\exp G$.

Рассмотрим группу G и её примарное разложение. Пусть $|G| = n$. Группа будет циклической тогда и только тогда, когда в ней есть элемент порядка n. Пусть $G = \langle a_1\rangle_{n_1} \times \ldots \times \langle a_s\rangle_{n_s}$. Тогда $n = n_1 \cdot \ldots \cdot n_s$. Далее, для $\forall\, x = (x_1, \ldots, x_s)$ имеем $O(x_i) \,\big|\, n_i$. Ясно, что элемент $a = (a_1, \ldots, a_s)$ имеет наибольший порядок в группе, поскольку $O(a_i) = n_i$. Очевидно, что $O(a) = \big[n_1, \ldots, n_s\big]$. Значит, G будет циклической группой $\Leftrightarrow$ числа $n_1, \ldots, n_s$ взаимно просты, поскольку тогда их наименьшее общее кратное совпадёт с их произведением, то есть с n. Отсюда следует, что группа циклическая $\Leftrightarrow \exp G = |G|$.

Теорема 6.1. *Конечная подгруппа $G \subset K^*$ является циклической.*

□ Пусть $d = \exp G$. Имеем $x^d = 1\, \forall\, x \in G$ по определению экспоненты. Поскольку уравнение $x^d - 1 = 0$ имеет не более d корней, получаем, что $|G| \leqslant d$. Но это означает, что $|G| = d$, поскольку случай $|G| < d$ невозможен. А это и означает цикличность G. ■

6.2. Разрешимость и неразрешимость групп

1° Подгруппа разрешимой группы разрешима, поскольку если $H \subset G$, то $H^{(i)} \subset G^{(i)}$.

2° Пусть $H \lhd G$ разрешима и $\overline{G} = {}^{G}\!/_{H}$ разрешима. Тогда G разрешима. В самом деле, рассмотрим естественный эпиморфизм $\pi \colon G \to \overline{G}$. Имеем $\overline{G}^{(m)} = \{\overline{e}\}$, а поскольку коммутант при гомоморфизме лежит в коммутанте образа, получаем $G^{(m)} \subset H$. Имеем $H^{(n)} = \{e\}$. Поэтому $\big(G^{(m)}\big)^{(n)} \subset H^{(n)} = \{e\}$, откуда $G^{(m+n)} = \{e\}$.

3° Пусть $H \lhd G$. Тогда $\overline{G} = {}^{G}\!/_{H}$ абелева $\Leftrightarrow G' \subset H$. Действительно, $\overline{G}$ абелева $\Leftrightarrow [\overline{a}, \overline{b}] = \overline{e} \Leftrightarrow [a, b] \in H \Leftrightarrow$ $\Leftrightarrow G' \subset H$.

Теорема 6.2. *Группа верхнетреугольных матриц $\mathbf{UT}_n(K) \subset \mathbf{GL}_n(K)$ разрешима.*

□ Обозначим нашу группу через G_n. Рассмотрим $\varphi \colon G_n \to \mathbf{GL}_n$, определённый по правилу

$$\varphi \colon \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \mapsto \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

То, что это гомоморфизм, очевидно, поскольку диагональный элемент произведения верхнетреугольных матриц есть произведение соответствующих диагональных элементов. Не менее очевидно, что $\operatorname{Ker}\varphi$ есть подгруппа унитреугольных матриц (это верхнетреугольные матрицы с единицами на главной диагонали), обозначим её H_n. Тогда $H_n \lhd G_n$. Более того, поскольку $\operatorname{Im}\varphi$ — это просто диагональные матрицы, по теореме о гомоморфизме получаем, что ${}^{G_n}\!/_{H_n}$ абелева и потому разрешима. Осталось доказать, что H_n разрешима, тогда в силу **2°** группа G_n разрешима.

