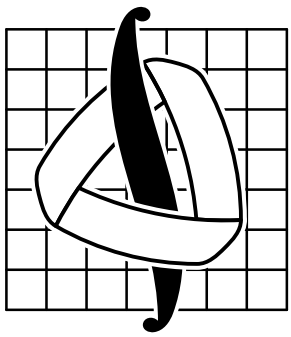
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
Механико-математический факультет



Курс лекций по высшей алгебре

Лектор — Евгений Соломонович Голод

II курс, 3 семестр, поток математиков

Москва, 2003 г.

Оглавление

Введение

Предисловие

Спасибо всем, кто принимал прямое/косвенное участие в создании этого документа! Прежде всего, хочется поблагодарить нескольких студентов МехМата: **Домбровскую А.** — за предоставление великолепного конспекта лекций; **Трушина Д.** и **Малыхина Ю.** — за ценные советы и доказательства некоторых теорем; **Краснобаева И.**, **Степанову М.**, **Короткова В.** — за обнаружение нескольких ошибок и опечаток.

Отдельная благодарность выносится **Юрию Кудряшову**, которого смело можно назвать главным редактором данного издания.

К сожалению, часть утверждений в этом курсе пришлось доказывать самостоятельно (лектору они казались совсем очевидными), так что вероятность наличия ошибок не равна нулю, но (по идее) должна стремиться к нему справа. Часть доказательств было заменено их аналогами, взятыми из других источников (в основном это учебник Э. Б. Винберга), поскольку они казались более простыми для понимания. Данная версия сего опуса уже далеко не первая, ибо благодаря стараниям вышеупомянутых лиц в тексте было исправлено огромное количество ошибок и опечаток. Остаётся надеяться, что он будет полезен будущим поколениям слушателей лекций автора курса.

В данной версии была сделано ещё несколько улучшений, на этот раз в основном с целью улучшить читаемость текста.

Список литературы

- Конспекты лекций по высшей алгебре. © МехМат, II курс, первый поток, 2003–2004 уч.г.
- Винберг Э. Б. *Курс алгебры.* — 3-е изд. — М.: Факториал-Пресс, 2002. — 544 с.
- Кострикин А. И. *Введение в алгебру: Основные структуры.* — 2-е изд. — М.: ФизМатЛит, 2001. — 272 с.
- B. L. van der Waerden. *Алгебра.* — М.: Наука, 1979. — 624 с.

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

1. Теория групп

1.1. Основные понятия и теоремы

1.1.1. Группы и подгруппы

Определение. Множество с ассоциативной бинарной операцией называется *полугруппой*. Полугруппа с нейтральным элементом называется *моноидом*. Моноид, в котором каждый элемент обратим, называется *группой*.

Определение. *Подгруппой* в группе G называется подмножество $H \subseteq G$, само являющееся группой.

Пусть $M_1, \ldots, M_s \subseteq G$. Тогда $M_1 \cdot \ldots \cdot M_s := \{x_1 x_2 \ldots x_s \mid x_i \in M_i\}$. Если M_i конечны, то $|M_1 \cdot \ldots \cdot M_s| \leqslant \leqslant |M_1| \ldots |M_s|$.

Определение. Пусть заданы группы $(G, \cdot)$ и $(G', *)$. *Гомоморфизмом* групп G и G' называется отображение $f\colon G \to G'$, такое, что $f(a \cdot b) = f(a) * f(b)$ для $\forall\, a, b \in G$. *Эпиморфизмом* называется сюръективный гомоморфизм.

При гомоморфизме единица переходит в единицу. В самом деле, $f(e) = f(e^2) = f(e)f(e)$, следовательно, $f(e)$ — единица группы G'.

Определение. *Циклической подгруппой* элемента $a \in G$ называется множество $\langle a \rangle := \{a^n\}, n \in \mathbb{Z}$.

Определение. *Порядком* элемента $a \in G$ называется число $O(a) := \min\{k > 0\colon a^k = e\}$.

1.1.2. Смежные классы

Определение. *Левым смежным классом* элемента g по подгруппе H группы G называется множество $gH = \{gh \mid h \in H\}$. Аналогично определяется правый смежный класс.

Рассмотрим отображение $f\colon H \to aH$, где элемент $a \in G$ — фиксирован, $f\colon h \mapsto ah$. Сюръективность f очевидна, докажем инъективность. Действительно, $f(h_1) = f(h_2) \Leftrightarrow ah_1 = ah_2 \Leftrightarrow h_1 = h_2$. Отсюда следует, что $|H| = |aH|$.

Утверждение 1.1. *Смежные классы либо не пересекаются, либо совпадают. $aH = bH \Leftrightarrow a^{-1}b \in H$.*

□ Действительно, пусть $aH \cap bH \neq \varnothing$, тогда найдутся $h_1, h_2 \in H$ такие, что $ah_1 = bh_2$, откуда $b = ah_1h_2^{-1}$. Значит, $bH = ah_1h_2^{-1}H = aH$, т. к. $h_1h_2^{-1} \in H$. Теперь докажем второе утверждение. Пусть $aH = bH$. Тогда $ah_1 = bh_2$, откуда $a^{-1}b = h_1h_2^{-1} \in H$. Обратно: $a^{-1}b \in H \Rightarrow a^{-1}b = h \Rightarrow bH = ahH = aH$. ■

Значит, имеется разбиение группы G на левые смежные классы: $G = \bigcup g_iH$. Есть биекция между левыми и правыми смежными классами: левому классу aH сопоставим правый класс Ha^{-1}. Это делает корректным

Определение. *Индексом* подгруппы H называется число $(G : H)$ смежных классов по этой подгруппе.

Из всего вышесказанного вытекает

Теорема 1.2 (Лагранжа). *Порядок группы является произведением порядка подгруппы на её индекс.*

Определение. Подгруппа $N \subseteq G$ называется *нормальной* в G, если $\forall\, g \in G$ имеем $gN = Ng$. Обозначение: $N \lhd G$.

Утверждение 1.3. *Следующие утверждения эквивалентны:*
1° *Подгруппа N нормальна в G;*
2° *$\forall\, g \in G$ имеем $gNg^{-1} = N$;*
3° *$\forall\, g \in G$ имеем $gNg^{-1} \subseteq N$;*
4° *Произведение множеств $(g_1N)(g_2N)$ — левый смежный класс g_1g_2N;*
5° *Существует гомоморфизм $f\colon G \to H$, такой что $N = \operatorname{Ker} f$.*

□ Эквивалентность пунктов **1°** и **2°** очевидна. Докажем, что из **3°** следует **2°**. Рассмотрим отображение $\varphi_g(x) = gxg^{-1}$, $x \in N$. Нам дано, что $\operatorname{Im}\varphi \subseteq N$. Проверим инъективность. Пусть $\varphi_g(x_1) = \varphi_g(x_2)$. Тогда $gx_1g^{-1} = gx_2g^{-1} \Rightarrow x_1 = x_2$. Проверим пункт **4°**. Если для $\forall\, g_1, g_2 \in G$ имеем равенство множеств $(g_1N)(g_2N) = = g_1g_2N$, то для $\forall\, n_1, n_2 \in N$ найдется элемент $n_3 \in N\colon g_1n_1g_2n_2 = g_1g_2n_3$. Сократим в равенстве на g_1, домножим справа на g_2^{-1} и слева на n_1^{-1}. Получим $g_2n_2g_2^{-1} = n_1^{-1}n_3 \in N$, то есть при сопряжении с любым элементом мы снова попадаем в N, а значит, верно свойство **3°**. Наоборот: если N нормальна, то $g_1Ng_2N = = g_1(Ng_2)N = g_1(g_2N)N = g_1g_2N$. Теперь докажем эквивалентность **1°** и **5°**. Если $N = \operatorname{Ker} f$, то

$$f(gNg^{-1}) = f(g)f(N)f(g^{-1}) = f(g)ef(g^{-1}) = f(gg^{-1}) = f(e) = e \in \operatorname{Ker} f = N, \tag{1}$$

то есть выполняется **3°**. Наоборот: возьмём отображение f, ставящее в соответствие элементу из G его смежный класс по подгруппе N. Очевидно, что это гомоморфизм, и его ядро есть N. ■

Определение. Отношение эквивалентности, сохраняющее операцию, называется *конгруэнцией*.

1.1.3. Факторгруппы

Введём на множестве смежных классов по подгруппе $H \lhd G$ естественную операцию $fH \cdot gH = fgH$. Таким образом, мы получили факторгруппу G/H. (свойства группы легко проверить).

Теорема 1.4 (О гомоморфизме). *Пусть $\varphi\colon G \to H$ — эпиморфизм, $\operatorname{Ker}\varphi =: K$, а $\pi\colon G \to G/K$ — канонический гомоморфизм. Тогда $G/K \cong H$. Более точно, $\exists!$ изоморфизм $\overline{\pi}\colon G/K \to H$, такой, что $\overline{\pi}\pi = \varphi$.*

□ Определим $\overline{\pi}$ следующим образом: $\overline{\pi}(gK) := \varphi(g)$. Это корректно, т. к. оно не зависит от выбора представителя смежного класса: если $g' = gk$, то $\varphi(g') = \varphi(g)\varphi(k) = \varphi(g)$. Операция сохраняется:

$$\overline{\pi}(g_1K \cdot g_2K) = \overline{\pi}(g_1g_2K) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \overline{\pi}(g_1K)\overline{\pi}(g_2K). \tag{2}$$

Значит, $\overline{\pi}$ — гомоморфизм. Докажем его инъективность:

$$\overline{\pi}(g_1K) = \overline{\pi}(g_2K) \Leftrightarrow \varphi(g_1) = \varphi(g_2) \Leftrightarrow e = \varphi(g_1^{-1})\varphi(g_2) = \varphi(g_1^{-1}g_2) \Leftrightarrow g_1^{-1}g_2 \in K, \tag{3}$$

а тогда по замечанию $g_1K = g_2K$. Итак, $\overline{\pi}$ — изоморфизм. Из условия $\overline{\pi}\pi = \varphi$ следует единственность $\overline{\pi}$, так как если $\varphi(g) = g'$, а $\pi(g) = [g]$, то $\overline{\pi}([g]) = \overline{\pi}\big(\pi(g)\big) = \varphi(g) = g'$, т. е. $\overline{\pi}$ определён однозначно. ■

1.1.4. Произведения подгрупп

Утверждение 1.5. *Пусть $K, L \subset G$. Множество KL является подгруппой $\Leftrightarrow KL = LK$.*

□ Докажем, что если $LK = KL$, то LK — подгруппа. Проверим, что $l_1k_1 \cdot l_2k_2 \in LK$. Поскольку наши множества совпадают, то $k_1l_2 = l'k' \in LK$. Тогда $l_1k_1l_2k_2 = l_1l'k'k_2 \in LK$. Обратный элемент: $(lk)^{-1} = k^{-1}l^{-1} \in KL = LK$. Таким образом, LK — подгруппа. В обратную сторону: пусть $H = KL$ — подгруппа. Мы имеем тождество $H^{-1} = H$. Тогда $(KL)^{-1} = \big\{(ab)^{-1} = b^{-1}a^{-1}\big\} = LK$, что и требовалось. ■

Замечание. Рассмотрим частный случай: $L \lhd G$. Тогда $KL = \bigcup\limits_{g\in K} gL \overset{\text{def}}{=} \bigcup\limits_{g\in K} Lg = LK$.

Теорема 1.6 (О соответствии). *Пусть есть эпиморфизм $\varphi\colon G \to F$, $\operatorname{Ker}\varphi =: H$. Рассмотрим все подгруппы в $A \subseteq G$, содержащие H (назовём их выделенными). Сопоставим каждой выделенной подгруппе A её образ $U := \varphi(A)$. Тогда такое сопоставление есть биекция между выделенными подгруппами и всеми подгруппами в F. При этом соответствующие друг другу группы одновременно нормальны и факторгруппы по ним изоморфны, т. е. $A \lhd G$, $H \subseteq A \Leftrightarrow U \lhd F$, и $G/A \cong F/U$.*

□ Докажем биективность соответствия. Сюръективность: рассмотрим полный прообраз A любой подгруппы $U \subseteq F$. Единица группы F лежит в U, а полный прообраз единицы и есть ядро. Значит, $\operatorname{Ker}\varphi \subseteq A$, т. е. A — выделенная подгруппа. Теперь докажем инъективность: пусть есть такие выделенные подгруппы A и B, что $\varphi(A) = \varphi(B)$. Тогда $\forall\, a \in A$ найдется $b \in B$: $\varphi(a) = \varphi(b)$. Следовательно, $\varphi(b)^{-1}\varphi(a) = e \Leftrightarrow \varphi(b^{-1}a) = e$, то есть $b^{-1}a \in \operatorname{Ker}\varphi$. Но $\operatorname{Ker}\varphi \subseteq B \Rightarrow a = bh \in B$, а значит $A \subseteq B$. Аналогично $B \subseteq A$. Значит, $A = B$ и первое утверждение доказано.

Докажем одновременную нормальность соответствующих подгрупп. Пусть A — выделенная подгруппа и $A \lhd G$. Тогда $\forall\, g \in G$ имеем $gAg^{-1} = A$. Применим φ к этому равенству: $\varphi(g)\varphi(A)\varphi(g^{-1}) = \varphi(A)$. Так как $\operatorname{Im}\varphi = F$, то если g пробегает по всей G, то $\varphi(g)$ пробегает по всей F. Тогда подгруппа $\varphi(A)$ нормальна в F. Остается показать изоморфность соответствующих факторгрупп. Обозначим $U := \varphi(A)$ и построим отображение $\pi\colon G \to$ $\to F/U$ по правилу $\pi(g) = \varphi(g)U$. Оно является гомоморфизмом, так как

$$\pi(g_1g_2) = \varphi(g_1g_2)U = \big(\varphi(g_1)\varphi(g_2)\big)U = \big(\varphi(g_1)U\big)\big(\varphi(g_2)U\big) = \pi(g_1)\pi(g_2). \tag{4}$$

Оно сюръективно, т. к. если g пробегает всю G, то $\varphi(g)U$ пробегает всю факторгруппу F/U. Теперь найдём его ядро: $g \in \operatorname{Ker}\pi \Leftrightarrow \pi(g) = \varphi(g)U = U \Leftrightarrow \varphi(g) \in U = \varphi(A) \Leftrightarrow g \in A$. Значит, $A = \operatorname{Ker}\pi$, а тогда по теореме о гомоморфизме $G/A \cong F/U$, что и требовалось. ■

Следствие 1.1. *Пусть $L \lhd K \lhd G$ и $L, K \lhd G$. Тогда $K/L \lhd G/L$ и $\frac{G/L}{K/L} \cong G/K$.*

□ Рассмотрим эпиморфизм $\varphi\colon G \to G/L$ и применим к нему утверждение теоремы. Очевидно, что $\operatorname{Ker}\varphi =$ $= L$. Имеем $\varphi(K) = K/L$, а значит, $\frac{G/L}{K/L} \cong G/K$. ■

Теорема 1.7 (Об изоморфизме). *Пусть $K \lhd G$, $H \subseteq G$, HK — подгруппа в G. Тогда $H \cap K \lhd H$ и $HK/K \cong H/(H \cap K)$.*

□ Если $K \lhd G$, то и подавно $K \lhd HK$, значит, можно рассмотреть факторгруппу HK/K. Рассмотрим канонический эпиморфизм $\pi\colon G \to G/K$. Через π_0 обозначим ограничение π на H. Тогда $h \overset{\pi_0}{\longmapsto} hK$. Теперь рассмотрим факторгруппу HK/K. Она состоит из смежных классов вида hkK, т. е. из множеств hK. Значит, $\operatorname{Im}\pi_0 = HK/K$. Тогда $\operatorname{Ker}\pi_0$ состоит из тех $h \in H$, для которых $\pi_0(h) = eK = K$. Но $hK = K \Leftrightarrow h \in K$, следовательно, имеем $h \in H \cap K$, т. е. $\operatorname{Ker}\pi_0 = H \cap K$. По теореме о гомоморфизме $HK/K \cong H/(H \cap K)$. ■

1.2. Автоморфизмы и классы сопряжённости

1.2.1. Преобразования. Автоморфизмы. Примеры.

$\mathbf{S}_M$ — группа биективных отображений множества M в себя. Рассмотрим группу движений плоскости, сохраняющих правильный n-угольник. В ней n вращений на угол $\frac{2\pi k}{n}$ и n осевых симметрий. Эта группа называется группой диэдра и обозначается $\mathbf{D}_n$. Очевидно, $|\mathbf{D}_n| = 2n$. Обозначим поворот на угол $\frac{2\pi}{n}$ через a и отражение через b, тогда любое преобразование имеет вид $a^k b$. Композиция отражений есть поворот, значит, $b'b = a^k \Rightarrow b' = a^k b$.

Определение. Изоморфизм группы на себя называется *автоморфизмом.*

Все автоморфизмы группы G образуют группу, обозначаемую $\operatorname{Aut} G$.

Утверждение 1.8. $\operatorname{Aut}\langle a\rangle_\infty = \{\mathrm{id}, a \mapsto a^{-1}\}$.

□ Пусть a — порождающий элемент, $\varphi(a) \neq a, a^{-1}$. Тогда $\varphi(a) = a^k,\ k \neq \pm 1$. Если a порождает всю группу, то и $\varphi(a)$ также порождает всю группу. Но $\langle\varphi(a)\rangle = \{(a^k)^m \mid m \in Z\} \neq G$, значит, φ — не автоморфизм. ■

Аналогично можно показать, что $\operatorname{Aut}\langle a\rangle_n = \{\varphi(a) = a^k \colon (n,k) = 1\}$. Таким образом, автоморфизмы циклической группы соответствуют обратимым элементам в $\mathbb{Z}/n\mathbb{Z}$, т. е. группа $\operatorname{Aut}\langle a\rangle_n$ изоморфна группе обратимых элементов в $\mathbb{Z}/n\mathbb{Z}$.

Определение. *Внутренним автоморфизмом* группы G называется отображение вида $\varphi_g(x) = gxg^{-1}$.

Определение корректно, так как

$$\varphi_g(x_1x_2) = gx_1x_2g^{-1} = (gxg^{-1})(gxg^{-1}) = \varphi_g(x_1)\varphi_g(x_2), \tag{5}$$

а биективность очевидна. Группа внутренних автоморфизмов обозначается $\operatorname{Int} G$. Покажем, что $\operatorname{Int} G \lhd \operatorname{Aut} G$. Рассмотрим внутренний автоморфизм $f(x) = gxg^{-1}$. При сопряжении произвольным автоморфизмом φ имеем

$$(\varphi^{-1} \circ f \circ \varphi)(x) = \varphi\big(f\big(\varphi^{-1}(x)\big)\big) = \varphi\big(g\varphi^{-1}(x)g^{-1}\big) = \varphi(g)x\varphi(g)^{-1}, \tag{6}$$

т. е. снова получился некоторый внутренний автоморфизм.

Определение. Группа *внешних автоморфизмов* есть факторгруппа $\operatorname{Out} G := \operatorname{Aut} G/\operatorname{Int} G$.

1.2.2. Центр группы

Определение. *Центром* группы G называется множество $Z(G) = \{g \colon gx = xg\,\forall\, x\}$.

Рассмотрим отображение $\pi \colon G \to \operatorname{Int} G$, определенное по правилу $g \mapsto \varphi_g$. Очевидно, что это гомоморфизм. Посмотрим на его ядро: $\pi(g) = \mathrm{id} \Leftrightarrow \forall\, x\ gxg^{-1} = x \Leftrightarrow \forall\, x\ gx = xg \Leftrightarrow g \in Z(G)$. Значит, $\operatorname{Ker}\pi = Z(G)$.

Утверждение 1.9. *Если группа G не абелева, то $G/Z(G)$ не может быть циклической.*

□ Допустим, $G/Z = \langle aZ\rangle$. Тогда $gZ = (aZ)^k = a^kZ$. Возьмём два элемента $g_1 = a^kz_1$ и $g_2 = a^lz_2$. Тогда имеем $g_1g_2 = a^kz_1a^lz_2 = a^lz_2a^kz_1 = g_2g_1$, так как z_1 и z_2 коммутируют со всеми. Противоречие. ■

1.2.3. Классы сопряженных элементов

Определение. Классом элементов, *сопряженных* с $x \in G$, называется множество $x^G := \{gxg^{-1} \mid g \in G\}$.

Подгруппа $H \subseteq G$ является нормальной, если она является объединением классов сопряженности (очевидно).

Пример 2.1. Наличие одинаковой жордановой формы у двух матриц является критерием их сопряженности.

Рассмотрим группу перестановок $\mathbf{S}_n$.

Утверждение 1.10. *Две перестановки сопряжены $\Leftrightarrow$ они имеют одинаковую цикловую структуру.*

□ Разложим перестановку $\pi \in \mathbf{S}_n$ на независимые циклы: $\pi = (i_1, \ldots, i_{k_1})(i_{k_1+1}, \ldots, i_{k_2}) \cdots (i_{k_s+1}, \ldots, i_n)$. Имеем

$$g\pi g^{-1} = \begin{pmatrix} i_1 i_2 \ldots i_{k_1} i_{k_1+1} \ldots i_n \\ j_1 j_2 \ldots j_{k_1} j_{k_1+1} \ldots j_n \end{pmatrix} \pi \begin{pmatrix} j_1 j_2 \ldots j_{k_1} j_{k_1+1} \cdots j_n \\ i_1 i_2 \ldots i_{k_1} i_{k_1+1} \ldots i_n \end{pmatrix} = (j_1, j_2, \ldots, j_{k_1})(j_{k_1+1}, \ldots, j_{k_2}) \cdots (j_{k_s+1}, \ldots, j_n).$$

Отсюда следует, что если перестановки сопряжены, то длины циклов одинаковые. Очевидно также то, что если у двух перестановок одинаковая цикловая структура, то они сопряжены — сопрягающую перестановку легко предъявить. ■

Теперь рассмотрим $\mathbf{A}_n \subset \mathbf{S}_n$ — знакопеременную группу чётных перестановок. Наличие одинаковой цикловой структуры необходимо и для $\mathbf{A}_n$. Чтобы найти достаточное условие, рассмотрим более общий случай. Вначале докажем вспомогательное

Утверждение 1.11. *Подгруппы индекса 2 всегда нормальны.*

□ $(G:H)=2 \Rightarrow$ имеется только 2 смежных класса: сама подгруппа $H=eH=He$ и некоторый левый класс gH, $g\notin H$. Тогда правый класс Hg совпадает либо с H, либо с gH. Но первая возможность отпадает, так как $g\notin H$, значит, $gH=Hg$, что и требовалось. ■

Утверждение 1.12. *Пусть $H\subset G$ и $(G:H)=2$. Тогда для $\forall x\in H$ возможны 2 случая:*
1° $x^H=x^G \Leftrightarrow \exists t\notin H\colon tx=xt$.
2° $x^G=x^H\cup x_1^H$, $x_1=txt^{-1}, t\notin H, |x^H|=|x_1^H| \Leftrightarrow \forall t\notin H\ tx\neq xt$.

□ Докажем **1°**. Пусть $x^G=x^H$. Из этого следует, что $\forall z\notin H\ \exists h\in H\colon zxz^{-1}=hxh^{-1}$, то есть $x=(z^{-1}h)x(h^{-1}z)$. Положим $t=z^{-1}h\notin H$, тогда $h^{-1}z=t^{-1}$, то есть $x=txt^{-1}\Leftrightarrow tx=xt$. Наоборот: пусть $\exists t\notin H\colon tx=xt$. Тогда $\forall z\notin H$ имеем $z=ht$. Значит,

$$zxz^{-1}=h\underbrace{txt^{-1}}_{x}h^{-1}=hxh^{-1}\in x^H, \tag{7}$$

то есть $x^G=x^H$.

Теперь докажем **2°**. Пусть $z,t\notin H, z=ht$. Тогда $zxz^{-1}=h\underbrace{txt^{-1}}_{x_1}h^{-1}=hx_1h^{-1}\in x_1^H$. Докажем, что $|x^H|=|x_1^H|$. Заметим, что $x\overset{\varphi}{\longmapsto} txt^{-1}$ — автоморфизм, а при нём классы сопряженных элементов переходят также в классы сопряженных. $\varphi(x)=x_1\Rightarrow\varphi(x^H)=x_1^H$. ■

Вернёмся к группе $\mathbf{A}_n$. Выясним, когда для чётной перестановки существует коммутирующая с ней нечётная. В следующем утверждении под циклами подразумеваются в том числе и циклы длины 1.

Утверждение 1.13. *Пусть $\pi\in\mathbf{A}_n$. Тогда:*
1° $\exists\tau\notin\mathbf{A}_n\colon \tau\pi=\pi\tau\Leftrightarrow\pi$ *содержит либо цикл чётной длины, либо 2 цикла равной нечётной длины.*
2° $\tau\pi\neq\pi\tau\,\forall\tau\notin\mathbf{A}_n\Leftrightarrow$ *все циклы в π разной нечётной длины.*

□ Разложим π на независимые циклы: $\pi=\sigma_1\sigma_2\sigma_3\cdots\sigma_s$. Пункт **1°**. Пусть (первый случай) σ_1 имеет чётную длину. Тогда просто положим $\tau=\sigma_1$. Второй случай: $\pi=(i_1,\dots,i_k)(j_1,\dots,j_k)\sigma_3\cdots\sigma_s$ и $k=2n+1$. В этом случае положим $\tau=(i_1j_1)(i_2j_2)\cdots(i_kj_k)$. Тогда $\tau\pi\tau^{-1}=(i_1,\dots,i_k)(j_1,\dots,j_k)\sigma_3\cdots\sigma_s=\pi$. Пункт **2°**. Пусть в π все циклы разной нечётной длины. Заметим, что сопряжение действует на независимые циклы независимо, т.е $\tau\pi\tau^{-1}=\pi\Leftrightarrow\tau\sigma_i\tau^{-1}=\sigma_i\,\forall i$. Значит, надо выяснить, какие перестановки коммутируют с одним циклом. Достаточно посмотреть, что происходит с циклом $\sigma=(1,2,\dots,n)$. Докажем, что не существует перестановки $\tau\notin\mathbf{A}_n\colon\tau\sigma=\sigma\tau$. Предположим противное. Тогда цикловая структура τ и σ должна быть одинаковая, а значит, $\tau=\sigma^k$. Но это значит, что τ — чётная перестановка. Противоречие. ■

1.3. Свободные группы

1.3.1. Системы порождающих элементов

Определение. Пусть G — группа. Рассмотрим подмножество $S\subset G$ и всевозможные произведения элементов из S и обратных к ним: $H=\left\{s_{i_1}^{\varepsilon_1}s_{i_2}^{\varepsilon_2}\cdots s_{i_k}^{\varepsilon_k}\right\}, \varepsilon_i=\pm1$. Оно называется подгруппой, *порождённой* множеством S. Обозначение: $H=\langle S\rangle$.

Множество H действительно будет подгруппой, так как для $\forall a\ \exists a^{-1}=s_{i_k}^{-\varepsilon_k}\cdots s_{i_1}^{-\varepsilon_1}$, $e=s_{i_1}s_{i_1}^{-1}$. Поскольку элементы не обязательно коммутируют, один и тот же элемент может встречаться несколько раз. Договоримся считать пустое произведение единицей. Очевидно, H — наименьшая подгруппа, содержащая S.

Пример 3.1. Группа с 1 порождающим элементом — циклическая. Пустая система порождает $\{e\}$.

Определение. S — *система порождающих* для G, если для $\forall g\in G\quad g=s_{i_1}^{\varepsilon_1}s_{i_2}^{\varepsilon_2}\cdots s_{i_k}^{\varepsilon_k}$, $s_{i_j}\in S$, $\varepsilon_j=\pm1$.

Замечание. Однозначности разложения в определении не требуется!

Пример 3.2. В группе диэдра $\mathbf{D}_n$ есть система из двух порождающих — поворот a на угол $\frac{2\pi}{n}$ и симметрия b относительно некоторой оси.

Определение. Будем называть комбинации порождающих элементов *словами. Правильными* назовём те слова, в которых не встречаются комбинации вида "$\dots s_is_i^{-1}\dots$".

Определение. Если в G имеет место равенство двух правильных слов a и b, будем говорить о соотношении между этими словами: $a=b\Leftrightarrow ab^{-1}=e$.

Пример 3.3. В группе $\mathbf{D}_n$ есть соотношения $a^n=e, b^2=e, (ab)^2=e$.

1.3.2. Свободные группы

Определение. Если из некоторого набора соотношений следуют все остальные соотношения, то этот набор называется набором *определяющих* соотношений.

Пусть S — абстрактное множество. Берём все правильные слова (*формальные выражения*), составленные из элементов S и обратных к ним, т. е. выражений вида "s" и "s^{-1}". Определим умножение слов u и v: приписываем одно слово к другому и производим сокращения на стыке слов.

Утверждение 1.14. *Построенное таким образом множество произведений является группой.*

□ Единица — есть (пустое произведение). Обратный элемент также имеется. Проверим ассоциативность. Пусть u, v, w — правильные слова. Докажем, что $(uv)w = u(vw)$. Если на стыках слов нет сокращений, то всё ясно, иначе рассмотрим 3 случая.

1° $u = ab,\ v = b^{-1}cd,\ w = d^{-1}f$, и подслово $c \neq \varnothing$. Тогда $(uv)w = (abb^{-1}cd)d^{-1}f = (acd)d^{-1}f = acf$. С другой стороны, $u(vw) = acf$.

2° Если $c = \varnothing$, то $u = ab,\ v = b^{-1}d,\ w = d^{-1}f$, и также получаем, что $(uv)w = u(vw)$.

3° $u = acb,\ v = b^{-1}c^{-1}d,\ w = d^{-1}cf$ — аналогично. ■

Определение. Построенная таким образом группа называется *свободной* группой с множеством свободных порождающих S. (Название объясняется тем, что в такой группе нет нетривиальных соотношений.)

Теперь уточним понятие определяющих соотношений. Пусть есть свободная группа $F = \langle \widetilde{S} \rangle,\ \widetilde{S} = \{x_i\}_{i \in I}$ и группа G, порожденная семейством $S = \{s_i\}_{i \in I}$. Рассмотрим эпиморфизм $f\colon F \to G$, определённый по правилу $f(x_i) = s_i$. В силу однозначности записи элемента свободной группы заданное отображение корректно. При этом $\operatorname{Ker} f =: N$ состоит в точности из тех слов, которые при подстановке $x_i \mapsto s_i$ переходят в единицу группы G, т. е. $x_{i_1}^{\varepsilon_1} \cdots x_{i_k}^{\varepsilon_k} \in \operatorname{Ker} f \Leftrightarrow s_{i_1}^{\varepsilon_1} \cdots s_{i_k}^{\varepsilon_k} = e$. По теореме о гомоморфизме $G \cong F/N$.

Определение. *Определяющая система соотношений* — это такая совокупность правильных слов, равных в G единице, что соответствующие слова в свободной группе порождают N как нормальную подгруппу.

N является минимальной подгруппой, содержащей все эти правильные слова и порождается выбранными соотношениями и сопряженными к ним. Заметим, что не существует алгоритма, определяющего, равны ли два некоторых правильных слова.

Пример 3.4. Свободная группа с одним порождающим элементом — бесконечная циклическая группа.

1.3.3. Определяющие соотношения в группах $\mathbf{D}_n$ и $\mathbf{S}_n$

Утверждение 1.15. *Соотношения в группе диэдра $a^n = e,\ b^2 = e,\ (ab)^2 = e$ являются определяющими.*

□ $\mathbf{D}_n = \langle a, b \rangle$. Рассмотрим свободную группу $F = \langle x, y \rangle$ и группу $N = \langle x^n, y^2, (xy)^2 \rangle$. Рассмотрим гомоморфизм $f\colon F \to \mathbf{D}_n$ такой, что $f(x) = a, f(y) = b$. Очевидно, что $N \subseteq \operatorname{Ker} f$. Докажем, что $F/N \cong \mathbf{D}_n$. Рассмотрим гомоморфизм $\overline{f}\colon F/N \to \mathbf{D}_n$. Найдём число смежных классов в факторгруппе: $(x^k)N$ — их n штук, и $(x^k y)N$ — ещё n штук. Но в группе $\mathbf{D}_n$ ровно $2n$ элементов, значит, $\overline{f}$ — изоморфизм и $N = \operatorname{Ker} f$, а это и требовалось. ■

Рассмотрим $\mathbf{S}_n$. Очевидно, что системами порождающих являются множества всех транспозиций и всех циклов. $\mathbf{S}_n = \langle \tau_1 = (12), \tau_2 = (23), \ldots, \tau_{n-1} = (n-1, n) \rangle = \langle (12), (123), \ldots, (12, \ldots, n) \rangle$.

Задача 1.1. *Доказать, что для системы $\{\tau_i\}$ верны соотношения*

$$\tau^2 = e; \quad \tau_i \tau_j = \tau_j \tau_i, |i - j| \geqslant 2; \quad \tau_i \tau_{i+1} \tau_i = \tau_{i+1} \tau_i \tau_{i+1}. \tag{8}$$

1.4. Прямое произведение групп

1.4.1. Понятие прямого произведения и его свойства

Определение. Дана группа G и $H_1, \ldots, H_s \subset G$. Группа G — *прямое произведение* $H_1, \ldots, H_s$, если:
1° $H_i \lhd G$;
2° $G = H_1 \cdot \ldots \cdot H_s$, т. е. $\forall\, g \in G$ имеем $g = g_1 \ldots g_s$, где $g_i \in H_i$;
3° Разложение в пункте **2°** единственно.
Обозначение: $G = H_1 \times \ldots \times H_s$.

Пример 4.1. Прямая сумма подпространств по операции сложения.

Следствие 1.2. *Если $G = H_1 \times \ldots \times H_s$, то $H_i \cap H_j = \{e\},\ i \neq j$.*

□ Допустим противное: $x \in H_i \cap H_j$. Тогда разложение неоднозначно: $e \ldots g_i \ldots e = x = e \ldots g_j \ldots e$. ■

Определение. *Коммутатором* элементов группы x и y называется элемент $[x, y] := xyx^{-1}y^{-1}$.

Утверждение 1.16. *Если $X \lhd G,\ Y \lhd G$, и $X \cap Y = \{e\}$, то их элементы коммутируют.*

□ Пусть $x \in X,\ y \in Y$. Условие $xy = yx \Leftrightarrow [x, y] = e$. Но так как $xyx^{-1} \in Y$, а $yx^{-1}y^{-1} \in X$, то имеем $[x, y] \in X,\ [x, y] \in Y$. В силу тривиальности пересечения $[x, y] = e$. ■

Следствие 1.3. $(g_1 \ldots g_s)(g'_1 \ldots g'_s) = (g_1 g'_1) \ldots (g_s g'_s)$.

Очевидно, что $g_1^{k_1}\dots g_s^{k_s}=e \Leftrightarrow g_i^{k_i}=e$. Следовательно, $O(g_1\dots g_s)=\text{НОК}\{O(g_1),\dots,O(g_s)\}$. Кроме того, если $|H_i|<\infty$, то $|G|=\prod|H_i|$.

Утверждение 1.17. *Следующие условия эквивалентны:*

I. $G=H_1\times\ldots\times H_s$ — *Группа G есть прямое произведение;*

II. $\mathbf{1}^\circ$, $\mathbf{2}^\circ$ - *те же, что и в определении;* $\mathbf{3}^\circ$ $H_j\cap\big(H_1\dots H_{j-1}H_{j+1}\dots H_s\big)=\{e\}$;

III. $\mathbf{1}^\circ$, $\mathbf{2}^\circ$ - *те же самые;* $\mathbf{3}^\circ$ $H_j\cap\big(H_1\dots H_{j-1}\big)=\{e\}$;

IV. $\mathbf{1}^\circ$ H_i — *подгруппы,* $\forall\, g_i\in H_i$, $\forall\, g_j\in H_j$ $g_ig_j=g_jg_i$; $\mathbf{2}^\circ$ - *то же самое;* $\mathbf{3}^\circ$ — *любое из* I, II, III.

□ *II.* То, что из определения следует тривиальность пересечения, было доказано выше. Теперь выведем единственность разложения из свойств пункта *II*. Допустим противное, т. е. существует $g=h_1\dots h_s=h'_1\dots h'_s$. Преобразуем равенство к виду $h_1'^{-1}h_1=h'_2\dots h'_sh_s^{-1}\dots h_2^{-1}$. Слева стоит произведение элементов из H_1, справа — из $H_2\dots H_s$. Пересечение тривиально $\Rightarrow h_1'^{-1}h_1=e\Leftrightarrow h_1=h'_1$. Аналогично $h_i=h'_i\,\forall\, i$, что и означает единственность разложения. *III*: Доказывается аналогично *II*, пользуясь индукцией по числу подгрупп. *IV*: Докажем нормальность подгрупп H_i. Пусть $h_j\in H_j$. Тогда $gh_jg^{-1}=g_1\dots g_sh_jg_s^{-1}\dots g_1^{-1}$. По условию элементы коммутируют, значит, их можно переставить с h_j, и они сократятся, а значит, $gh_jg^{-1}=h_j$, что и даёт нормальность. ■

Теперь рассмотрим случай конечной группы G. Тогда можно привести ещё несколько эквивалентных определений прямого произведения.

Утверждение 1.18. *Следующие условия эквивалентны определению прямого произведения для конечных групп:*

V. $\mathbf{1}^\circ$, $\mathbf{2}^\circ$ — *те же, что и в первых 4 группах условий;* $\mathbf{3}^\circ$ $|G|=|H_1|\dots|H_s|$;

VI. $\mathbf{1}^\circ$ — *то же самое;* $\mathbf{2}^\circ$ $|G|=|H_1|\dots|H_s|$; $\mathbf{3}^\circ$ — *любое из предыдущих.*

□ *VI*: Рассмотрим $H=H_1\times\ldots\times H_s$ — прямое произведение. Тогда $|H|=|H_1|\dots|H_s|$, так как группы конечны. Следовательно, $H=G$. *V*: Выведем единственность. Из $\mathbf{1}^\circ$ и $\mathbf{2}^\circ$ следует, что $|G|\leqslant|H_1|\dots|H_s|$. Рассмотрим всевозможные произведения $g_1\dots g_s$. Если бы какие-то из них совпадали, то неравенство было бы строгим, а такого по условию не бывает. Утверждение доказано. ■

В аддитивной терминологии прямое произведение называется прямой суммой: $G=H_1\oplus\ldots\oplus H_s$.