Проведём доказательство разрешимости H_n по индукции: для $n = 1$ доказывать нечего. Пусть $n > 1$, и предположение индукции верно для H_k при $k < n$. Рассмотрим $A = \left(\begin{array}{c|c} A' & u \\ \hline 0 & 1 \end{array}\right)$, $B = \left(\begin{array}{c|c} B' & v \\ \hline 0 & 1 \end{array}\right)$, где $A', B' \in H_{n-1}$, а u, v — столбцы высоты $n-1$. Заметим, что $AB = \left(\begin{array}{c|c} A'B' & A'v + u \\ \hline 0 & 1 \end{array}\right)$. Рассмотрим отображение $\varphi \colon H_n \to H_{n-1}$, определённое по правилу $\varphi \colon A \mapsto A'$. Очевидно, что φ — гомоморфизм с ядром

$K_n := \left\{ A_u := \left(\begin{array}{c|c} E_{n-1} & u \\ \hline 0 & 1 \end{array} \right) \right\}$, где E_{n-1} — единичная матрица, а u — столбец. Легко видеть, что K_n абелева, поскольку $A_u \cdot A_v = A_{u+v} = A_{v+u} = A_v \cdot A_u$, ибо сложение столбцов коммутативно. По теореме о гомоморфизме имеем $H_{n-1} = {}^{H_n}\!/_{K_n}$. Тогда, со ссылкой на **2°** получается, что H_n разрешима, ибо H_{n-1} разрешима по предположению индукции. ■

Лемма 6.3. *Пусть $N \lhd \mathcal{S}_n$. Пусть $\sigma \in N$. Тогда N содержит все подстановки того же циклического строения, что и σ.*

□ Разложим σ в независимые циклы. Без ограничения общности можно считать, что $\sigma = (i_1, \ldots, i_k)$, поскольку для нескольких циклов рассуждения аналогичны. В силу того, что $N \lhd \mathcal{S}_n$, эта подгруппа должна выдерживать сопряжения. Покажем, что $\forall \tau \in \mathcal{S}_n$ имеем $\tau\sigma\tau^{-1} = \big(\tau(i_1), \ldots, \tau(i_k)\big)$. Пусть

$$\tau = \begin{pmatrix} 1 & 2 & \ldots & s & \ldots & n \\ j_1 & j_2 & \ldots & j_s & \ldots & j_n \end{pmatrix}.$$

Посмотрим, как подстановка $\tau\sigma\tau^{-1}$ действует на элемент j_s. Если $s \in (i_1, \ldots, i_k)$, то $\tau\sigma\tau^{-1}(j_s) = \tau\sigma(s) = j_{\sigma(s)}$. Если же $s \notin (i_1, \ldots, i_k)$, то $\tau\sigma\tau^{-1}(j_s) = j_s$. Но это и требовалось доказать, поскольку τ пробегает всю $\mathcal{S}_n$. ■

Лемма 6.4. *Все тройные циклы порождают группу $\mathcal{A}_n$.*

□ Поскольку любая подстановка есть произведение транспозиций, а чётная подстановка содержит чётное число транспозиций, нам достаточно доказать, что имея все тройные циклы, можно получить любую пару транспозиций. Пусть нам надо получить пару $(ac)(bd)$. Имеем $(abc)(abd) = (ac)(bd)$. ■

Лемма 6.5. *Если $N \lhd \mathcal{A}_n$ содержит хотя бы один тройной цикл, то $N = \mathcal{A}_n$.*

□ По лемме 6.3, N содержит все тройные циклы[1]. Применяем лемму 6.4 и получаем требуемое. ■

Теорема 6.6. *Группа $\mathcal{A}_n$ при $n \geqslant 5$ простая.*

□ Пусть $N \lhd \mathcal{A}_n$ и $N \neq \{e\}$. Докажем, что в N есть тройной цикл. Тогда утверждение теоремы будет следовать из лемм. Пусть $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_s \in N$ — разложение подстановки в независимые циклы. Рассмотрим циклическую группу $\langle\sigma\rangle$. Она содержит циклическую группу простого порядка, значит, можно считать, что σ имеет простой порядок p, и число p — минимальное. Тогда без ограничения общности можно считать, что первый цикл в σ имеет длину p, т. е. $\sigma_1 = (1, \ldots, p)$. Поскольку все сопряженные с σ элементы лежат в N, то у нас есть перестановка $\tau = \sigma_1\sigma_2^{-1}\sigma_3^{-1} \ldots \sigma_s^{-1}$. Тогда $\sigma\tau = \sigma_1^2$, т. е. тоже цикл длины p. Для p есть три возможности: $p = 2, p = 3, p \geqslant 5$. Если $p = 3$, то $\sigma\tau$ — тройной цикл и всё доказано.

Рассмотрим случай $p \geqslant 5$. Мы уже знаем, что в N есть все циклы длины p, тогда возьмём перестановки $\pi_1 := (1, 2, 3, 4, 5, \ldots, p)$ и $\pi_2 := (1, 3, 4, 2, 5, \ldots, p)$. Легко видеть, что перестановка $\pi_1^{-1}\pi_2$ оставляет на месте число p, а значит, в ней есть цикл длины меньше p. Противоречие.