1.4.2. Разложение циклических групп

Пример 4.2. $(\mathbb{Z},+)$ — не разлагается в прямое произведение, так как для $\forall\, m,n$ имеем $mn\mathbb{Z}\subset m\mathbb{Z}\cap n\mathbb{Z}$.

Пример 4.3. $G=\langle a\rangle_n$, где n конечно. Если H — подгруппа в G, то $H=\left\langle a^d\right\rangle$, $|H|=\frac{n}{d}$. Если $n=p^k$, где число p простое, то $H_i=\left\langle a^{p^i}\right\rangle, i\leqslant k$. Тогда прямого произведения нет:

$$\langle a\rangle\supset\langle a^p\rangle\supset\ldots\supset\left\langle a^{p^{k-1}}\right\rangle\supset\{e\}\,. \tag{9}$$

Определение. Группа порядка p^k называется *p-примарной* группой.

Пусть $n=p_1^{k_1}\dots p_s^{k_s}$, и $p_i\neq p_j$, $i\neq j$. Пусть $m_i:=p_i^{k_i}$. Рассмотрим группы $H_i=\left\langle a^{\frac{n}{m_i}}\right\rangle_{m_i}$ и их произведение $G=\prod H_i$. Если $x\in H_j$, то $O(x)$ — некоторая степень числа p_j. Пусть $x\in\bigcap H_i$. Тогда очевидно, что $O(x)=1$ и $x=e$. Кроме того, имеем $\prod|H_i|=\prod p_i^{k_i}=|G|$. Тем самым любая циклическая группа разлагается в прямое произведение примарных циклических групп.

1.4.3. Внешнее прямое произведение

Определение. Пусть $G_1,\dots,G_s$ — группы. Составим из них группу

$$G:=\{(g_1,\dots,g_s)\mid g_i\in G_i\}=G_1\dot\times\ldots\dot\times G_s. \tag{10}$$

Она является множеством векторов-строк из g_i и называется *внешним прямым произведением* групп G_i.

Можно отождествить внешнее и внутреннее произведение следующим образом. Пусть $G=H_1\times\ldots\times H_s$ (произведение подгрупп), а $\widetilde G=G_1\dot\times\ldots\dot\times G_s$ (внешнее произведение). Построим изоморфизм $\varphi\colon G\to\widetilde G$ по правилу $g_1\dots g_s\overset{\varphi}{\longmapsto}(g_1,\dots,g_s)$. Отображение задано корректно, так как элементы из разных подгрупп коммутируют, и $(g_1\dots g_s)(g'_1\dots g'_s)=(g_1g'_1)\dots(g_sg'_s)\mapsto(g_1g'_1,\dots,g_sg'_s)$. Подгруппы H_i можно отождествить с множествами векторов $\{(e,\dots,e,g_i,e,\dots,e)\}$, т. е. с подгруппами во внешнем произведении, и таким образом, внешнее и внутреннее произведения можно не различать.

1.4.4. Гомоморфизмы произведений групп

Пусть есть гомоморфизм $G \to H = H_1 \times \ldots \times H_s$ и набор гомоморфизмов $\varphi_i \colon G \to H_i$. Определим гомоморфизм $\varphi \colon G \to H$ следующим образом: $\varphi(g) := \big(\varphi_1(g), \ldots, \varphi_s(g)\big)$. Наоборот, по отображению φ можно определить φ_i. Имеется биекция между набором гомоморфизмов из G в H и множеством $\{\varphi_i \mid \varphi_i \colon G \to H_i\}$.

Зададим гомоморфизм $\varphi \colon G = G_1 \times \ldots \times G_s \to H$. Достаточно задать ограничения $\varphi_i = \varphi\Big|_{G_i}$, $\varphi_i \colon G_i \to H$. Отображение φ задается ограничениями однозначно: $\varphi(g) = \varphi(g_1 \ldots g_s) = \big(\varphi_1(g_1) \ldots \varphi_s(g_s)\big)$. Отображение φ будет гомоморфизмом, когда элементы образов различных φ_i коммутируют: $y_i \in \operatorname{Im}\varphi_i$, $y_j \in \operatorname{Im}\varphi_j \Rightarrow y_i y_j = y_j y_i$. В том случае, когда группа H — абелева, то всегда есть биективное соответствие между множеством гомоморфизмов из G в H и наборами $\{\varphi_1 \ldots \varphi_s\}$.

Теорема 1.19. *Пусть $G = G_1 \times \ldots \times G_s$, и $H_i \lhd G_i$. Тогда $H \lhd G$ и $G/H \cong G_1/H_1 \times \ldots \times G_s/H_s$.*

□ Построим эпиморфизм $\varphi \colon G \to G_1/H_1 \times \ldots \times G_s/H_s$. Положим $\varphi(g_1 \ldots g_s) = (g_1 H_1, \ldots, g_s H_s)$. Очевидно, что отображение задано корректно. Найдём его ядро. Имеем

$$\operatorname{Ker}\varphi = \{g_1 \ldots g_s \colon g_i H_i = H_i \Rightarrow g_i \in H_i \,\forall\, i\}\,. \tag{11}$$

Следовательно, $\operatorname{Ker}\varphi = H_1 \times \ldots \times H_s$, а по теореме о гомоморфизме $G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$. ■

Следствие 1.4. *Частный случай теоремы: $G = H_1 \times H_2 \Rightarrow G/H_1 \cong H_2$.*

1.5. Абелевы группы

1.5.1. Основные свойства

В абелевой группе всякая подгруппа нормальна.

Рассмотрим гомоморфизмы вида $\varphi \colon G \to K$, где G — произвольная группа, K — абелева. Попробуем ввести на множестве гомоморфизмов структуру группы. Определим произведение гомоморфизмов так: $(\varphi_1 \cdot \varphi_2)(x) := \varphi_1(x)\varphi_2(x)$. Если K — абелева, то произведение гомоморфизмов есть гомоморфизм (*для неабелевых групп это неверно!!!*):

$$(\varphi \cdot \psi)(xy) = \varphi(xy)\psi(xy) = \varphi(x)\underbrace{\varphi(y)\psi(x)}_{\text{комм.}}\psi(y) = \big(\varphi(x)\psi(x)\big)\big(\varphi(y)\psi(y)\big) = (\varphi \cdot \psi)(x)(\varphi \cdot \psi)(y).$$

Определим обратное отображение $\varphi^{-1}(x) := \varphi(x)^{-1}$. Оно будет гомоморфизмом только тогда, когда K — абелева группа. В качестве нейтрального элемента возьмём гомоморфизм, переводящий всё в единицу. Таким образом мы построили группу $\operatorname{Hom}(G, K)$. Заметим, что она будет абелевой.

1.5.2. Системы порождающих в абелевой группе

Поскольку в абелевых группах все элементы коммутируют, правильными словами будут те, в которых все элементы попарно различны. Пусть дана группа $(G, +)$. Тогда любой элемент представляется в виде целочисленной линейной комбинации порождающих, в которой только конечное число коэффициентов отличны от нуля: $g = \sum\limits_{i \in I} n_i a_i$, $n_i \in \mathbb{Z}$. Однако запись элемента по-прежнему неоднозначна.

Задача 1.2. *Доказать, что какую бы мы не взяли систему порождающих в группах $(\mathbb{Q}, +)$ и $(\mathbb{Q}, \cdot)$, из неё можно выкинуть какой-то элемент.*

Будем теперь рассматривать абелевы группы с конечной системой порождающих.

Определение. Конечнопорождённая абелева группа G называется *свободной абелевой* группой со свободной системой порождающих $\{a_1, \ldots, a_n\}$, если запись элемента в виде целочисленной линейной комбинации этих порождающих однозначна. Система порождающих называется в этом случае *базисом*, а число n — *рангом* группы.

Абелева группа свободна, если она обладает базисом. $G = \langle a_1 \rangle_\infty \oplus \ldots \oplus \langle a_n \rangle_\infty$.

Теорема 1.20. *Конечнопорождённая абелева группа изоморфна некоторой факторгруппе свободной группы того же ранга, т. е. если F — свободная абелева группа с базисом $\{x_1, \ldots, x_n\}$, а $G = \langle a_1, \ldots, a_n \rangle$, то найдётся подгруппа $H \subset F$, такая что $G \cong F/H$.*

□ Определим эпиморфизм $\varphi \colon F \to G$ так: $\varphi(x_i) := a_i$. Тогда $\varphi(\sum n_i x_i) = \sum n_i a_i$. Очевидно, его образ есть вся группа G. По теореме о гомоморфизме $F/\operatorname{Ker}\varphi \cong G$. Ядро φ и будет искомой подгруппой в F. ■

1.5.3. Разложение конечнопорождённых абелевых групп

Пусть F — свободная абелева группа с базисом $\{x_1, \dots, x_n\}$, и $H \subseteq F$, Γ — некоторое множество индексов, и $\left\{y_\gamma = \sum a_{i\gamma} x_i \;\middle|\; a_{i\gamma} \in \mathbb{Z}, \gamma \in \Gamma\right\}$ — система порождающих подгруппы H. Числа $a_{i\gamma}$ образуют матрицу A, в которой n строк и, возможно, бесконечное число столбцов. Есть 3 типа целочисленных элементарных преобразований (ЭП) такой матрицы:

1° К одной строке можно прибавить другую, умноженную на целое число;

2° Можно менять строки местами;

3° Можно умножать строку на обратимые элементы кольца $\mathbb{Z}$, то есть на ± 1.

Аналогичные преобразования можно осуществлять со столбцами.

Теорема 1.21. *Посредством элементарных преобразований можно привести матрицу коэффициентов к «диагональному» виду* $\operatorname{diag}(d_1, \dots, d_n)$. *При этом* $d_1 | d_2| \dots | d_n$ *и итоговый вид матрицы определён однозначно.*

□ Докажем индукцией по числу строк (их конечное число). Если матрица нулевая, доказывать нечего. База индукции: $n = 1$. Выберем наименьший по модулю ненулевой элемент $a_{i\gamma}$. Если все остальные элементы делятся на него, то можно путём ЭП первого типа обнулить все эти элементы. Если существует элемент $a_{i\delta}$, не делящийся на $a_{i\gamma}$, то с помощью столбца γ поделим $a_{i\delta}$ с остатком, и получим меньший по модулю элемент (остаток). После конечного числа шагов все элементы строки будут делиться на какой-то из её элементов. База индукции есть.

Теперь предположим, что всё доказано для $n-1$ строки, тогда докажем для n строк. Выберем наименьший по модулю ненулевой элемент, и проведём аналогичные действия для той строки и того столбца, в котором стоит этот элемент. (Если всё на него делится, тогда можно всё кроме него обнулить, а если не делится, то поделим с остатком, и т.д.) Таким образом можно обнулить некоторый «крест» в матрице, а на пересечении строки и столбца этого креста стоит ненулевой элемент d_k, и все остальные элементы на него делятся. Путём перестановки строк и столбцов можно сдвинуть крест в левый верхний угол матрицы. Тогда останется матрица с $n-1$ строкой, и шаг индукции доказан. Очевидно, что на каждом шаге каждый ненулевой элемент d_k делит все элементы минора матрицы порядка k и является наибольшим общим делителем чисел этого минора. Из алгоритма Евклида следует, что при элементарных преобразованиях указанного типа НОДы элементов не меняются (сам алгоритм Евклида есть последовательность таких преобразований). Значит, набор $d_1, \dots, d_n$ определён однозначно. ■

Изучим влияние ЭП на базис. Очевидно, что ЭП 2 и 3 типа несущественны. Остается разобрать случай ЭП первого типа. Для строк $(i), (j)$: при ЭП $(i) \mapsto (i) + \lambda(j)$, $\lambda \in \mathbb{Z}$ имеем

$$y_\gamma = (a_{ij} + \lambda a_{j\gamma}) x_i + a_{j\gamma}(x_j - \lambda x_i) + \sum_{k \neq i,j} a_{k\gamma} x_k. \tag{12}$$

Очевидно, что такое преобразование соответствует элементарной замене базиса $x_j \mapsto x_j - \lambda x_i$. Рассуждения для столбцов аналогичны.

Теорема 1.22. *Пусть F — свободная абелева группа, $H \subseteq F$. Тогда можно выбрать новый базис $F = \langle x'_1, \dots, x'_n \rangle$ и новую систему порождающих $H = \langle y'_1, \dots, y'_n \rangle$ так, что $y'_j = d_j x'_j$, $d_1 | d_2 | \dots | d_n$ и H является свободной группой с рангом* $\operatorname{rk} H \leqslant n$.

□ Следует из предыдущей теоремы. Приведением матрицы к диагональному виду элементарными преобразованиями и соответствующими им заменами базисов можно найти требуемый базис и систему порождающих. Пусть $d_1, \dots, d_k \neq 0, d_{k+1}, \dots, d_n = 0$. Тогда $H = \langle y'_1, \dots, y'_k \rangle$. Эти порождающие свободны, так как если бы $\lambda_1 y'_1 + \dots + \lambda_k y'_k = 0$, то и $\lambda_1 d_1 x'_1 + \dots + \lambda_k d_k x'_k = 0$, а это противоречит тому, что $\{x_1, \dots, x_n\}$ — базис F. ■

Теорема 1.23 (Существование разложения). *Любая конечно порождённая абелева группа разлагается в прямую сумму конечного числа бесконечных циклических групп и примарных циклических групп.*

□ Пусть $G = \langle a_1, \dots, a_n \rangle$ — абелева группа. Поскольку $G \cong F/H$, по предыдущей теореме существует базис: $F = \langle x_1, \dots, x_n \rangle$, $H = \langle d_1 x_1, \dots, d_k x_k, d_{k+1} x_{k+1}, \dots, d_n x_n \rangle$, где $d_{k+1} = \dots = d_n = 0$. Имеем

$$F = \langle x_1 \rangle_\infty \oplus \dots \oplus \langle x_n \rangle_\infty, H = \langle d_1 x_1 \rangle_\infty \oplus \dots \oplus \langle d_k x_k \rangle_\infty \oplus \underbrace{\langle d_{k+1} x_{k+1} \rangle_\infty \oplus \dots \oplus \langle d_n x_n \rangle_\infty}_{0}.$$

По теореме о факторизации по прямым слагаемым

$$G \cong \frac{\langle x_1 \rangle}{\langle d_1 x_1 \rangle} \oplus \dots \oplus \frac{\langle x_k \rangle}{\langle d_k x_k \rangle} \oplus \frac{\langle x_{k+1} \rangle}{\{0\}} \oplus \dots \oplus \frac{\langle x_n \rangle}{\{0\}}.$$

Если $d_i > 1$, то i-е слагаемое есть циклическая группа $\mathbb{Z}/d_i\mathbb{Z}$. Если $d_i = 0$, остается бесконечное циклическое слагаемое $\mathbb{Z}$. Если же $d_i = 1$, то $\langle x \rangle / \langle x \rangle = \{0\}$, и такое слагаемое можно отбросить. Итак, получаем разложение

$$G \cong \bigoplus_{i=1}^{k} (\mathbb{Z}/d_i\mathbb{Z}) \oplus \mathbb{Z}^{n-k}.$$

В свою очередь, каждую конечную циклическую группу разложим на примарные, что и требовалось. ■

Определение. Приведённое выше разложение называется *каноническим*, если $d_1 | \ldots | d_k$.

Теорема 1.24 (Единственность разложения). *В разложении абелевой группы в прямую сумму циклических групп число слагаемых и их порядки определены однозначно.*

□ Пусть $G = \langle c_1 \rangle_{p_1^{k_1}} \oplus \ldots \oplus \langle c_s \rangle_{p_s^{k_s}} \oplus \langle c_{s+1} \rangle_\infty \oplus \ldots \oplus \langle c_{s+t} \rangle_\infty$. Рассмотрим подгруппу кручения (т. е. подгруппу элементов конечного порядка)

$$\operatorname{Tor} G := \{a \in G \colon ma = 0 \text{ для некоторого } m \in \mathbb{Z},\ m \neq 0\}.$$

Очевидно, что $\operatorname{Tor} G$ есть сумма конечных слагаемых (s штук). Тогда имеем $G = \operatorname{Tor} G \oplus \mathbb{Z}^t$, или $G/\operatorname{Tor} G \cong \mathbb{Z}^t$. Определение $\operatorname{Tor} G$ не зависит от разложения, а значит и число t не зависит от разложения.

Разберёмся теперь с конечными слагаемыми. Для каждого p рассмотрим подгруппы p-кручения

$$\operatorname{Tor}_p G := \left\{a \in G \colon p^k a = 0 \text{ для некоторого } k \in \mathbb{Z}\right\},$$

т. е. суммы p-примарных слагаемых при фиксированном p. Аналогично первому случаю число таких подгрупп определяется однозначно. Остаётся рассмотреть случай, когда G — примарная группа порядка p^k. Пусть есть разложение $G = \langle c_1 \rangle_{p^{k_1}} \oplus \ldots \oplus \langle c_r \rangle_{p^{k_r}}$, и $k_1 + \ldots + k_s = k$. Докажем индукцией по k, что набор чисел $\{k_1, \ldots, k_r\}$ от разложения не зависит. При $k = 1$ всё очевидно. Пусть $k > 1$. Тогда рассмотрим подгруппу $pG := \{pa \mid a \in G\}$. Очевидно, что

$$pG = \langle pc_1 \rangle_{p^{k_1 - 1}} \oplus \ldots \oplus \langle pc_r \rangle_{p^{k_r - 1}}. \tag{13}$$

Если $k_i = 1$, то это слагаемое при умножении на p исчезнет. Определение pG от разложения не зависит, а по предположению индукции для порядка меньше p^k набор чисел $\{k_i\}$ не зависит от разложения. Тем самым теорема доказана. ■

Замечание. Подгруппу кручения иногда называют периодической частью абелевой группы.

Как по разложению определить, изоморфны ли группы? Нужно разложить их в примарные циклические. В силу единственности разложения можно по нему судить об изоморфности групп.

1.5.4. Конечные абелевы группы

Определение. *Показателем* группы называется число $d := \min\left\{k > 0 \colon x^k = e\, \forall\, x \in G\right\}$.

Выясним, когда прямая сумма циклических групп циклическая. Пусть $G = \langle a_1 \rangle_{n_1} \oplus \ldots \oplus \langle a_s \rangle_{n_s}$, и $|G| = n = n_1 \ldots n_s$. Группа G — циклическая, когда в ней есть элемент порядка n. Для $\forall\, x = (x_1, \ldots, x_s)$ имеем $O(x_i) | n_i$. Возьмём элемент $a = (a_1, \ldots, a_s)$ — он, очевидно, имеет наибольший порядок. $O(a) = \operatorname{НОК}\{n_1, \ldots, n_s\}$. Значит, G — циклическая $\Leftrightarrow$ числа $n_1, \ldots, n_s$ попарно взаимно просты.

Утверждение 1.25. *Конечная абелева группа G циклическая $\Leftrightarrow$ её показатель d равен порядку группы.*

□ Очевидно, что $d = \operatorname{НОК}\{O(x) | x \in G\}$. Разложим группу в прямую сумму циклических групп. Если их порядки не взаимно просты, то $d < |G|$ и группа не циклическая. Наоборот, если порядки слагаемых взаимно просты, то $d = |G|$ и группа циклическая. ■

Есть биекция между конечными абелевыми группами порядка n и разложениями числа n в произведение степеней простых чисел.