Теперь рассмотрим случай $p = 2$. Тогда σ имеет вид $(12)(34)\rho$, где ρ — произведение некоторых других транспозиций. Рассмотрим сопряжённую перестановку $\tau := (13)(24)\rho$. Поскольку $\rho^2 = e$, то имеем $\sigma\tau = (14)(23) \in N$. Значит, в N имеются все пары транспозиций. Тогда рассмотрим перестановку $\pi_1 := (12)(34)$ и $\pi_2 := (12)(45)$. Имеем $\pi_1\pi_2 = (345)$, т. е. тройной цикл. Значит, $N = \mathcal{A}_n$. ■

6.3. Явный вид функции Эйлера и малая теорема Ферма

Определение. Пусть $n \in \mathbb{N}$, тогда $\varphi(n) := |\{m \in \mathbb{N} \colon (m, n) = 1, m < n\}|$ — *функция Эйлера.*

Определение. Функция f называется *мультипликативной*, если для любых взаимно простых $m, n \in \mathbb{N}$ имеем $f(mn) = f(m)f(n)$.

Теорема 6.7. *Функция Эйлера φ мультипликативна.*

□ В самом деле, пусть $(m, n) = 1$. Рассмотрим $G = \langle a\rangle_m \times \ldots \times \langle b\rangle_n$. Мы знаем, что тогда $G = \langle c\rangle_{mn}$. Заметим, что число порождающих в G равно $\varphi(mn)$. Рассмотрим $d \in G$. Тогда $\exists!$ разложение вида $d = a^k \cdot b^l$. Заметим, что $O(d) = \big[O(a^k), O(b^l)\big] = mn \Leftrightarrow O(a^k) = m, O(b^l) = n \Leftrightarrow$ элемент d — порождающий. Поэтому количество порождающих есть $\varphi(m)\varphi(n)$: на каждую порождающую из $\langle a\rangle$ можно взять одну из порождающих $\langle b\rangle$. Но это и означает, что $\varphi(mn) = \varphi(m)\varphi(n)$. ■

Выведем формулу для φ: пусть $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ — каноническое разложение числа n на простые множители. Используя мультипликативность φ, получаем $\varphi(n) = \varphi\big(p_1^{k_1}\big) \cdot \ldots \cdot \varphi\big(p_s^{k_s}\big)$. Легко видеть, что все числа, не взаимно простые с p^k и меньшие его, суть числа $p, 2p, \ldots, \big(p^{k-1} - 1\big)p$, и всего их $p^{k-1} - 1$ штук. Существует $p^k - 1$ чисел,

[1] Устраните логический пробел в этом утверждении! Первая лемма применима к $\mathcal{S}_n$, а не к $\mathcal{A}_n$! Доказательство можно посмотреть в учебнике Э. Б. Винберга — *Прим. ред.*

меньших p^k. Поэтому $\varphi\big(p^k\big) = p^k - 1 - \big(p^{k-1} - 1\big) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$. Отсюда выводим формулу:

$$\varphi(n) = p_1^{k_1}\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot p_s^{k_s}\left(1 - \frac{1}{p_s}\right) = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right) = n\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right).$$

Теорема 6.8 (Малая теорема Ферма). *Пусть* $(m, n) = 1$. *Тогда* $m^{\varphi(n)} \equiv 1 \mod n$.

□ Рассмотрим кольцо $\mathbb{Z}_n$. Зададимся вопросом: когда элемент $[m] \in \mathbb{Z}_n$ обратим по умножению? Если $(m, n) \neq 1$, то $[m]$ является делителем нуля и потому не может быть обратим. Действительно, допустим, что $[m][k] = [0]$, причём $[m] \neq [0]$, $[k] \neq [0]$ и $[m]$ обратим, т. е. $\exists\,[m]^{-1}$: $[m]^{-1}[m] = [1]$. Тогда имеем $[0] = [m]^{-1}[0] = [m]^{-1}[m][k] = [m^{-1}m][k] = [1][k] = [k] \neq [0]$, противоречие. Если же $(m, n) = 1$, тогда по формуле «$fu + gv$» получаем $mu + nv = 1$, и производя редукцию по модулю n, получаем $[m][u] = [1]$, откуда $[u] = [m]^{-1}$. Обозначим через $\mathbb{Z}_n^*$ группу обратимых элементов в $\mathbb{Z}_n$ (проверка того, что это группа, предоставляется читателю). Тогда, поскольку $|\mathbb{Z}_n^*| = \varphi(n)$, по теореме Лагранжа $\forall\,[m] \in \mathbb{Z}_n^*$ получаем $[m]^{\varphi(n)} = [1]$, но это и означает, что $m^{\varphi(n)} \equiv 1 \mod n$. ■

6.4. Китайская теорема об остатках

Теорема 6.9 (Китайская теорема об остатках). *Пусть* $n_1, \ldots, n_s$ — *попарно взаимно простые числа,* $n_i \in \mathbb{N}$. *Пусть* $0 \leqslant r_i < n_i \in \mathbb{N}$. *Тогда* $\exists\, m \in \mathbb{N}$: $m \equiv r_i \mod n_i$.

□ Рассмотрим $G = \langle a \rangle_n$, где $n = n_1 \cdot \ldots \cdot n_s$. Пусть $a_i := a^{n_1 \cdot \ldots \cdot \widehat{n_i} \cdot \ldots \cdot n_s}$. Очевидно, $G = \langle a_1 \rangle_{n_1} \times \ldots \times \langle a_s \rangle_{n_s}$. Рассмотрим $b = a_1 \cdot \ldots \cdot a_s$. Имеем $O(b) = \big[O(a_1), \ldots, O(a_s)\big] = n_1 \cdot \ldots \cdot n_s = n$, откуда b — порождающий элемент G. Рассмотрим элемент $a_1^{r_1} \cdot \ldots \cdot a_s^{r_s}$. Он есть некоторая степень порождающей b. Поэтому $\exists\, m < n$, для которого $a_1^{r_1} \cdot \ldots \cdot a_s^{r_s} = b^m = a_1^m \cdot \ldots \cdot a_s^m$. Отсюда, по свойствам прямого произведения групп получаем $a_1^{m-r_1} \cdot \ldots \cdot a_s^{m-r_s} = e = e \cdot \ldots \cdot e$, и в силу единственности представления элемента в виде произведения элементов из прямых множителей, получаем $a_i^{m-r_i} = e$, а это означает, что $n_i \,\big|\, (m - r_i)$, т. е. $m \equiv r_i \mod n_i$. ■

6.5. Теорема Вильсона

Теорема 6.10 (Вильсона). *Пусть* $p \in \mathfrak{P}$, *тогда* $(p-2)! \equiv 1 \mod p$.

□ Рассмотрим $\mathcal{S}_p$. Поскольку $|\mathcal{S}_p| = p!$, все силовские p-подгруппы имеют порядок p и потому циклические и пересекаются только по id. Циклов длины p в $\mathcal{S}_p$ существует всего $(p-1)!$ штук, и каждая силовская p-подгруппа содержит по $p-1$ циклу. Тогда $\frac{(p-1)!}{p-1} = (p-2)! \equiv 1 \mod p$ по последней теореме Силова. ■

7. Return to Linear Representations

7.1. Пространство линейных отображений

Рассмотрим векторные пространства V и W над полем K. Рассмотрим $\mathrm{Lin}(V, W)$ — *пространство линейных отображений* из V в W. Оно наделено операциями $+$ и $\cdot$ на скаляры, т. е. естественной структурой линейного пространства. Пусть $\varphi, \psi \in \mathrm{Lin}(V, W)$. Тогда $(\varphi + \psi)(x) := \varphi x + \psi x$ и $(\lambda\varphi)(x) = \lambda\varphi(x)$. Очевидно, что если $\dim V = m$, а $\dim W = n$, то $\dim \mathrm{Lin}(V, W) = mn$, поскольку $\mathrm{Lin}(V, W) \cong \mathbf{M}(m \times n, K)$ при зафиксированных базисах V и W.