Пример 5.1. $|G| = 72 = 8 \cdot 9 = 4 \cdot 2 \cdot 9 = 2 \cdot 2 \cdot 2 \cdot 9 = 8 \cdot 3 \cdot 3 = 4 \cdot 2 \cdot 3 \cdot 3 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$.

$$G_1 = \mathbb{Z}_8 \oplus \mathbb{Z}_9$$

$$G_2 = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$$

$$\ldots$$

$$G_6 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

1.5.5. Свойства подгрупп в мультипликативной группе поля

Пусть K — поле, $K^* = K \setminus \{0\}$ — его мультипликативная группа.

Утверждение 1.26. *Любая конечная подгруппа в мультипликативной группе поля циклическая.*

□ Пусть $G \subseteq K^*$, $|G| = n$, d — показатель G. Имеем $x^d = 1\, \forall\, x \in G$. Поскольку уравнение $x^d - 1 = 0$ имеет не более чем d корней, то $|G| \leqslant d \Rightarrow |G| = d$, что и означает цикличность группы. ■

1.5.6. Геометрические приложения абелевых групп. Дискретные подгруппы в $\mathbb{R}^n$

Определение. Пусть $V = \mathbb{R}^n$ — евклидово пространство. Подгруппа $G \subseteq (V, +)$ называется *решёткой*, если:
1° G дискретна, т. е. $\exists\, \varepsilon > 0\colon \{x \in V\colon |x| < \varepsilon\} \cap G = \{0\}$;
2° $\langle G \rangle = V$, т. е. линейная оболочка G с вещественными коэффициентами совпадает с V.

Теорема 1.27. *Любая решётка G в $\mathbb{R}^n$ является свободной абелевой группой, порождённой некоторым базисом пространства V, т. е. $G = \{\sum k_i e_i \mid k_i \in \mathbb{Z}\}$.*

□ Из второго пункта определения G следует, что существует базис $u_1, \ldots, u_n$ пространства V, где $u_i \in G$. Пусть $x \in G$, тогда $x = \sum \xi_i u_i$. Возможны 3 случая для коэффициентов решётки:
1° $\forall\, x \in G \forall\, \xi_i \in \mathbb{Q}$, и все знаменатели у ξ_i ограничены сверху;
2° $\xi_i \in Q$, но имеют сколь угодно большие знаменатели;
2° $\exists\, x$, у которого хотя бы одна из координат иррациональна.

Покажем, что из всех случаев возможен только случай **1°**. Пусть $F = \left\{\sum k_i u_i \;\middle|\; k_i \in \mathbb{Z}\right\}$ — свободная абелева группа ранга n (здесь и далее суммирование идёт по $i = \overline{1, n}$). Взяв НОК всех знаменателей коэффициентов, можно найти N такое, что $Nx \in F$ для $\forall\, x \in G$. Очевидно, что отображение $x \overset{\varphi}{\longmapsto} Nx$ есть инъективный гомоморфизм $G \to F$. Тогда $G \cong \operatorname{Im}\varphi \subseteq F \Rightarrow G$ — свободная группа (как подгруппа свободной группы), и $\operatorname{rk} G \leqslant n$. Но так как $\langle G \rangle = V$, то $\operatorname{rk} G = n$. Значит, базис V есть базис G.

Докажем, что случаи **2°** и **3°** для дискретной подгруппы невозможны. Во втором случае, так как знаменатели коэффициентов неограниченны, можно отбросить целые части координат и рассмотреть в G подмножество $M := \{x \in G \mid x = \sum \xi_i u_i, \xi_i \in [0, 1]\}$. Оно, очевидно, ограничено и бесконечно, а значит, обладает предельной точкой, в любой окрестности которой есть точки из G. Это противоречит дискретности.

В третьем случае пусть $x = \xi_1 u_1 + \ldots + \xi_n u_n$ и для определённости координата $\xi_1 \notin \mathbb{Q}$. Рассмотрим последовательность векторов $x_m = \{mx \mid m \in \mathbb{Z}\}$ (аналогично отбросим целые части координат и оставим только дробные). Докажем, что все элементы этой последовательности различны. Пусть $mx = lx$, тогда $mx - lx = \sum\limits_{i=1}^{n} k_i u_i, k_i \in \mathbb{Z}$, а значит, $m\xi_1 - l\xi_1 = k_1$, т. е. $\xi_1 \in \mathbb{Q}$, а по условию это не так. Значит, все x_i различны. Но они все находятся в ограниченной области, а значит есть предельная точка и противоречие с дискретностью G. ■

1.6. Нормальные ряды группы. Теорема Жордана – Гёльдера

Определение. *Нормальным рядом* называется последовательность подгрупп

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \ldots \rhd H_k = \{e\}\,. \tag{14}$$

Число k называется *длиной* нормального ряда, а факторгруппы H_{k-1}/H_k — *факторами* нормального ряда.

Определение. Пусть дан нормальный ряд $G = H_0 \rhd H_1 \rhd H_2 \rhd \ldots \rhd H_k = \{e\}$. Другой нормальный ряд $G = F_0 \rhd F_1 \rhd F_2 \rhd \ldots \rhd F_m = \{e\}$ называется *уплотнением* первого, если все подгруппы первого ряда встречаются во втором.

В ряду любой член может повторяться несколько раз. Если этого нет, то говорят о ряде без повторений.

Определение. *Композиционный* ряд — нормальный ряд, который нельзя уплотнить (без повторений).

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

Очевидно, что ряд композиционный $\Leftrightarrow$ все его факторы простые.

Теорема 1.28 (Жордана – Гёльдера). *Пусть G обладает композиционным рядом длины k. Тогда все нормальные ряды в G имеют длину не больше k, а все композиционные ряды имеют одинаковую длину и их факторы изоморфны после некоторой перестановки.*

□ Пусть в G есть соответственно композиционный и нормальный ряды

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \ldots \rhd H_k = \{e\}\,, \quad G = K_0 \rhd K_1 \rhd K_2 \rhd \ldots \rhd K_m = \{e\}\,.$$

Докажем, что $m \leqslant k$. Проведём индукцию по числу k. Если $k = 1$, то группа простая и всё очевидно. Пусть утверждение теоремы верно для рядов длины меньше k, докажем для рядов длины k.

1° Первый случай: $K_1 \subseteq H_1$. Тогда $H_1 \rhd K_1 \rhd K_2 \rhd \ldots K_m$ — нормальный ряд в H_1. Но по условию в H_1 есть композиционный ряд длины $k - 1$, а тогда по предположению индукции все ряды в H_1 имеют длину $\leqslant k - 1$. Значит, $m - 1 \leqslant k - 1 \Rightarrow m \leqslant k$.

2° Второй случай: $K_1 \nsubseteq H_1$. Но тогда и $H_1 \nsubseteq K_1$, поскольку в противном случае по теореме о соответствии $K_1/H_1 \lhd G/H_1$, а этого не бывает, так как все факторы простые. Обозначим $L := (H_1 \cap K_1)$. Итак, имеем $L \lhd H_1, L \neq H_1$. Рассмотрим H_1K_1. Имеем $H_1 \subsetneq H_1K_1 \lhd G \Rightarrow H_1K_1 = G$. По второй теореме об изоморфизме $G/H_1 = H_1K_1/H_1 \cong K_1/L$ и $G/K_1 = H_1K_1/K_1 \cong H_1/L$. В H_1 есть композиционный ряд длины $\leqslant k - 1$, а в L есть композиционный ряд длины $\leqslant k - 2$, так как $L \lhd H_1$. С другой стороны, $L \lhd K_1, L \neq K_1$, и K_1/L —

простая группа. Значит, и в K_1 есть композиционный ряд длины $k-1$. Значит, можно применить индуктивное предположение, и во втором случае также получаем $m \leqslant k$. Отсюда следует, что все композиционные ряды в G имеют одинаковую длину.

Теперь докажем второе утверждение об изоморфности факторов. Пусть в G есть два композиционных ряда

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \ldots \rhd H_k = \{e\}, \quad G = K_0 \rhd K_1 \rhd K_2 \rhd \ldots \rhd K_k = \{e\}.$$

Проведём индукцию по длине ряда. Рассмотрим два случая. Первый случай: $H_1 = K_1$. Тогда применим предположение индукции к H_1 и сведём утверждение к меньшему числу факторов. Второй случай: $H_1 \neq K_1$. Тогда рассмотрим подгруппу $L_2 := (H_1 \cap K_1)$. Имеем $L_2 \lhd H_1 \lhd G$ и $L_2 \lhd K_1 \lhd G$. Тогда имеем ряды

(1) $G \rhd H_1 \rhd H_2 \rhd H_3 \rhd \ldots$
(2) $G \rhd H_1 \rhd L_2 \rhd L_3 \rhd L_4 \rhd \ldots$
(3) $G \rhd K_1 \rhd L_2 \rhd L_3 \rhd L_4 \rhd \ldots$
(4) $G \rhd K_1 \rhd K_2 \rhd K_3 \rhd \ldots$

Здесь $L_3 \rhd L_4 \rhd \ldots$ — некоторый композиционный ряд в L_2. Посмотрим на первые два ряда. В H_1 имеем два композиционных ряда длины $k-1$, а значит по индуктивному предположению их факторы $\frac{H_1}{H_2}, \frac{H_2}{H_3}, \ldots$ и $\frac{H_1}{L_2}, \frac{L_2}{L_3}, \ldots$ изоморфны после некоторой перестановки. То же самое можно сказать про два последних ряда: $\frac{K_1}{K_2}, \frac{K_2}{K_3}, \ldots$ и $\frac{K_1}{L_2}, \frac{L_2}{L_3}, \ldots$ Остаётся заметить, что $G = H_1K_1$, тогда $\frac{G}{H_1} = \frac{H_1K_1}{H_1} \cong \frac{K_1}{L_2}$, и $\frac{G}{K_1} = \frac{H_1K_1}{K_1} \cong \frac{H_1}{L_2}$, то есть первые и вторые факторы во втором и третьем рядах изоморфны «крест-накрест». Теорема доказана. ■

Пример 6.1. Композиционные ряды векторных пространств есть цепочки вложенных подпространств. Все ряды одинаковой длины ⇒ число элементов в базисе одинаково.

1.7. Коммутант. Разрешимые группы. Простые группы

1.7.1. Коммутант

Определение. Группа называется *разрешимой*, если она обладает нормальным рядом с абелевыми факторами.

Попытаемся построить такой ряд. Нужно построить подгруппу $N \lhd G$, такую, что G/N — абелева. Для этого возьмём коммутаторы $[a,b]$ всех элементов группы.

Лемма 1.29. *Дана группа G и $N \lhd G$. Факторгруппа G/N будет абелевой $\Leftrightarrow [a,b] \in N \,\forall\, a,b \in G$.*

□ G/N — абелева $\Leftrightarrow [aN, bN] = eN = N \Leftrightarrow (aN)(bN)(a^{-1}N)(b^{-1}N) = aba^{-1}b^{-1}N = N \Leftrightarrow [a,b] \in N$. ■

Свойства коммутатора: $[a,b]^{-1} = [b,a]$. Кроме того, сопряженный к коммутатору есть коммутатор сопряженных:

$$g[a,b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} = [gag^{-1}, gbg^{-1}]. \tag{15}$$

Определение. Подгруппа, порожденная всеми коммутаторами в группе G, называется *коммутантом* G и обозначается G'. Коммутант иногда называют *производной* подгруппой.

Очевидно, что коммутант есть наименьшая нормальная подгруппа в G, факторгруппа по которой абелева. Приведём некоторые другие свойства коммутанта.

Лемма 1.30. *При гомоморфизме $f\colon G \to K$ имеем $f(G') \subset K'$. Если f — эпиморфизм, то $f(G') = K'$.*

□ Имеем

$$f\big([a,b]\big) = f(a)f(b)f(a)^{-1}f(b)^{-1} = \big[f(a), f(b)\big]. \tag{16}$$

Пусть $f(a) = x, f(b) = y$. По доказанному $[x,y] \in K'$. Если f сюръективен, то любой элемент K' есть образ некоторого коммутатора, значит, $f(G') = K'$. ■

По индукции определяются коммутанты высших порядков: $G^{(i+1)} := \big(G^{(i)}\big)'$. По индукции очевидным образом доказывается предыдущее утверждение для коммутантов произвольного порядка.

1.7.2. Разрешимость групп

Построим ряд из коммутантов группы: $G \rhd G^{(1)} \rhd G^{(2)} \rhd \ldots$

Теорема 1.31. *Группа G разрешима $\Leftrightarrow \exists\, l\colon G^{(l)} = \{e\}$, т. е. существует нормальный ряд из коммутантов группы.*

□ Пусть есть ряд с абелевыми факторами $G \rhd H_1 \rhd H_2 \rhd \ldots$ Докажем по индукции, что $G^{(i)} \subseteq H_i \,\forall\, i$. База: $G' \subseteq H_1$, так как G/H_1 — абелева. Шаг индукции: пусть $G^{(i-1)} \subseteq H_{i-1}$. Так как H_{i-1}/H_i — абелева, то $H'_{i-1} \subseteq H_i$. Тогда имеем $G^{(i)} \subseteq H'_{i-1} \subseteq H_i$, что и требовалось доказать. ■

Следствие 1.5. *Всякая подгруппа разрешимой группы разрешима.*

□ В самом деле, если $G^{(l)} = \{e\}$ и $H \subseteq G$, то $H^{(l)} \subseteq G^{(l)} \Rightarrow H^{(l)} = \{e\}$. ■

Утверждение 1.32. *Пусть $H \lhd G$, группы H и G/H разрешимы. Тогда G разрешима.*

□ В силу разрешимости $\exists\, n, m\colon (G/H)^{(n)} = \{\overline{e}\}$, и $H^{(m)} = \{e\}$. Рассмотрим гомоморфизм $\varphi\colon G \to G/H$. По доказанному $\varphi(G^{(n)}) \subseteq (G/H)^{(n)} = \{\overline{e}\}$, т. е. $G^{(n)} \subseteq \operatorname{Ker}\varphi = H$. Значит, $G^{(n+m)} = \{e\}$. ■

1.7.3. Примеры разрешимых групп

Любая абелева группа, очевидно, разрешима. Группа $\mathbf{D}_n$ разрешима, так как в ней есть нормальная подгруппа вращений R, а $\mathbf{D}_n/R \cong \mathbb{Z}_2$ — абелева. Группы $\mathbf{S}_3$ и $\mathbf{A}_3$ разрешимы, так как $\mathbf{A}_3$ абелева, а $\mathbf{S}_3 \cong \mathbf{D}_3$.

Рассмотрим более сложный пример: невырожденные верхнетреугольные матрицы $\mathbf{T}_n(\mathbb{K})$ над полем $\mathbb{K}$.

Утверждение 1.33. *Группа верхнетреугольных матриц $\mathbf{T}_n(\mathbb{K})$ разрешима.*

□ Зададим гомоморфизм $f\colon \mathbf{T}_n(\mathbb{K}) \to (\mathbb{K}^*)^n$, где $\mathbb{K}^*$ — мультипликативная группа поля $\mathbb{K}$:

$$\begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \xmapsto{f} (a_1, \ldots, a_n).$$

Очевидно, что $\operatorname{Ker} f = \mathbf{UT}_n(\mathbb{K})$ — группа верхних унитреугольных матриц. $\operatorname{Im} f$ есть абелева группа (множество векторов-строк). Остаётся доказать разрешимость $\operatorname{Ker} f$. Проведём индукцию по размерности n. База индукции очевидна. Пусть утверждение верно для $n-1$. Тогда построим гомоморфизм $g\colon \mathbf{UT}_n(\mathbb{K}) \to \mathbf{UT}_{n-1}(\mathbb{K})$, при котором угловой минор размерности $n-1$ отображается тождественно (грубо говоря, отрезаем от матрицы последнюю строку и последний столбец). Сюръективность g очевидна, а $\operatorname{Ker} g$ состоит из матриц вида

$$\begin{pmatrix} 1 & & 0 & b_1 \\ & \ddots & & \vdots \\ 0 & & 1 & b_{n-1} \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Тогда $\operatorname{Ker} g \cong \mathbb{K}^{n-1}$, т. к. $\operatorname{Ker} g \cong \{(b_1, \ldots, b_{n-1})\}$. Произведение матриц при этом переходит в сумму строк, а образ есть абелева группа по сложению, и шаг индукции доказан. По предыдущему утверждению $\mathbf{T}_n(\mathbb{K})$ разрешима. ■

Очевидно, что если в нормальном ряду есть хоть один неразрешимый фактор, то и вся группа неразрешима.

1.7.4. Простые группы

Абелева группа проста $\Leftrightarrow$ она циклическая простого порядка.

Лемма 1.34. *Группа $\mathbf{A}_n$ порождается тройными циклами.*

□ Любая чётная подстановка есть произведение чётного числа транспозиций. Любую пару транспозиций можно получить из тройных циклов: $(ac)(bd) = (abc)(abd)$, а все тройные циклы у нас есть по условию. ■

Лемма 1.35. *Если нормальная подгруппа $N \lhd \mathbf{A}_n$ содержит хотя бы один тройной цикл, то $N = \mathbf{A}_n$.*

□ При $n \geqslant 5$ все тройные циклы сопряжены, а нормальная подгруппа есть объединение классов сопряженности, значит, она содержит все тройные циклы и тем самым по предыдущей лемме порождает $\mathbf{A}_n$. ■

Теорема 1.36. *Группа $\mathbf{A}_n$ при $n \geqslant 5$ простая.*

□ Пусть $N \lhd \mathbf{A}_n$ и $N \neq \{e\}$. Докажем, что в N есть тройной цикл. Тогда утверждение теоремы будет следовать из лемм. Пусть $\sigma = \sigma_1\sigma_2\sigma_3 \ldots \sigma_s \in N$. 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, $N = \mathbf{A}_n$. ■

Теорема 1.37. *Группа $\mathbf{SO}_3(\mathbb{R})$ простая.*

□ Из курса аналитической геометрии известно, что любая матрица $A \in \mathbf{SO}_3(\mathbb{R})$ подобна матрице

$$A = \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{17}$$

Отсюда следует, что все матрицы в $\mathbf{SO}_3(\mathbb{R})$ сопряжены. Пусть в $\mathbf{SO}_3(\mathbb{R})$ есть нетривиальная нормальная подгруппа N. Тогда в ней есть матрица (17) с некоторым фиксированным углом поворота α. Рассмотрим матрицу

$$B(\varphi) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix}$$

Положим $C(\varphi) := AB(\varphi)A^{-1}B^{-1}(\varphi) \in N$ — коммутатор матриц A и B. Докажем, что в N есть матрицы X со следом $\operatorname{tr} X \in [-1;3]$. Рассмотрим функцию $f(\varphi) = \operatorname{tr} C(\varphi)$. Имеем $f(0) = 3$, и $f(\varphi) < 3$ при $\varphi \neq 0$. Очевидно, что f непрерывна. Тогда в N есть матрицы со сколь угодно малым углом поворота ψ, так как $\cos\psi = \frac{\operatorname{tr} C - 1}{2}$. Но тогда есть и матрица с углом поворота $-\psi$. Значит, для любой матрицы D с углом поворота φ можно найти такую матрицу $G \in N$ и подходящую степень k, что $D = G^k$. Тем самым $N = \mathbf{SO}_3(\mathbb{R})$. ■

1.8. Действия групп на множествах

1.8.1. Понятие действия

Определение. *Действием* группы G на множестве $\mathcal{M}$ называется гомоморфизм $\rho\colon G \to \mathbf{S}_{\mathcal{M}}$, где $\mathbf{S}_{\mathcal{M}}$ — группа биективных отображений $\mathcal{M}$ на себя. Обозначение: $G\colon \mathcal{M}$. Ядро гомоморфизма ρ называется *ядром действия*. Действие называется *точным*, если $\operatorname{Ker}\rho = \{e\}$.