Пусть (G, ρ, V) и (G, τ, W) — представления. Пусть $\mathrm{Hom}(\rho, \tau)$ — множество гомоморфизмов представлений. Тогда $\mathrm{Hom}(\rho, \tau) \subset \mathrm{Lin}(V, W)$ — пока это всего лишь подмножество. Покажем, что это подпространство. Для этого достаточно доказать, что если $\varphi, \psi \in \mathrm{Hom}(\rho, \tau)$, то $(\varphi + \psi)$ и $\lambda\varphi$ тоже лежат в $\mathrm{Hom}(\rho, \tau)$. В самом деле, рассмотрим $(\varphi + \psi)\big(\rho(g)x\big) = \big\{$ по определению суммы операторов $\big\} = \varphi\big(\rho(g)x\big) + \psi\big(\rho(g)x\big) = \big\{$ в силу того, что φ и ψ согласованы с действием $\big\} = \tau(g)\varphi(x) + \tau(g)\psi(x) = \tau(g)\big(\varphi(x) + \psi(x)\big) = \tau(g)\big((\varphi + \psi)x\big)$, что и требовалось доказать. Аналогично доказывается свойство умножения на скаляр λ. Итак, $\mathrm{Hom}(\rho, \tau)$ — подпространство в $\mathrm{Lin}(V, W)$.

Пусть $\varphi\colon V \to W$. Пусть $V = V_1 \oplus \ldots \oplus V_m$. Тогда $\forall\, x \in V$ имеет место единственное представление $x = x_1 + \ldots + x_m$. Ввиду того, что $\varphi(x) = \varphi(x_1) + \ldots + \varphi(x_m)$, можно ограничить действия φ на каждое из слагаемых и ввести операторы $\varphi_i\colon V_i \to W$, действующие по правилу $\varphi_i(x) = \varphi\big|_{V_i}(x_i)$. Важно, что при этом можно расширить область действия каждого из φ_i на всё пространство V, получив m операторов $\widehat{\varphi}_i\colon V \to W$, и мысленно отождествить их с φ_i. Тогда получается, что $\varphi = \varphi_1 + \ldots + \varphi_m$. Тогда ясно, что $\mathrm{Lin}(V_1 \oplus \ldots \oplus \oplus V_m, W) \cong \mathrm{Lin}(V_1, W) \oplus \ldots \oplus \mathrm{Lin}(V_m, W)$. Однако не будем рассматривать всё Lin целиком, а ограничимся рассмотрением $\mathrm{Hom}(\rho, \tau) \cong \bigoplus_{i=1}^{m} \mathrm{Hom}(\rho_i, \tau)$.

7.2. Кратность неприводимого представления

Определение. Определим *кратность неприводимого представления*: пусть $\rho = \bigoplus\limits_{i=1}^{m} \rho_i^{r_i}$, где ρ_i — неприводимые представления. Тогда число r_i называется кратностью неприводимого представления ρ_i в ρ. Ясно, что необходима проверка корректности данного определения.

Теорема 7.1. *Пусть K алгебраически замкнуто, а ρ и τ — неприводимые представления G. Тогда*

$$\dim \operatorname{Hom}(\rho, \tau) = \begin{cases} 0, \rho \ncong \tau, \\ 1, \rho \cong \tau. \end{cases}$$

□ В самом деле, пусть $\rho \ncong \tau$. Тогда по лемме Шура получаем $\operatorname{Hom}(\rho, \tau) = \{0\}$, и потому $\dim \operatorname{Hom}(\rho, \tau) = 0$. Теперь рассмотрим случай $\rho \cong \tau$. Тогда их можно отождествить: теперь мы будем рассматривать $\operatorname{Hom}(\rho, \rho)$. Пусть $\varphi \in \operatorname{Hom}(\rho, \rho)$. Тогда, поскольку $\varphi\colon V \to V$ сохраняет действие группы, получаем $\varphi\big(\rho(g)x\big) = \rho(g)\varphi(x)$. В силу алгебраической замкнутости K, у φ есть собственный вектор с собственным значением λ. Покажем, что V_λ есть G-инвариантное подпространство. Действительно, $x \in V_\lambda \Leftrightarrow \varphi(x) = \lambda x$, тогда $\varphi\big(\rho(g)x\big) = \rho(g)\varphi(x) = \rho(g)(\lambda x) = \lambda\rho(g)x$. Таким образом, вектор $\rho(g)x$ является собственным вектором с собственным значением λ. Значит, V_λ действительно G-инвариантно. Но ρ неприводимо, а потому $V_\lambda = V$, ведь оно ненулевое. Значит, наш оператор есть просто гомотетия с коэффициентом λ, то есть $\varphi = \lambda\mathcal{E}$. Но пространство гомотетий, очевидно, одномерно. Поэтому $\dim \operatorname{Hom}(\rho, \rho) = 1$. ■