Иначе говоря, каждому элементу $g \in G$ ставится в соответствие некоторое преобразование $\rho(g)$ множества $\mathcal{M}$. При этом произведению элементов соответствует композиция преобразований, т. е. $\rho(gh) = \rho(g) \circ \rho(h)$. Из определения следует, что:

1° $\forall\, g, h \in G$, $\forall\, x \in \mathcal{M}$ имеем $(gh)x = g(hx)$, так как $(gh)x = \rho(gh)(x) = \big(\rho(g) \circ \rho(h)\big)(x) = \rho(g)(hx) = g(hx)$;

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

1.8.2. Орбиты и стабилизаторы

Определение. *Стабилизатором*[1] элемента $m \in \mathcal{M}$ называется подгруппа $\operatorname{St}(m) := \{g \in G\colon gm = m\}$.

Покажем, что это действительно подгруппа. Проверим свойства. Очевидно, $e \in \operatorname{St}(m)\,\forall\, m$. Произведение: если $g_1, g_2 \in \operatorname{St}(m)$, то $(g_1g_2)m = g_1(g_2m) = g_1m = m \Rightarrow g_1g_2 \in \operatorname{St}(m)$. Обратный элемент: $g \in \operatorname{St}(m) \Rightarrow gm = m$. Умножим равенство слева на g^{-1}. Тогда $m = g^{-1}m$, т. е. $g^{-1} \in \operatorname{St}(m)$.

Очевидно, что ядро действия есть пересечение всех стабилизаторов.

Определение. *Орбитой* элемента $m \in \mathcal{M}$ называется множество $\operatorname{Orb}(m) = Gm := \{gm \mid g \in G\}$. Точка m называется неподвижной точкой действия, если $\operatorname{Orb}(m) = \{m\}$. Мощность орбиты называется её *длиной*.

Утверждение 1.38. *Элементы орбиты находятся в биективном соответствии с левыми смежными классами по стабилизатору фиксированного элемента m.*

□ Имеем $gm = hm \Leftrightarrow (h^{-1}g)m = m \Leftrightarrow h^{-1}g \in \operatorname{St}(m) \Leftrightarrow g \in h\operatorname{St}(m)$. ■

Утверждение 1.39. *Любые две орбиты либо не пересекаются, либо совпадают.*

□ Орбита определяется одним элементом: $gm \in \operatorname{Orb}(m) \Rightarrow \operatorname{Orb}(gm) = G(gm) = (Gg)m = Gm = \operatorname{Orb}(m)$. ■

Следствие 1.6. *Имеется разбиение множества $\mathcal{M}$ на орбиты.*

Введём отношение эквивалентности: $m_1 \sim m_2 \Leftrightarrow m_1, m_2$ лежат на одной орбите $\Leftrightarrow \exists\, g\colon gm_1 = m_2$.

Определение. Пусть $H \subset G, g \in G$. Подгруппа gHg^{-1} называется *сопряжённой* с H.

Фиксируем некоторый элемент $m \in \mathcal{M}$, и рассмотрим стабилизатор элемента $gm \in \mathcal{M}$ для некоторого $g \in G$:

$$\operatorname{St}(gm) = \{h \in G\colon h(gm) = gm\} = \big\{h \in G\colon (g^{-1}hg)m = m\big\} \Leftrightarrow g^{-1}hg \in \operatorname{St}(m) \Leftrightarrow h \in g\operatorname{St}(m)g^{-1}.$$

Таким образом, $\operatorname{St}(gm) = g\operatorname{St}(m)g^{-1}$.

Следствие 1.7. *Если m и m' лежат на одной орбите, т. е. $m' = gm$, то их стабилизаторы сопряжены:*

$$\operatorname{St}(m') = g\operatorname{St}(m)g^{-1}.$$

[1] Иногда стабилизатор называют *стационарной подгруппой*.

Определение. Действие *транзитивно*, если его орбита единственна, т. е. $\forall\, m_1, m_2 \in \mathcal{M}\ \exists\, g\colon gm_1 = m_2$.

Итак, мы имеем разбиение множества $\mathcal{M} = \bigcup \mathrm{Orb}(m_i)$. Из утверждения 1.38 и теоремы Лагранжа следует, что

$$|\mathcal{M}| = \sum |\,\mathrm{Orb}(m_i)| = \sum \big(G : \mathrm{St}(m_i)\big), \tag{18}$$

так как длина орбиты элемента m_i равна числу левых смежных классов по $\mathrm{St}(m_i)$, то есть индексу $\mathrm{St}(m_i)$.

Пример 8.1. Группа $\mathbf{S}_n$ действует на множестве $\{1, \ldots, n\}$.

Пример 8.2. Группа $\mathbf{GL}_n(\mathbb{K})$ действует на $\mathbb{K}^n$.

1.8.3. Действия группы на себе. Централизаторы и нормализаторы

Можно также определить действие группы на самой себе (например, левыми сдвигами): $g \cdot x = gx$. Все действия, рассматриваемые выше, были левыми действиями. Правое действие: $g \cdot x = xg^{-1}$.

Определение. *Централизатором* элемента x называется множество $Z(x) := \{g \in G\colon xg = gx\}$.

Рассмотрим действие группы на себе сопряжениями: $g \cdot x = gxg^{-1}$. Тогда стабилизатором каждого элемента будет его централизатор, а орбиты превращаются в классы сопряжённости. Пусть $x \in G$, а $C(x)$ — класс сопряжённых ему элементов. Тогда $|C(x)| \cdot |Z(x)| = |G|$.

Теперь пусть M — множество всех подгрупп в G. Рассмотрим действие сопряжениями $g \cdot H = gHg^{-1}$. Тогда имеем $\mathrm{St}(H) = \big\{g\colon gHg^{-1} = H\big\}$. Подгруппа $\mathrm{St}(H)$ будет наибольшей подгруппой, в которой H нормальна. Она называется нормализатором H и обозначается $N(H)$.

Утверждение 1.40. *Число подгрупп, сопряжённых с данной, равно индексу её нормализатора.*

□ Длина орбиты равна числу подгрупп, сопряжённых с H. Остается применить формулу (18). ■

Пусть S — некоторое подмножество в G. Рассмотрим действие $g \cdot S = gS$. Тогда $H := \mathrm{St}(S) = \{h\colon hS = S\}$. Если $HS = S$, то S — объединение смежных классов по H.

1.9. Конечные p-группы. Теоремы Силова

1.9.1. Формула классов. Конечные p-группы

Определение. Группа G называется p-группой, если p — простое и $|G| = p^k$.

Пусть группа G разбита на классы сопряжённых элементов $x_1^G, \ldots, x_r^G$. Очевидно, что если $x \in Z(G)$, то $x^G = \{x\}$. Пусть $|Z(G)| = q$. Тогда получаем так называемую формулу классов:

$$|G| = |Z(G)| + \sum_{i=q+1}^{r} \frac{|G|}{|Z(x_i)|} = |Z(G)| + \sum_{i=q+1}^{r} |x_i^G|.$$

Теорема 1.41. *Всякая p-группа имеет нетривиальный центр.*

□ Если группа абелева, то тогда её центр есть вся группа. Если она не абелева, то в формуле классов размер каждого нецентрального класса делится на p. Тогда имеем $|G| = p^k = |Z(G)| + pm$, а значит, и $|Z(G)|$ делится на p, т. е. в центре кроме единицы ещё что-то есть. ■

Следствие 1.8. *Всякая p-группа разрешима.*

□ Докажем по индукции по порядку группы. Пусть $|G| = p^k$. Имеем $Z(G) \lhd G$. Тогда $|G/Z(G)| < |G|$, так как центр нетривиален. Факторгруппа имеет меньший порядок, и можно применить индукцию. ■

Теорема 1.42. *Всякая группа G порядка p^2 абелева.*

□ Центр G имеет порядок либо p, либо p^2. Во втором случае доказывать нечего, а иначе $|G/Z(G)| = p$, но факторгруппа неабелевой группы по центру не может быть циклической. Противоречие. ■

Рассмотрим несколько примеров p-групп.

Пример 9.1. Группа кватернионов $\mathbf{Q}_8$.

Пример 9.2. Группа унитреугольных матриц $\mathbf{UT}_3(\mathbb{F}_p)$.

1.9.2. Полупрямое произведение групп

Пусть $N \lhd G$, а H — подгруппа в G. Тогда произведение подгрупп NH является подгруппой, так как

$$(n_1h_1)(n_2h_2) = (n_1 \underbrace{h_1n_2h_1^{-1}}_{\in N})(h_1h_2) \in NH, \text{ и } (nh)^{-1} = \underbrace{h^{-1}n^{-1}h}_{\in N}h^{-1} \in NH.$$

Это обстоятельство позволяет дать следующее

Определение. Группа G есть *полупрямое произведение* подгрупп N и H (обозначение: $G = N \leftthreetimes H$), если:
1° $N \lhd G, H \subset G$;
2° $NH = G$;
3° $N \cap H = \{e\}$.

Замечание. Полупрямое произведение несимметрично!

Пусть $G = N \leftthreetimes H$. Для каждого $h \in H$ рассмотрим ограничение внутреннего автоморфизма $\Phi_h(x) := hxh^{-1}$ на подгруппу N. В силу нормальности подгруппы N получаем, что $\Phi_h \in \operatorname{Aut} N$ и отображение $h \mapsto \Phi_h$ является гомоморфизмом $H \to \operatorname{Aut} N$. Тогда умножение элементов из $N \leftthreetimes H$ происходит так:

$$(n_1h_1)(n_2h_2) = \big(n_1\Phi_{h_1}(n_2)\big)(h_1h_2).$$

Также можно определить внешнее полупрямое произведение. Пусть есть какие-то группы N и H, задан гомоморфизм $\varphi\colon H \to \operatorname{Aut} N$, и элемент $h \overset{\varphi}{\longmapsto} \Phi_h$. Определим в декартовом произведении $N \times H$ умножение по формуле $(n_1, h_1) \cdot (n_2, h_2) := \big(n_1\Phi_{h_1}(n_2), h_1h_2\big)$.

Очевидно, что аксиомы группы выполняются. Полученная группа и будет внешним полупрямым произведением групп $N \leftthreetimes H$. Аналогично прямому произведению, можно отождествить группы N и H с множествами пар $\{(n, e)\}$ и $\{(e, h)\}$ соответственно и не различать внешнее и внутреннее произведения.

Вернёмся к p-группам. Пусть $N = \langle a \rangle_{p^2}, H = \langle b \rangle_p$. Группа автоморфизмов циклической группы изоморфна группе обратимых элементов кольца вычетов $\mathbb{Z}/p^2\mathbb{Z}$, поэтому имеем $|\operatorname{Aut} N| = p(p-1)$. В $\operatorname{Aut} N$ есть элемент порядка p, следовательно, есть циклическая подгруппа порядка p. Значит, существует нетривиальный гомоморфизм $H \to \operatorname{Aut} N$ и можно построить полупрямое произведение $G = N \leftthreetimes H$ порядка p^3.

1.9.3. Теоремы Силова

Определение. Пусть $|G| = p^n m$, где p — простое и $(p, m) = 1$. Рассмотрим подгруппу $H \subset G$ порядка p^n. Она называется *силовской* p-подгруппой.

Теорема 1.43 (Первая теорема Силова). *Силовская p-подгруппа существует.*

□ Если группа G абелева, то разложим её на примарные циклические. Очевидно, что силовской p-подгруппой будет произведение всех тех слагаемых, порядки которых являются степенями числа p. В общем случае применим индукцию по $|G|$. Если $|G| = 1$, то доказывать нечего. Пусть $|G| > 1$. Рассмотрим разбиение G на классы сопряжённых элементов. Возможны 2 случая:

1° Есть нетривиальный класс $C(x)$, число элементов которого не делится на p. Тогда, так как $|Z(x)| \cdot |C(x)| = |G| = p^n m$, то $|Z(x)|$ делится на p^n. Порядок централизатора меньше $|G|$, значит, по индуктивному предположению в $Z(x)$ есть силовская p-подгруппа порядка p^n. Тогда она же будет искомой подгруппой в G.

2° Такого класса нет, т. е. количество элементов во всех нетривиальных классах делится на p. Тогда по формуле классов $|Z(G)|$ делится на p. Пусть $|Z(G)| = p^k l$, и $(p, l) = 1$. Тогда в центре $Z(G)$ есть подгруппа $Z' \subset Z(G)$ порядка p^k. Факторгруппа G/Z' имеет порядок $p^{n-k}m$, и снова по индуктивному предположению в ней есть подгруппа порядка p^{n-k}. Её полный прообраз при каноническом гомоморфизме $G \to G/Z'$ и будет силовской p-подгруппой в G. ■

Теорема 1.44 (Вторая теорема Силова). *Всякая p-подгруппа содержится в некоторой силовской p-подгруппе. Все силовские p-подгруппы сопряжены.*

□ Пусть $S \subset G$ — силовская p-подгруппа в G, и T — какая-то p-подгруппа. Рассмотрим действие T на факторможестве[1] G/S левыми сдвигами. При таком действии длина любой нетривиальной орбиты будет делиться на p, так как порядок стабилизатора делит порядок группы, и, стало быть, является некоторой степенью числа p. Заметим, что $|G/S|$ не делится на p. Значит, у данного действия есть неподвижные точки. Пусть gS — такая точка. Тогда $\forall\, t \in T$ имеем $t \cdot gS \subseteq gS$, т. е. $\forall\, s \in S \;\; tgs = gs'$. После преобразования этого равенства имеем

$$t = g\underbrace{s's^{-1}}_{\in S}g^{-1}, \text{ т. е. } t \in gSg^{-1} \Rightarrow T \subseteq gSg^{-1}.$$

Таким образом, первое утверждение доказано, так как gSg^{-1} будет некоторой силовской p-подгруппой. А если порядки у T и S совпадают, то $T = gSg^{-1}$, что и даёт сопряжённость всех силовских p-подгрупп. ■

Теорема 1.45 (Третья теорема Силова). *Число силовских p-подгрупп сравнимо с 1 по модулю p.*

□ Пусть S — силовская p-подгруппа в G и $C(S)$ — класс подгрупп, сопряженных с S, т. е. класс всех силовских p-подгрупп. Рассмотрим действие группы G сопряжениями на $C(S)$. При таком действии стабилизатор любой подгруппы S' равен её нормализатору $N(S')$. Ограничим это действие на S. Тогда всё множество $C(S)$

[1] G/S вовсе не обязано быть группой! (Прим. наб.)

разобьётся на нетривиальные орбиты (длина каждой из них делится на p, как и в теореме 1.44), и на неподвижные точки. Докажем, что единственной неподвижной точкой будет сама подгруппа S, откуда и будет следовать, что $|C(S)| \equiv 1 \pmod p$.

Пусть $S' \in C(S)$ — какая-то неподвижная точка. Это значит, что любой элемент из S действует на S' тождественно, то есть лежит в стабилизаторе $\mathrm{St}(S')$. Таким образом, $S \subset \mathrm{St}(S') = N(S')$. Тогда S и S' будут силовскими p-подгруппами в группе $N(S')$ и, значит, сопряжены в ней. Но S' — нормальная подгруппа в своём нормализаторе, то есть сопряжена только сама себе. Следовательно, $S' = S$. ■

Следствие 1.9. *Силовская подгруппа единственна $\Leftrightarrow$ она нормальна.*

Следствие 1.10. *Из сопряженности всех силовских p-подгрупп вытекает, что их количество N_p равно индексу нормализатора одной из этих подгрупп, т. е. если $|G| = p^n m$, то $N_p | m$.*

Следствие 1.11. *Если $\forall\, p_i || G|$ силовская подгруппа $G_{p_i} \lhd G$, то $G = G_{p_1} \times \ldots \times G_{p_q}$ и $|G| = |G_{p_1}| \ldots |G_{p_q}|$.*

□ Докажем, что пересечение каждой подгруппы с произведением остальных тривиально. Допустим противное. Пусть существует $x \in G$: $x = x_1 = x_2 \ldots x_q$, где $x_i \in G_{p_i}$. Тогда порядок элемента слева есть некоторая степень p_1, а у любого x_i справа порядок не может делиться на p_1. Противоречие. ■

1.9.4. Группы порядка pq

Рассмотрим группу G порядка pq, где p и q — простые, и $p < q$. Рассмотрим силовские q-подгруппы. По следствию 1.10 имеем $N_q | p$ и $N_q \equiv 1 \pmod p \Rightarrow N_q = 1$. Тогда по следствию 1.9 теорем Силова получаем, что $G_q \lhd G, |G_q| = q, |G/G_q| = p$, а значит, группа разрешима. Теперь рассмотрим силовские p-подгруппы. Имеем $N_p | q$ и $N_p \equiv 1 \pmod p$. Возможны 2 случая:

1° q не сравнимо с $1 \pmod p \Rightarrow N_p = 1 \Rightarrow G_p \lhd G \Rightarrow G = G_p \times G_q$ — циклическая группа.

2° $q \equiv 1 \pmod p$. Тогда покажем, что существует неабелева группа порядка pq. Возьмём группы N: $|N| = q$ и H: $|H| = p$. Имеем $\mathrm{Aut}\, N \cong \mathbb{F}_q^*$. Тогда $\mathrm{Aut}\, N$ содержит подгруппу порядка p и можно построить вложение $H \hookrightarrow \mathrm{Aut}\, N$ и получить тем самым внешнее полупрямое произведение групп $G = N \leftthreetimes H$.

2. Кольца. Поля. Алгебры

2.1. Основные понятия и теоремы

2.1.1. Кольца. Гомоморфизмы колец. Идеалы и факторкольца

Напомним, что кольцом называется множество $(R, +, \cdot)$ с двумя операциями. По сложению R есть абелева группа, а умножение дистрибутивно по отношению к сложению.

Определение. *Гомоморфизмом* колец R и S называется отображение f: $R \to S$ со следующими свойствами:
1° $f(a+b) = f(a) + f(b)$ для $\forall\, a, b \in R$;
2° $f(ab) = f(a)f(b)$ для $\forall\, a, b \in R$;
3° $f(1) = 1$ — это требование только для колец с 1. Если f сюръективно, то **3°** есть следствие **1°** и **2°**.

Будем пока рассматривать кольца с 1.

Пример 1.1. Рассмотрим кольцо квадратных матриц $\mathbf{M}_n$. В нём есть единица — единичная матрица. Рассмотрим теперь подкольцо $\mathbf{M}_{n-1} \subset \mathbf{M}_n$. Оно не является подкольцом с единицей, так как единичная матрица размерности $n-1$ *не совпадает* с единицей в всём кольце.

Рассмотрим гомоморфизм колец f, и обозначим $I := \mathrm{Ker}\, f$. Оно обладает двумя свойствами:
1° I - подгруппа по сложению;
2° $\forall\, x \in I,\ r \in R$ имеем $rx \in I,\ xr \in I$, так как $f(rx) = f(r)f(x) = 0 \Rightarrow rx \in I$, и аналогично $xr \in I$.

Определение. Подгруппа I аддитивной группы кольца R, удовлетворяющая этим двум свойствам, называется (*двусторонним*) *идеалом* кольца. Если идеал выдерживает только левое умножение, он называется левым идеалом. Аналогично определяется правый идеал. Обозначение: $I \lhd R$.

Замечание. Идеал является аналогом нормальной подгруппы в теории групп.

Определение. *Факторкольцом* кольца R по идеалу I называется множество $R/I := \{r + I \mid r \in R\}$ смежных классов по I.

Введём операцию умножения смежных классов по правилу $(a+I)(b+I) := ab + I$. Проверим корректность, т. е. что произведение не зависит от выбора представителя смежного класса. Пусть $a + I = a' + I,\ b + I = b' + I$. Докажем, что $ab + I = a'b' + I$. Пусть $a' = a + x,\ x \in I$; $b' = b + y,\ y \in I$. Тогда $a'b' = ab + \underbrace{ay + xb + xy}_{\in I}$, то есть R/I действительно является кольцом. Часто говорят, что R/I — кольцо вычетов по модулю I.

2.1.2. Основные теоремы о кольцах

Теорема 2.1 (О гомоморфизме колец). *Пусть $\varphi\colon A \to B$ — эпиморфизм колец, $\pi\colon A \to A/\operatorname{Ker}\varphi$ — канонический гомоморфизм. Тогда существует изоморфизм $\overline{\pi}\colon A/\operatorname{Ker}\varphi \to B$, такой, что $\varphi = \pi\overline{\pi}$.*

□ Для аддитивных групп существование искомого изоморфизма уже установлено. Проверим сохранение операции умножения. Пусть $\varphi(x) = u$ и $\varphi(y) = v$. Тогда $\varphi(xy) = uv$ и $\overline{\pi}(uv) = \pi(xy) = \pi(x)\pi(y) = \overline{\pi}(u)\overline{\pi}(v)$. ■

Для колец, как и для групп, верна

Теорема 2.2 (О соответствии). *Существует биекция между подкольцами в кольце, содержащими идеал, и всеми подкольцами в факторкольце по этому идеалу. Верно также, что если $I \subseteq J \lhd R$, то $R/J \cong \frac{R/I}{J/I}$.*

Утверждение 2.3. *Существует биекция между идеалами в R/I и идеалами в R, содержащими I.*

□ Пусть $\pi\colon R \to R/I$ — канонический гомоморфизм. Пусть $I \subseteq J \lhd R$, и $\overline{J} \lhd R/I$. Имеем $\overline{J} = J/I = \pi(J)$, $J = \pi^{-1}(\overline{J})$ — полный прообраз $\overline{J}$. ■

Теорема 2.4 (Об изоморфизме). *Пусть R — кольцо, K — его подкольцо и $I \lhd R$. Тогда*

$$(K + I)/I \cong K/(K \cap I). \tag{1}$$

□ Рассмотрим естественный эпиморфизм $\pi\colon R \to R/I$ и его ограничение $\pi_0 := \pi|_K$. Его образ состоит из смежных классов $x + I$, $x \in K$, т. е. $\operatorname{Im}\pi_0 = (K + I)/I$. Ядро $\operatorname{Ker}\pi_0$ состоит из всех тех элементов из K, для которых $x + I = I$. Значит, $\operatorname{Ker}\pi_0 = K \cap I$. По теореме о гомоморфизме получаем, что $(K + I)/I \cong K/(K \cap I)$. ■

Замечание. Идеал в кольцах без единицы является подкольцом. В кольцах с 1 очевидно, что если единица лежит в идеале, то он совпадает со всем кольцом. Очевидно также, что если некоторый обратимый элемент кольца лежит в идеале, то он также совпадает со всем кольцом: в самом деле, умножим такой элемент на обратный к нему, получим единицу. При этом по определению идеала результат умножения лежит в нём, т. е. $1 \in I$.

Определение. Кольцо называется *простым*, если в нём нет нетривиальных идеалов.

Пример 1.2. Примеры простых колец — поля и тела. Заметим, что вследствие простоты гомоморфизмы полей и тел будут вложениями.

2.1.3. Идеалы в кольце квадратных матриц

Теорема 2.5. *Пусть R — кольцо с 1. Для всякого идеала $I \lhd R$ имеем $\mathbf{M}_n(I) \lhd \mathbf{M}_n(R)$. Верно и обратное: любой идеал в кольце квадратных матриц $\mathbf{M}_n(R)$ есть кольцо матриц над некоторым идеалом кольца R.*

□ Первое утверждение теоремы очевидно и следует из правила умножения матриц. Докажем второе утверждение. Пусть M — идеал в $\mathbf{M}_n(R)$. Покажем, что $M = \mathbf{M}_n(I)$, где I — некоторый идеал в R. В самом деле, идеал M выдерживает левое и правое умножение, в частности, на матричные единицы E_{ij}. Рассмотрим матрицу $A = (a_{ij}) \in M$. Умножим её слева и справа на E_{ki} и E_{jl}. Получим $E_{ki}AE_{jl} = a_{ij}E_{kl}$. По определению идеала результат лежит в M, значит, вместе с матрицей A идеал M содержит все матрицы, составленные из её элементов, поставленных в произвольную строку и столбец. Рассмотрим множество всех чисел из R, которые могут составлять матрицы из M, и обозначим его через I. Покажем, что это идеал в R, т. е. покажем, что для $\forall\, a \in I$ верно $xa \in I$, $\forall\, x \in R$. Рассмотрим матрицу $aE_{ij} \in M$, причём i, j можно брать любыми. Так как M — идеал, то для $\forall\, x \in R$ имеем $(xa)E_{ij} \in M$. Значит, по определению множества I, число xa также лежит в I. Аналогично $ax \in I$, значит, I — идеал. ■

Следствие 2.1. *В частности, кольцо квадратных матриц над простым кольцом простое.*

Будем теперь рассматривать коммутативные кольца.

Утверждение 2.6. *Простое коммутативное кольцо с 1 является полем.*

□ Докажем, что каждый ненулевой элемент в таком кольце обратим. Пусть $x \in R$, $x \neq 0$. Тогда $xR = R$, так как кольцо простое. Следовательно, $\exists\, y\colon xy = 1$. Элемент y и будет обратным к x. ■

Определение. Идеал, порождённый одним элементом, называется *главным*. Кольцо, в котором все идеалы главные, называется *кольцом главных идеалов*.

Будем обозначать для краткости идеалы, порождённые элементом x, через (x), если из контекста ясно, о каком кольце идёт речь.

Утверждение 2.7. *Кольцо многочленов $\mathbb{K}[x]$ является кольцом главных идеалов.*

□ Пусть $I \lhd \mathbb{K}[x]$ и $f \in I$ — многочлен наименьшей степени. Докажем, что $I = (f)$. Очевидно, $(f) \subseteq I$. Докажем, что любой элемент $g \in I$ делится на f. Поделим g с остатком: $g = fq + r$. Многочлен $fq \in I \Rightarrow r \in I$. Но так как $\deg r < \deg f$, то $r = 0$. ■

Абсолютно также доказывается, что *любая евклидова область есть кольцо главных идеалов*.

2.2. Алгебры

2.2.1. Основные определения и примеры

Определение. *Алгеброй* над полем $\mathbb{K}$ называется множество $(R, +, *_R, *_{\mathbb{K}})$ с операциями сложения, умножения и умножения на элементы поля $\mathbb{K}$, обладающими следующими свойствами:

1° По сложению и умножению на элементы поля $\mathbb{K}$ множество R есть векторное пространство;

2° По сложению и умножению R есть кольцо;

3° $\forall\, \lambda \in \mathbb{K}, a, b \in R \;\; \lambda(ab) = (\lambda a)b = a(\lambda b)$.

Пример 2.1. $\mathbf{M}_n(\mathbb{K}), \mathbb{K}[x]$.

Определение. *Центром* кольца (алгебры) R называется подмножество $Z(R) := \{r \in R\colon rx = xr \,\forall\, x \in R\}$.

Заметим, что центр тела является полем.

Определение. Ненулевая алгебра называется *простой*, если ней нет нетривиальных идеалов.

Пусть R — алгебра над $\mathbb{K}$, и R обладает единицей. Тогда поле $\mathbb{K}$ вкладывается в $\mathbb{R}$ очевидным образом: $\lambda \mapsto \lambda \cdot 1$. Очевидно, что поле при этом оказывается в центре алгебры. Наоборот, если в $Z(R)$ содержится поле $\mathbb{K}$, то R — алгебра над $\mathbb{K}$.

Определение. *Идеал* алгебры — то же самое, что и идеал кольца, но он должен выдерживать умножение на элементы поля, т. е. быть подпространством.

Определение. *Гомоморфизмом* алгебр R и S над полем $\mathbb{K}$ называется отображение $f\colon R \to S$ со свойствами:

1° $f(x + y) = f(x) + f(y)$;

2° $f(xy) = f(x)f(y)$;

3° $f(\lambda x) = \lambda f(x) \;\; \forall\, x \in R,\; \lambda \in \mathbb{K}$.

Множество R является алгеброй с 1 над $\mathbb{K} \Leftrightarrow R$ — кольцо с 1 и $\mathbb{K} \subset Z(R)$. В одну сторону — очевидно, в другую — проверить аксиомы алгебры. Если алгебра с 1, то $f(\lambda \cdot 1) = \lambda \cdot f(1) = \lambda \in S$. Получаем следующее

Утверждение 2.8. *Если алгебра обладает единицей, то при гомоморфизме алгебр элементы поля отображаются тождественно. Верно и обратное: если f — гомоморфизм колец с 1 и он тождественно действует на элементы поля, то f является гомоморфизмом алгебр. В этом случае говорят, что f является гомоморфизмом над $\mathbb{K}$.*

Поскольку алгебра R есть векторное пространство над полем $\mathbb{K}$, можно выбрать базис: $R = \langle e_1, \ldots, e_n \rangle$. Зададим умножение на базисных векторах:

$$e_i e_j = \sum_{k=1}^{n} c_{ij}^k e_k.$$

Числа c_{ij} называются *структурными константами*.

Замечание. Задание структурных констант не гарантирует ассоциативности!

Пример 2.2. В матричной алгебре базис составляют матричные единицы.

2.2.2. Групповая алгебра конечной группы

Пусть дана конечная группа G. Занумеруем (формально) базисные векторы элементами группы: $\{e_g \mid g \in G\}$.

Определение. *Групповой алгеброй* группы G над полем $\mathbb{K}$ называется множество

$$\mathbb{K}G := \left\{ a = \sum_{g \in G} a_g e_g \;\middle|\; a_g \in \mathbb{K} \right\} \text{ с правилом умножения базисных векторов } e_g e_h = e_{gh}.$$

Обычно базисные элементы отождествляют с элементами группы, поэтому любой элемент алгебры записывается в виде $a = \sum\limits_{g \in G} a_g g$. Из ассоциативности умножения элементов группы следует ассоциативность умножения в алгебре.

Структурные константы алгебры зависят от базиса и являются тензорами типа $(2, 1)$. Умножение элементов алгебры R — билинейное отображение $m\colon R \times R \to R$, $m(x, y) = xy$. Сопоставим этому отображению трилинейное отображение $T\colon R \times R \times R^* \to \mathbb{K}$, $T(x, y, f) = f\big(m(x, y)\big)$.

2.2.3. Факторалгебра алгебры многочленов

Рассмотрим $\mathbb{K}[x]$. Возьмём идеал, порождённый ненулевым многочленом f степени n. Построим факторалгебру $\mathbb{K}[x]/(f) = \{g + (f)\}$. Каждый смежный класс, очевидно, содержит единственный многочлен степени меньше n. Поэтому факторалгебру можно отождествить (как множество) с множеством многочленов степени меньше n. Обозначим $\overline{g} := g + (f)$ — остаток от деления на f. Сумма и произведение остатков также есть

остаток, а значит, данное множество действительно является факторалгеброй. Базис её составляют многочлены $\{\overline{1}, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{n-1}\}$.

Утверждение 2.9. *Если R — конечномерная алгебра с 1 над $\mathbb{K}$, то всякий неделитель нуля обратим.*

□ Пусть $a \in R$ и a неделитель нуля. Зададим отображение $\varphi\colon R \to R$ по правилу $\varphi(x) = ax$. Оно невырожденно, а значит, сюръективно и $\exists\, y\colon y \mapsto 1 \Rightarrow ay = 1$. Аналогично найдём левый обратный элемент. ■

Следствие 2.2. *Конечномерная алгебра без делителей нуля является телом.*

□ Докажем, что в такой алгебре есть единица. Пусть α — неделитель нуля. Рассмотрим отображение $x \mapsto \alpha x$. Оно невырожденно, а потому сюръективно, и найдётся элемент $e\colon f(e) = \alpha$, т. е. $\alpha e = \alpha$. Заметим, что тогда выполняется и равенство $ex = x$, так как равенство $\alpha e = \alpha$ можно домножить на α справа, а затем заменить α в правой части на αe. Получим $\alpha e \alpha = \alpha\alpha e$, откуда $e\alpha = \alpha e$. Докажем, что для $\forall\, x \neq 0$ верно $xe = x$. Умножим равенство $e\alpha = \alpha$ слева на x и вынесем α за скобки. Получим $(xe - x)\alpha = 0 \Leftrightarrow xe - x = 0 \Leftrightarrow xe = x$. ■

Определение. Алгебра, являющаяся телом, называется *алгеброй с делением*.

Коммутативная конечномерная алгебра без делителей нуля является полем.

Вернёмся к алгебре многочленов. Если порождающий элемент f идеала (f) приводим, т. е. $f = gh$, то в факторалгебре есть делители нуля: $\big(g + (f)\big)\big(h + (f)\big) = f + (f) = (f) = \overline{0}$. Верно и обратное: если f неприводим, то делителей нуля нет, так как если бы $\big(g + (f)\big)\big(h + (f)\big) = \overline{0}$, то $gh \in (f) \Rightarrow f | gh$, т. е. $f | g$ или $f | h$.

2.3. Поля и их расширения

2.3.1. Расширения. Алгебраические и трансцендентные элементы

Определение. Говорят, что поле L есть *расширение* поля K, если $K \subset L$.

Если L — расширение K, то L является алгеброй над K.

Определение. Размерность расширения L как алгебры над K называется *степенью* расширения и обозначается $\dim_K L$ или $(L : K)$.

В частности, $K \subset K[x]/(f)$.

Теорема 2.10. *Пусть K — поле, и $f(x) \in K[x]$, $f(x) \neq \text{const}$. Тогда $\exists\, L \supset K$, в котором f имеет корень.*

□ Пусть $p(x)$ — неприводимый множитель $f(x)$. Рассмотрим факторкольцо $L := K[x]/(p)$. В силу неприводимости p оно будет полем. Пусть $\overline{x} = x + (p) \in L$. Тогда $p(\overline{x}) = p(x) + (p) = \overline{0}$, т. е. $\overline{x}$ — корень $p(x)$. ■

Определение. Дано расширение L поля K. Число $\alpha \in L$ называется *алгебраическим* элементом над K, если существует ненулевой многочлен $f \in K[x]$, такой, что $f(\alpha) = 0$, и *трансцендентным* в противном случае.

Можно рассмотреть наименьшее подполе в расширении L, содержащее K и корень α. Это будет поле рациональных функций.

Определение. Многочлен f называется *аннулирующим* для числа α, если $f(\alpha) = 0$.

Теорема 2.11. *Если расширение конечное, то любой элемент α в нём является алгебраическим.*

□ Пусть R — конечномерная алгебра с 1 и $K \subset R$. Покажем, что для α есть аннулирующий многочлен. Пусть степень расширения равна n. Тогда рассмотрим элементы $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$. Они линейно зависимы, т. е. $\exists\, \lambda_i \in K\colon \lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \ldots + \lambda_n\alpha^n = 0$. Значит, многочлен с коэффициентами λ_i и будет аннулирующим. ■

Очевидно, что множество всех аннулирующих многочленов для корня α является идеалом.

Определение. *Минимальный* многочлен корня α — его аннулирующий многочлен наименьшей степени.

Утверждение 2.12. *Пусть α — алгебраический элемент. Тогда его минимальный многочлен p неприводим.*

□ Пусть $p = gh$. Тогда $p(\alpha) = g(\alpha)h(\alpha) \Rightarrow g(\alpha) = 0$ или $h(\alpha) = 0 \;\Rightarrow\; \deg g, \deg h < \deg p$. Противоречие. ■

2.3.2. Простое расширение

Пусть L — расширение K, число $\alpha \in L$ — алгебраический элемент над K, и p — минимальный многочлен для α. Построим гомоморфизм $\varphi\colon K[x] \to L$. Положим $\varphi(x) := \alpha$, $\varphi(g(x)) = g(\alpha)$. По теореме о гомоморфизме имеем $\operatorname{Im}\varphi \cong K[x]/\operatorname{Ker}\varphi$. Ядро φ будет множеством всех аннулирующих многочленов, а тогда $\operatorname{Im}\varphi \cong K[x]/(p)$. Но мы знаем, что $K[x]/(p) = \{g(\overline{x}) \mid \deg g < \deg p\}$. Имеем $\overline{x} = x + (p) \mapsto \alpha \Rightarrow \operatorname{Im}\varphi$ — множество многочленов от α степени меньше $\deg p$. Это множество является полем и, кроме того, это наименьшее поле, содержащее K и α. Оно обозначается $K(\alpha)$ и называется простым расширением поля K. Итак, если p — минимальный многочлен для α, то $K(\alpha) \cong K[x]/(p)$.

Утверждение 2.13. *Пусть есть расширения L_1, L_2 поля K, $\alpha_1 \in L_1$, $\alpha_2 \in L_2$ и минимальные многочлены этих двух корней совпадают. Тогда $K(\alpha_1)$ и $K(\alpha_2)$ изоморфны как алгебры над K, т. е. существует изоморфизм $\varphi\colon \varphi(\alpha_1) = \alpha_2$, при котором элементы основного поля отображаются тождественно.*

□ $K(\alpha_1)$ и $K(\alpha_2)$ изоморфны одной и той же факторалгебре. Изоморфизм: $\varphi(g(\alpha_1)) := g(\alpha_2)$. ■

Пример 3.1. Пусть $z \in \mathbb{C},\ z \notin \mathbb{R},\ p(x) \in \mathbb{R}[x],\ p(z) = 0$. Тогда $\mathbb{R}[x]/(p) \cong \mathbb{R}(z) = \mathbb{C}$.

2.3.3. Башни полей

Будем рассматривать цепочки вложенных друг в друга полей — так называемые «башни полей».