Следствие 7.1. *Кратность неприводимого представления для алгебраически замкнутых полей является инвариантом.*

□ Рассмотрим $\rho = \bigoplus\limits_{i=1}^{m} \rho_i^{r_i}$, причём ρ_i попарно неизоморфны. Рассмотрим

$$\operatorname{Hom}(\rho, \rho_k) \cong \operatorname{Hom}(\rho_k^{r_k}, \rho_k) \oplus \operatorname{Hom}\left(\bigoplus_{i \neq k} \rho_i^{r_i}, \rho_k\right) \cong \operatorname{Hom}(\rho_k, \rho_k)^{r_k} \oplus \left(\bigoplus_{i \neq k} \operatorname{Hom}(\rho_i, \rho_k)^{r_i}\right) \cong \operatorname{Hom}(\rho_k, \rho_k)^{r_k},$$

поскольку по доказанной выше теореме получаем, что последние слагаемые будут нулевыми. Отсюда получаем, вновь используя доказанную теорему: $\dim \operatorname{Hom}(\rho, \rho_k) = \dim \operatorname{Hom}(\rho_k, \rho_k)^{r_k} = r_k \cdot \dim \operatorname{Hom}(\rho_k, \rho_k) = r_k$. Следовательно, r_k есть размерность некоторого пространства, а она инвариантна. ■

Замечание. Несущие подпространства V_i определены однозначно, если $r_i = 1$.

7.3. Кратность неприводимых представлений в регулярном представлении

Рассмотрим регулярное представление (G, Λ, KG) и (G, ρ, V). Пусть $\varphi_x \in \operatorname{Hom}(\Lambda, \rho)$, причём $x \in V$ и $\varphi_x(e) = x$, а $\varphi_x(g) = \rho(g)x$. Из свойств линейных отображений выводим правило сложения гомоморфизмов $(\varphi_x + \varphi_y)(e) = \varphi_x(e) + \varphi_y(e) = x + y = \varphi_{x+y}(e)$, откуда $\varphi_{x+y} = \varphi_x + \varphi_y$; и умножения на скаляры: $\varphi_{\lambda x}(e) = \lambda x = (\lambda\varphi_x)(e)$, откуда $\varphi_{\lambda x} = \lambda\varphi_x$.

Рассмотрим отображение $\Phi\colon \operatorname{Hom}(\Lambda, \rho) \to V$, определённое по правилу $\Phi\colon \varphi_x \mapsto x$. Сюръективность очевидна. Проверим линейность: $\Phi(\varphi_x + \varphi_y) = \Phi(\varphi_{x+y}) = x + y = \Phi(\varphi_x) + \Phi(\varphi_y)$. Аналогично, $\Phi(\lambda\varphi_x) = \lambda\Phi(\varphi_x)$. Отсюда следует, что $\operatorname{Ker}\Phi = 0$, поскольку имеет место равенство $\varphi_x(e) = x$. Значит, Φ осуществляет изоморфизм линейных пространств. Следовательно, $\dim \operatorname{Hom}(\Lambda, \rho) = \dim \rho$.

Теорема 7.2. *Кратность неприводимого представления группы в её регулярном представлении совпадает с его размерностью.*

□ Как мы знаем, $\Lambda = \rho_i^{r_i} \oplus \ldots \oplus \rho_m^{r_m}$. Здесь ρ_i — неприводимые представления. Заметим, что $r_i = \dim \rho_i$. Действительно, возьмём некоторое представление (G, ρ_k, V_k). Используя рассуждения, аналогичные тем, что были в теореме об инвариантности кратности, получаем $\operatorname{Hom}(\Lambda, \rho_k) \cong \operatorname{Hom}(\rho_k, \rho_k)^{r_k}$, и потому $\dim \operatorname{Hom}(\Lambda, \rho_k) = \dim \rho_k = \dim V_k$. ■

Следствие 7.2. *В условиях теоремы Машке* $|G| = \sum\limits_{i=1}^{m} \big(\dim \rho_i\big)^2$.

□ Действительно, мы знаем, что $\dim \Lambda = |G|$, поскольку элементы группы образуют базис групповой алгебры. Далее, $|G| = \sum\limits_{i=1}^{m} r_i \dim \rho_i = \sum\limits_{i=1}^{m} \big(\dim \rho_i\big)^2$, поскольку $\dim \rho_i = r_i$. ■