Теорема 2.14. *Пусть $K \subset L \subset F$. Тогда $(F : K) = (L : K) \cdot (F : L)$.*

□ Выберем базис L над K: $\{\omega_1, \ldots, \omega_m\}$, и базис F над L: $\{\xi_1, \ldots, \xi_n\}$. Докажем, что всевозможные попарные произведения базисных векторов $\{\omega_i \xi_j\}$ образуют базис F над K. Любой элемент выражается:

$$u \in F, u = \sum_{j=1}^{n} x_j \xi_j,\ x_j \in L, \quad x_j = \sum_{i=1}^{m} a_{ij} \omega_i,\ a_{ij} \in K \ \Rightarrow\ u = \sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij} \omega_i \xi_j.$$

Линейная независимость: пусть $\sum\limits_{j=1}^{n} \underbrace{\sum\limits_{i=1}^{m} a_{ij} \omega_i}_{\in L} \xi_j = 0 \ \Rightarrow\ \forall j \ \sum\limits_{i=1}^{m} a_{ij} \omega_i = 0 \ \Rightarrow\ a_{ij} = 0$. Значит, это базис. ■

Следствие 2.3. *Пусть $\alpha_1, \ldots, \alpha_s \in L$ — алгебраические элементы над K. Рассмотрим наименьшее поле, содержащее K и все эти элементы: $K(\alpha_1, \ldots, \alpha_s) = K(\alpha_1)(\alpha_2) \ldots (\alpha_s)$. По предыдущей теореме полученное простое расширение имеет конечную степень над K.*

Следствие 2.4. *Множество всех алгебраических над K элементов в данном расширении является полем.*

□ Пусть α_1 и α_2 алгебраичны над K. Тогда $K(\alpha_1, \alpha_2)$ — конечное расширение, а по теореме 2.11 любой элемент в нём (в частности, сумма и произведение любых двух элементов) будет алгебраическим. ■

2.3.4. Поле разложения многочлена

Определение. *Полем разложения* многочлена f над K называется такое расширение $L \supset K$, что в $L[x]$ многочлен f разлагается на линейные множители, и L — наименьшее поле, содержащее все корни f.

Теорема 2.15. *Для любого многочлена f над полем K существует поле разложения.*

□ Докажем индукцией по степени f. Если $\deg f = 1$, то полем разложения будет поле K. Пусть $\deg f = n$ и для многочленов меньшей степени всё доказано. По теореме 2.10 существует поле $K_1 \supset K$, в котором f имеет корень (обозначим его α_1). Тогда над K_1 многочлен f имеет разложение $f(x) = (x - \alpha_1)g$, где $g \in K_1[x]$. Имеем $\deg g = n - 1$, и можно применить предположение индукции к g и полю K_1. Пусть K_2 — поле разложения для g. Тогда в нём он разлагается на линейные множители. Значит, и f разлагается в K_2 на линейные множители: $f(x) = \prod\limits_{i=1}^{n} (x - \alpha_i)$. Тогда $L := K(\alpha_1, \ldots, \alpha_n)$ будет искомым полем разложения. ■

2.3.5. Конечные поля

Пусть F — конечное поле характеристики p. Очевидно, что F содержит $\mathbb{F}_p$ — поле вычетов по модулю p и F является конечным расширением для $\mathbb{F}_p$. Пусть $(F : \mathbb{F}_p) = n$. Выберем базис $\{w_1, \ldots, w_n\}$, тогда любой элемент $x \in F$ записывается в виде $x = \sum a_i w_i,\ a_i \in \mathbb{F}_p$. Следовательно, $|F| = p^n$.

Поскольку $|F^*| = p^n - 1$, то для $\forall a \in F^*$ по теореме Лагранжа имеем $a^{p^n - 1} = 1$, то есть $a^{p^n} = a$. Таким образом, любой элемент поля F является корнем многочлена $f(x) := x^{p^n} - x \in \mathbb{F}_p[x]$, а значит, он разлагается над F на линейные множители. Следовательно, F — поле разложения $f(x)$.

Теорема 2.16. *Для любого простого числа p и любого числа $n \in \mathbb{N}$ существует поле из p^n элементов.*

□ Рассмотрим $\mathbb{F}_p \supset L$ – поле разложения многочлена $f(x) := x^{p^n} - x$ над $\mathbb{F}_p$. Заметим, что $f' = -1$, а значит, многочлен f взаимно прост со своей производной и потому не имеет кратных корней. Рассмотрим множество корней этого многочлена $\{\alpha_1, \ldots, \alpha_{p_n}\}$. Докажем, что они образуют искомое поле. В самом деле, пусть x, y — корни. Тогда $(x + y)^{p^n} = x^{p^n} + y^{p^n} = x + y$, т. е. число $x + y$ также является корнем. Аналогично $(xy)^{p^n} = x^{p^n} y^{p^n} = xy$. Очевидно, что если x — корень, то и x^{-1} — тоже корень. ■

Лемма 2.17. *Над полем $\mathbb{F}_p$ существуют неприводимые многочлены любой степени.*

□ Рассмотрим поле F из p^n элементов (мы уже знаем, что оно есть), и его мультипликативную группу F^*. Пусть $F^* = \langle \alpha \rangle$. Рассмотрим отображение $\varphi\colon \mathbb{F}_p[x] \to F$ по правилу $\varphi\colon f \mapsto f(\alpha)$. Поскольку $\varphi(0) = 0$, а $\varphi(x^k) = \alpha^k$, получаем, что φ – эпиморфизм. По теореме о гомоморфизмах колец имеем $\mathbb{F}_p[x]/\operatorname{Ker}\varphi \cong F$. Заметим, что $\operatorname{Ker}\varphi$ – главный идеал, порождённый некоторым неприводимым многочленом d. Действительно, если бы он был приводим, то факторкольцо $\mathbb{F}_p[x]/\operatorname{Ker}\varphi$ не было бы полем. Его степень будет в точности n. ■

Теорема 2.18. *Конечные поля, содержащие одинаковое число элементов, изоморфны между собой.*

□ Пусть $|F_1| = |F_2| = p^n$. Докажем, что $F_1 \cong F_2$. Пусть $F_1 = \mathbb{F}_p(\alpha),\ p(x)$ — минимальный многочлен для α степени n. Все элементы F_1 — корни многочлена $f(x) := x^{p^n} - x$, то есть он является аннулирующим

для α. Пусть $f(x)$ разлагается над $\mathbb{F}_p$ так: $f(x) = p(x)g(x)$. С другой стороны, в поле F_2 многочлен $f(x)$ также разлагается на линейные множители. Пусть β — некоторый корень $f(x)$ в поле F_2. Тогда $F_2 = \mathbb{F}_p(\beta)$. Таким образом, поля F_1 и F_2 содержат корни одного и того же многочлена, а значит, изоморфны. ■

Задача 2.1. *Доказать, что $n \mid \varphi(p^n - 1)$, где φ — функция Эйлера, а p — простое число.*

2.4. Алгебры с делением

2.4.1. Определения, примеры. Алгебры с делением над $\mathbb{C}$ и $\mathbb{R}$

Определение. *Алгеброй с делением* над полем $\mathbb{K}$ называется ассоциативная алгебра с единицей, в которой каждый ненулевой элемент обратим по умножению. Другими словами, алгебра с делением — это тело, являющееся алгеброй.

Задача 2.2. *Доказать, что центр простого кольца с единицей является полем.*

Утверждение 2.19. *Пусть R — алгебра с делением над полем $\mathbb{K}$. Тогда для любого элемента $\alpha \in R$ его минимальный многочлен неприводим над $\mathbb{K}$.*

□ От противного: пусть $p(x) = g(x)h(x)$. Тогда $p(\alpha) = g(\alpha)h(\alpha) = 0$, но так как делителей нуля нет, то либо $g(\alpha) = 0$, либо $h(\alpha) = 0$, т. е. есть аннулирующий многочлен меньшей степени. Противоречие. ■

Рассмотрим минимальную алгебру, содержащую поле $\mathbb{K}$ и элемент α, $p(x)$ — минимальный многочлен для α. Эта алгебра содержит все многочлены от α (линейные комбинации всех степеней α). Совокупность таких выражений будет подалгеброй (сумма и произведение элементов данного множества принадлежит этому же множеству — это следует из пункта **3°** определения алгебры). $\{f(\alpha)\} = \mathbb{K}(\alpha)$, $\mathbb{K}(\alpha) \cong \mathbb{K}[x]/(p)$. Но так как $p(x)$ неприводим, то $\mathbb{K}(\alpha)$ — поле.

Далее слово «алгебра» означает «алгебра с делением».

Теорема 2.20. *Всякая конечномерная алгебра над $\mathbb{C}$ совпадает с $\mathbb{C}$.*

□ Поле $\mathbb{C}$ алгебраически замкнуто, значит, неприводимыми являются только многочлены первой степени, а значит, минимальный многочлен любого элемента имеет вид $p(x) = x - z$. Если $p(\alpha) = 0$, то $\alpha = z \Rightarrow \alpha \in \mathbb{C}$. ■

Теорема 2.21. *Коммутативная конечномерная алгебра D над полем $\mathbb{R}$ совпадает либо с $\mathbb{R}$, либо с $\mathbb{C}$.*

□ Имеем $\mathbb{R} \subset D$. Рассмотрим произвольный элемент $\alpha \in D$ и его минимальный многочлен $p(x)$. Он либо линейный, либо квадратный (других неприводимых над $\mathbb{R}$ не бывает). Если для всех α минимальные многочлены линейны, то аналогично предыдущей теореме получаем, что $\alpha \in \mathbb{R}$ и $D = \mathbb{R}$. Если же среди минимальных многочленов есть квадратные, то $\mathbb{R}(\alpha) \cong \mathbb{R}[x]/(p) \cong \mathbb{C}$. ■

2.4.2. Тело кватернионов. Теорема Фробениуса

Поставим вопрос о том, можно ли построить алгебру над $\mathbb{R}$ размерности больше 2. Ответ: можно, но только она не будет коммутативной. Четырёхмерная алгебра над $\mathbb{R}$ называется алгеброй кватернионов и обозначается $\mathbb{H}$. Строится она следующим образом: берём векторное пространство $\mathbb{R}^4 = \langle 1, i, j, k\rangle$ и задаем умножение базисных векторов (структурных констант) так: $i^2 = j^2 = k^2 = -1$; $ij = k$, $jk = i$, $ki = j$; $ji = -k$, $kj = -i$, $ik = -j$, т. е. элементы антикоммутируют. Проверка ассоциативности неинтересна (хотя и нужна), и мы её здесь опустим. Сопряжённым к кватерниону $u = a + bi + cj + dk$ называют кватернион $\overline{u} = a - bi - cj - dk$. Нормой кватерниона u называется число $N(u) := u\overline{u} = a^2 = b^2 + c^2 + d^2$. Любой ненулевой элемент обратим, так как

$$u \cdot \frac{\overline{u}}{|u|^2} = 1.$$

Очевидно, что $\overline{u+v} = \overline{u} + \overline{v}$, $\overline{\overline{u}} = u$, $|u| \cdot |v| = |uv|$. А вот произведением сопряженных будет сопряженный к произведению в обратном порядке: $\overline{uv} = \overline{v} \cdot \overline{u}$. Таким образом, кватернионы образуют тело.

Замечание. Отображение $u \mapsto \overline{u}$ называют антиавтоморфизмом.

Теорема 2.22 (Фробениуса). *Любая конечномерная алгебра D с делением над $\mathbb{R}$ изоморфна либо $\mathbb{R}$, либо $\mathbb{C}$, либо $\mathbb{H}$.*

□ Рассмотрим центр алгебры $Z(D)$. Он является конечномерной коммутативной алгеброй над $\mathbb{R}$, и по теореме 2 изоморфен либо $\mathbb{R}$, либо $\mathbb{C}$. Во втором случае можно рассмотреть D как алгебру над $Z(D)$, и по теореме 1 получаем, что $D \cong \mathbb{C}$. В первом случае рассмотрим элемент $\alpha \notin Z(D) = \mathbb{R}$. Тогда имеем $\mathbb{R}(\alpha) = \mathbb{C}$, $\mathbb{C} \subset D$, $i \in \mathbb{C} \Rightarrow i \in D$. Рассмотрим D как векторное пространство над $\mathbb{C}$. Зададим умножение на скаляры: для $\forall\, u \in D$, $z \in \mathbb{C}$ положим $z \cdot u := zu$. Рассмотрим линейный оператор $\varphi\colon D \to D$, определённый по правилу $\varphi(u) := ui$. Проверим корректность: в силу ассоциативности имеем $\varphi(zu) = (zu)i = z(ui) = z\varphi(u)$, т. е. это действительно линейный оператор. Заметим, что $\varphi^2(u) = (ui)i = u(i^2) = -u$, поэтому $\varphi^2(u) + u = 0$, т. е. многочлен $t^2 + 1$ является аннулирующим для φ. Собственными значениями φ являются числа $\pm i$. Значит, D как векторное пространство есть прямая сумма собственных подпространств: $D = D_+ \oplus D_-$, и

$$D_+ = \{u \in D\colon \varphi(u) = iu\} = \{u \in D\colon ui = iu\}\,,$$
$$D_- = \{u \in D\colon \varphi(u) = -iu\} = \{u \in D\colon ui = -iu\}\,.$$

Таким образом, подпространство D_+ есть всё, что коммутирует с $\mathbb{C}$. Значит, D_+ есть подалгебра в D и она содержится в центре D, откуда вытекает, что $D_+ = \mathbb{C}$. Если подпространство D_- нулевое (т. е. D коммутативна), то $D = \mathbb{C}$. Если же D некоммутативна, то $D_- \neq \{0\}$. В этом случае докажем, что $D \cong \mathbb{H}$. Для этого рассмотрим элемент $h \in D_-,\ h \neq 0$. Пусть $u \in D_-$, тогда $i(uh) = -uih = uhi$, т. е. для $\forall\, u \in D_-$ имеем $uh \in D_+$. Теперь рассмотрим линейное отображение $\psi\colon D_- \to D_+$ над $\mathbb{C}$, определённое таким образом: $\psi(u) = uh$. Делителей нуля в алгебре нет, значит, $\operatorname{Ker}\psi = 0$ и это инъективное отображение. Таким образом, $\psi(D_-) \subset D_+$. Но D_+ одномерно, а значит, и $\psi(D_-)$ также одномерно, а потому $\psi(D_-) = D_+$. Теперь возьмём любой ненулевой элемент $h \in D_-$ в качестве базисного, тогда $D_- = \{zh\}_{z\in\mathbb{C}}$. Рассмотрим элемент $\psi(h) = h^2 \in D_+ = \mathbb{C}$. Этот элемент коммутирует с $\mathbb{C}$, а так как $D_- = \{zh\}$, то h^2 коммутирует и с D_-. Значит, $h^2 \in Z(D)$, то есть $h^2 =: a \in \mathbb{R}$. Но поскольку $h \notin \mathbb{R}$, то многочлен $x^2 - a$ будет минимальным для a и неприводимым над $\mathbb{R}$. Значит, $a < 0$. Теперь рассмотрим элемент $j := \frac{h}{\sqrt{|a|}}$. Имеем $j^2 = -1,\ j \in D_- \Rightarrow ij = -ji$. Любой элемент $u \in D$ однозначно записывается в виде $u = z_1 + z_2 j$, где $z_1, z_2 \in \mathbb{C}$. Пусть $z_1 = a + bi,\ z_2 = c + di$. Тогда $u = a + bi + cj + dij$. Обозначим $ij =: k$, получим, что $D \cong \mathbb{H}$ (все свойства легко проверить). ■

Замечание. Процесс расширения алгебр над $\mathbb{R}$ можно продолжать и дальше, однако 8-мерная алгебра над $\mathbb{R}$ неассоциативна, а 16-мерная имеет делители нуля.

Одним из важных утверждений, связанных с алгебрами над $\mathbb{R}$, является теорема о «причёсывании ежа»:[2]

Теорема 2.23. *Если существует n-мерная алгебра с делением, то сфера S^{n-1} параллелизуема, т. е. на ней существует касательное векторное поле без особых точек.*

2.4.3. Геометрические приложения кватернионов

Используем свойство $|uv| = |u||v|$. Рассмотрим сферу $S^3 := \{u \in \mathbb{H}\colon |u| = 1\}$. Она является группой по умножению.

Утверждение 2.24. $S^3 \cong \mathbf{SU}(2)$ — *группа двумерных унитарных матриц с определителем* 1.

□ Пусть $u \in S^3$. Имеем $u = a + bj,\ |a|^2 + |b|^2 = 1$. Построим изоморфизм по правилу $u \mapsto \begin{pmatrix} \overline{a}, & -\overline{b} \\ b, & a \end{pmatrix}$. ■

Найдём связь S^3 и $\mathbf{SO}_3$. Пусть $w \in \mathbb{H}, u \in S^3$. Учитывая то, что при этом $u^{-1} = \overline{u}$, рассмотрим отображение $\varphi_u(w) := uwu^{-1} = uv\overline{u}$. Оно сохраняет единицу и сохраняет длины векторов, значит, это ортогональный оператор. Отсюда получаем, что $\langle 1\rangle^\perp = \langle i, j, k\rangle =: V$, и $\dim_{\mathbb{R}} V = 3$, т. е., построено отображение $\varphi\colon S^3 \to \mathbf{O}(V)$. Множество S^3 линейно связно, а так как определитель линейного оператора на V есть непрерывная функция, то в $\operatorname{Im}\varphi$ все операторы имеют один и тот же определитель $\Rightarrow \operatorname{Im}\varphi \subseteq \mathbf{SO}_3$.

Задача 2.3. *Доказать, что на самом деле* $\operatorname{Im}\varphi = \mathbf{SO}_3$.

3. Модули над кольцами и алгебрами

3.1. Основные понятия

3.1.1. Модули, подмодули, гомоморфизмы модулей. Фактормодули

Определение. *Левым модулем* над кольцом R называется множество M с операциями сложения и умножения (слева) на элементы кольца. При этом должны выполняться аксиомы:

1°– **4°** $(M, +)$ — абелева группа;

5° $r(x + y) = rx + ry$ для $\forall\, x, y \in M,\ r \in R$;

6° $(r + s)x = rx + sx$ для $\forall\, x \in M,\ r, s \in R$;

7° $(rs)x = r(sx)$ для $\forall\, x \in M,\ r, s \in R$ (а для правых модулей — $x(rs) = (xr)s$);

8° Если R — кольцо с 1, то должно быть $1 \cdot x = x$ для $\forall\, x \in R$.

Определим модуль над алгеброй R над полем $\mathbb{K}$. К набору аксиом добавится ещё 2 условия: $(M, +, *_R, *_{\mathbb{K}})$ — векторное пространство над $\mathbb{K}$, и для $\forall\, x \in M,\ r \in R,\ \lambda \in \mathbb{K}$ выполняется равенство $r(\lambda x) = \lambda(rx) = (\lambda r)x$.

Замечание. Если алгебра обладает единицей, то последнее свойство выводится из остальных, так как поле $\mathbb{K}$ содержится в алгебре.

Определение. *Гомоморфизмом* левых R-модулей M и N называется такое отображение $\varphi\colon M \to N$, что:

1° $\varphi(x + y) = \varphi(x) + \varphi(y)$ для $\forall\, x, y \in M$;

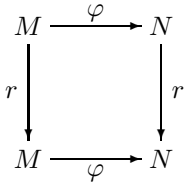
[2] Доказательства этой теоремы в нашем курсе не будет.

2° $\varphi(rx) = r\varphi(x)$ для $\forall\, x \in M,\ r \in R$.

Замечание. Алгебру можно рассматривать как левый (или правый) модуль над собой: $r \cdot x = rx \Rightarrow R$ — левый модуль, а если $r \cdot x = xr$, то правый.

Любой элемент r из кольца R задает линейный оператор на модуле M.

Определение. *Изоморфизмом* левых R-модулей M и N называется биективное отображение $\varphi\colon M \to N$, являющееся изоморфизмом векторных пространств. При этом $r\varphi(x) = \varphi(rx)$, т. е. диаграмма коммутативна:



Определение. *Подмодулем* N модуля M называется подмножество модуля M, замкнутое относительно сложения и умножения на элементы кольца (алгебры), т. е. выполнены свойства:

1° N — подгруппа по сложению;

2° $rx \in N \forall\, x \in N,\ r \in R$;

3° Если R — алгебра без 1, то требуем, чтобы N было подпространством: $\lambda x \in N$ для $\forall\, x \in N,\ \lambda \in \mathbb{K}$.

Определение. *Ядром* гомоморфизма φ называется множество $\operatorname{Ker}\varphi := \{x \in M\colon \varphi(x) = 0\}$. Оно, очевидно, является подмодулем.

Рассмотрим *смежные классы* в модуле M. Для $\forall\, y_0 \in \operatorname{Im}\varphi$ рассмотрим полный прообраз $\varphi^{-1}(y_0) = x_0 + N$, где $N = \operatorname{Ker}\varphi$. Легко видеть, множество таких классов является модулем.

Определение. Множество смежных классов $M/N := \{x + N \mid x \in M\}$ называется *фактормодулем*.

Умножение на элементы кольца в фактормодуле задаётся так: $r(x+N) = rx+N$. Корректность определения очевидна. Если R без 1, то определим умножение на скаляры: $\lambda(x+N) = \lambda x + N$. Как и в случае групп, можно рассматривать каноническую проекцию $\pi\colon M \to M/N\colon \pi(x) = x + N$.

3.1.2. Основные теоремы о модулях

Теорема 3.1 (О гомоморфизме). *Пусть $f\colon M \to N$ — гомоморфизм R-модулей, $\pi\colon M \to M/\operatorname{Ker} f$ — канонический гомоморфизм. Тогда существует изоморфизм $\varphi\colon \operatorname{Im} f \to M/\operatorname{Ker} f$, такой, что $f = \varphi \circ \pi$.*

□ Мы уже знаем, что между фактормодулем и $\operatorname{Im} f$ имеется изоморфизм групп. Проверим коммутирование φ с умножением на элементы кольца R. Пусть $f(x) = y$. Тогда $f(rx) = ry$, и $\varphi(ry) = \pi(rx) = r\pi(x) = r\varphi(y)$. ■

Теорема 3.2 (О соответствии). *Имеется биективное соответствие между подмодулями в фактормодуле по $\operatorname{Ker} f$ и подмодулями в исходном модуле, содержащими $\operatorname{Ker} f$.*

Теорема 3.3 (Об изоморфизме). *Пусть P, Q — подмодули в M. Тогда $(P+Q)/Q \cong P/(P \cap Q)$.*

3.2. Прямые суммы и ряды модулей. Системы порождающих модуля

3.2.1. Прямые суммы модулей

Определение. Пусть $Q_1, \ldots, Q_s$ — подмодули в M. Говорят, что M — *прямая сумма* $Q_1, \ldots, Q_s$, если M как абелева группа есть прямая сумма подгрупп Q_i. Это эквивалентно тому, что любой элемент $x \in M$ записывается однозначно в виде суммы $x = x_1 + \ldots + x_s$, где $x_i \in Q_i$. Обозначение: $M = Q_1 \oplus \ldots \oplus Q_s$.

Умножение на скаляр в прямой сумме почленное, так как слагаемые являются подмодулями: $rx = rx_1 + \ldots + rx_s$. Аналогично группам определяется внешняя прямая сумма. Если R — алгебра, то прямая сумма модулей будет прямой суммой подпространств.

3.2.2. Ряды подмодулей. Простые модули

Рассмотрим ряд вложенных модулей $M = M_0 \supset M_1 \supset \ldots \supset M_s = \{0\}$. Рассмотрим фактормодули M_i/M_{i+1}.

Определение. Ненулевой модуль называется *простым*, если в нём нет нетривиальных подмодулей (отличных от нуля и его самого). Простые модули иногда называют *неприводимыми*.

Определение. Ряд из модулей называется *композиционным*, если все его факторы — простые модули.

Для модулей имеет место

Теорема 3.4 (Жордана – Гёльдера). *Если модуль обладает композиционным рядом, то любой его ряд уплотняется до композиционного, все композиционные ряды имеют одинаковую длину и факторы этих рядов изоморфны после некоторой перестановки.*

Следствие 3.1. *Пусть есть 2 разложения модуля на простые: $M = Q_1 \oplus \ldots \oplus Q_s = P_1 \oplus \ldots \oplus P_t$. Тогда $s = t$ и слагаемые изоморфны после некоторой перестановки.*

□ Рассмотрим ряд подмодулей в M:

$$M = M_0 \supset \underbrace{(Q_2 \oplus \ldots \oplus Q_s)}_{M_1} \supset \underbrace{(Q_3 \oplus \ldots \oplus Q_s)}_{M_2} \supset \ldots \underbrace{(Q_s)}_{M_{s-1}} \supset \{0\}.$$

Факторы этого ряда будут простыми по условию: $M_{i-1}/M_i \cong Q_i$. Аналогичным образом построим ряд из P_i. Остается лишь применить теорему Жордана – Гёльдера. ■

Определение. *Длиной* модуля называется длина его композиционного ряда.

Замечание. Векторное пространство — частный случай модуля, его размерность совпадает с длиной.

3.2.3. Системы порождающих модуля. Циклические модули

Начиная с этого момента все рассматриваемые кольца и алгебры — с единицей.

Определение. Пусть $Q \subset M$. Система $S \subset Q$ называется *системой порождающих* для Q, если любой элемент $x \in Q$ записывается в виде $x = r_1x_1 + \ldots + r_kx_k$, где $x_i \in S,\ r_i \in R$. Обозначение: $Q = \langle S \rangle = \{\sum r_ix_i \mid x_i \in S,\ r_i \in R\}$. Если порождающее семейство конечно, модуль называется *конечнопорождённым*.

Кольцо — частный случай модуля, идеалы кольца — подмодули, поэтому можно говорить о системе порождающих для левых идеалов. Пусть N — левый идеал в R. Система $S \subset N$ будет системой порождающих для N, если $N = \langle S \rangle$. Очевидно, что любая система S порождает некоторый левый идеал.

Определение. Подмодуль, порождённый одним элементом a, называется *циклическим*: $M = \{ra \mid r \in R\}$.

Пример 2.1. В кольце циклическими подмодулями будут главные левые идеалы.

Если M — циклический модуль, то и M/Q — также циклический: $M = \langle a \rangle \Rightarrow M/Q = \langle a + Q \rangle$. Очевидно также, что любой простой модуль является циклическим.

Теорема 3.5. *Всякий циклический R-модуль M изоморфен модулю вида R/I, где I — левый идеал в R.*

□ Пусть $M = \langle a \rangle$. Рассмотрим гомоморфизм $\varphi\colon R \to M$, при котором $\varphi(r) = ra$. Очевидно, что φ сюръективен. По теореме о гомоморфизме $M \cong R/I$, где $I = \operatorname{Ker}\varphi$. ■

Пример 2.2. Любая абелева группа является $\mathbb{Z}$-модулем. Циклические подмодули в ней — циклические подгруппы.

3.3. Свободные модули. Конечнопорождённые модули над кольцом многочленов

3.3.1. Свободные модули

Пусть $V = \langle e_1, \ldots, e_n \rangle_R$ — конечномерное векторное пространство над R. В нём любой элемент однозначно выражается через базис. Однако в случае модулей базис есть не всегда.

Определение. R-модуль M называется *свободным*, если в нём существует такая система порождающих $e_1, \ldots, e_n$, что любой элемент $x \in M$ однозначно представляется в виде $x = r_1e_1 + \ldots + r_ne_n$, где $r_i \in R$, т. е. модуль обладает базисом.

Пример 3.1. Кольцо R, как левый модуль над собой, обладает базисом: $R = \langle 1 \rangle$, а значит, является свободным.

Пусть есть свободный R-модуль $M = \langle e_1, \ldots, e_n \rangle$. Имеем $R \cong \langle e_i \rangle$ (изоморфизм очевиден: $r \to re_i$). Тогда получаем, что $M = \langle e_1 \rangle \oplus \ldots \oplus \langle e_n \rangle \Rightarrow$ *прямая сумма нескольких экземпляров кольца есть свободный модуль.*

Теорема 3.6. $\forall$ *конечнопорождённый модуль изоморфен фактормодулю свободного модуля по некоторому подмодулю.*

□ Пусть $M = \langle a_1, \ldots, a_n \rangle$. Рассмотрим свободный модуль $F = \langle e_1, \ldots, e_n \rangle$. Рассмотрим гомоморфизм $\varphi\colon F \to M$, ставящий в соответствие элементу $x = r_1e_1 + \ldots + r_ne_n \in F$ элемент $\varphi(x) = r_1a_1 + \ldots + r_na_n$. Поскольку F свободен, то отображение задано корректно. Элементы a_i — порождающие $\Rightarrow \varphi$ сюръективен. Обозначая $Q := \operatorname{Ker}\varphi$, получаем, что $M \cong F/Q$. ■

3.3.2. Конечнопорождённые модули над кольцом многочленов

Рассмотрим алгебру многочленов $R := \mathbb{K}[\lambda]$. Рассмотрим модуль V над R. Для этого V должно быть векторным пространством над $\mathbb{K}$, и нужно для $\forall\, x \in V$ задать умножение на λ, т. е. определить линейное отображение (оператор) $x \to \lambda \cdot x$. Наоборот, если задано векторное пространство V над $\mathbb{K}$ и оператор φ, тогда V естественным образом становится модулем над R: зададим умножение на элементы R по правилу $f(\lambda) \cdot x := f(\varphi)x$, где $x \in V,\ f \in \mathbb{K}[\lambda]$, т. е. подействуем на x многочленом от оператора.

Теперь рассмотрим некоторый набор многочленов $f_1, \ldots, f_k \in \mathbb{K}[\lambda]$ и идеал, порождённый этими многочленами: $\langle f_1, \ldots, f_k \rangle = \{g_1(\lambda)f_1 + \ldots + g_k(\lambda)f_k\}$. Поскольку этот идеал главный, то он порождается одним элементом и равен $d(x)\mathbb{K}[\lambda]$, где $d(x) = \text{НОД}(f_1, \ldots, f_k)$.

Рассмотрим $R = \mathbb{K}[\lambda]$ — свободный циклический бесконечномерный модуль и циклический модуль M, который изоморфен фактормодулю свободного модуля: $M \cong \mathbb{K}[\lambda]/(f)$, где $f \in \mathbb{K}[\lambda],\ f \neq 0$. Пусть $\deg f = n$, тогда $\dim_{\mathbb{K}} M = n$. Это число называется порядком модуля.

Определение. Конечномерный циклический R-модуль называется *примарным*, если $f(\lambda) = p(\lambda)^k$ — степень неприводимого многочлена.

Лемма 3.7. *Если u, v — взаимно простые элементы кольца R главных идеалов, то $R/(uv) \cong R/(u) \oplus R/(v)$.*

□ Рассмотрим отображение $f\colon R \to R/(u) \oplus R/(v)$, определённый так: $x \xmapsto{f} \big(x+(u), x+(v)\big)$. Оно является гомоморфизмом колец. По условию существуют элементы кольца a, b такие, что $au + bv = 1$. Тогда

$$f(bv) = \big(bv + (u), bv + (v)\big) = \big(1 - au + (u), 0 + (v)\big) = \big(1 + (u), 0 + (v)\big), \text{ и аналогично } f(au) = \big(0 + (u), 1 + (v)\big).$$

Значит, f сюръективен. Очевидно, что $\operatorname{Ker} f = (uv)$. Остается применить теорему о гомоморфизме. ■

Теорема 3.8. *Пусть M — циклический модуль над $\mathbb{K}[\lambda]$, и $M = \mathbb{K}[\lambda]/(f)$. Пусть $f = gh$, и g, h взаимно просты. Тогда $M \cong \mathbb{K}[\lambda]/(g) \oplus \mathbb{K}[\lambda]/(h)$.*

□ Очевидно, что выполняются условия леммы ($\mathbb{K}[x]$ — кольцо главных идеалов). Изоморфизм, построенный при доказательстве леммы, является и изоморфизмом модулей. Теорема доказана. ■

Следствие 3.2. *Любой конечномерный циклический модуль изоморфен прямой сумме примарных циклических модулей. Прямая сумма конечномерных циклических модулей является циклическим модулем $\Leftrightarrow$ их порядки взаимно просты.*

Замечание. Всё это верно только для модулей над кольцом многочленов.[3]

Теорема 3.9. *Всякий конечнопорождённый модуль M над $R := \mathbb{K}[\lambda]$ есть прямая сумма конечного числа бесконечномерных циклических модулей и конечного числа примарных циклических модулей.*

□ Докажем по аналогии с абелевыми группами. Пусть $M = \langle a_1, \ldots, a_n \rangle$, и $F = \langle x_1, \ldots, x_n \rangle$ — свободный модуль. Мы знаем, что $\exists Q\colon M \cong F/Q$. Пусть $Q = \langle b_i \rangle_{i \in I}$, где $b_j = b_{1j}e_1 + \ldots + b_{nj}e_n$ — соотношения между a_i. Составим матрицу $B = (b_{ij})$ размера $n \times I$. Приведём её с помощью элементарных преобразований и алгоритма Евклида к диагональному виду, осуществляя соответствующие замены базиса: $B' = \operatorname{diag}(b'_1, \ldots, b'_n)$. Новые базисы будут иметь вид $F = \langle e'_1, \ldots, e'_n \rangle,\ Q = \langle b'_1 e'_1, \ldots, b'_n e'_n \rangle$. Тогда $F = Re'_1 \oplus \ldots \oplus Re'_n,\ Q = Rb'_1 e'_1 \oplus \ldots \oplus \oplus Rb'_n e'_n$. Отсюда следует, что $F/Q \cong R/(b'_1) \oplus \ldots \oplus R/(b'_n)$. Заметим, что если в каком-то слагаемом $b_i = 0$, то оно будет бесконечномерным. ■

Имеет место и теорема о единственности такого разложения.

3.3.3. Альтернативное доказательство теоремы о жордановом базисе

Применим нашу теорию для конечномерного векторного пространства V, на котором задан оператор φ. Рассмотрим V как модуль над $\mathbb{K}[\lambda] =: R$, задав умножение на скаляры так: $\lambda \cdot x := \varphi(x)$, т. е. $f(\lambda) \cdot x = f(\varphi)x$. Пусть $V = \langle e_1, \ldots, e_n \rangle_{\mathbb{K}}$, оператор φ имеет матрицу $A = (a_{ij})$. Тогда

$$\lambda \cdot e_j = \varphi(e_j) = a_{1j}e_1 + \ldots + a_{nj}e_n,\ j = \overline{1,n} \ \Rightarrow\ a_{1j}e_1 + \ldots + (a_{jj} - \lambda)e_j + \ldots + a_{nj}e_n = 0.$$

Пусть $F = \langle u_1, \ldots, u_n \rangle_{\mathbb{K}[\lambda]}$ — свободный R-модуль. Представим V как фактормодуль свободного модуля: $V = F/N$ и рассмотрим канонический гомоморфизм $\pi\colon F \to V\colon \pi(u_i) = e_i$. Имеем $\operatorname{Ker}\pi = N$. Рассмотрим элементы $y_j := a_{1j}u_1 + \ldots + (a_{jj} - \lambda)u_j + \ldots + a_{nj}u_n \in N$. Покажем, что $\{y_j\}$ есть набор определяющих соотношений, т. е. что они порождают N. Возьмём их линейную оболочку $N' := \langle y_1, \ldots, y_n \rangle_{\mathbb{K}[\lambda]}$ и докажем, что она совпадает с N. Очевидно, что $N' \subseteq N$. Рассмотрим гомоморфизм $F/N' \to F/N \cong V$, при котором $h + N' \mapsto h + N$. Покажем, что F/N' как векторное пространство имеет размерность n (достаточно показать, что она не превосходит n). Имеем $\lambda u_j = a_{1j}u_1 + \ldots + a_{nj}u_n - y_j$. Значит, если вместо λ подставить произвольный многочлен $f(\lambda)$, то получается, что $f(\lambda)u_j \in \langle u_1, \ldots, u_k \rangle_{\mathbb{K}} + N'$. Тогда $\forall\, x \in F$ лежит в $\langle u_1, \ldots, u_k \rangle_{\mathbb{K}} + N'$, так как $x = \sum f_i(\lambda)u_i$. Значит, если $\overline{x} \in F/N'$, то $\overline{x} \in \langle \overline{u_1}, \ldots, \overline{u_n} \rangle_{\mathbb{K}}$, т. е. факторпространство F/N' есть линейная оболочка n векторов $\Rightarrow \dim_{\mathbb{K}} F/N' \leqslant n$. Таким образом, $N' = N$.

Теперь представим модуль V в виде суммы циклических модулей. Для этого приведём матрицу определяющих соотношений (это в точности $A - \lambda E$) к диагональному виду:

[3] На самом деле не только над $\mathbb{K}[x]$. См. Э. Б. Винберг. «Курс алгебры». Стр. 368-369 (Прим. наб.)

$$\begin{pmatrix} a_{11}-\lambda & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn}-\lambda \end{pmatrix} \rightsquigarrow \begin{pmatrix} d_1(\lambda) & & 0 \\ & \dots & \\ 0 & & d_n(\lambda) \end{pmatrix}.$$

При этом $d_1(\lambda)|\dots|d_n(\lambda)$. Таким образом, $V \cong \mathbb{K}[x]/(d_1) \oplus \dots \oplus \mathbb{K}[x]/(d_n)$. В данном случае $d_i \neq 0$, так как пространство конечномерное. Заметим, что характеристический многочлен оператора $\chi_\varphi(\lambda)$ с точностью до константы равен $d_1(\lambda)\dots d_n(\lambda)$. Минимальный многочлен для φ делится на все $d_i \Rightarrow$ он равен $d_n(\lambda)$. Теперь дорасложим каждое слагаемое в сумму примарных циклических модулей: $d_j(\lambda) = \prod\limits_{i=1}^{s_j} p_{ji}(\lambda)^{k_{ji}}$, где p_{ij} неприводимы.

Итак, мы перешли к новым базисам в F и в N следующего вида: $F = \langle u'_1, \dots, u'_n\rangle$, $N = \langle y'_1, \dots, y'_n\rangle$, $y'_j = d_j(\lambda)u'_j$. Порождающие циклических модулей — это образы $\overline{u'}_j$ элементов u'_j в пространстве V (это не обязательно векторный базис!). Выразим $\overline{u'}_j$ через u'_j:

$$\left(\begin{array}{ccc|ccc} a_{11}-\lambda & \dots & a_{1n} & 1 & & 0 \\ & & & & \ddots & \\ a_{n1} & \dots & a_{nn}-\lambda & 0 & & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} d_1(\lambda) & & 0 & \\ & \dots & & C^{-1} \\ 0 & & d_n(\lambda) & \end{array}\right).$$

Матрица в правой части после приведения матрицы $A-\lambda E$ к диагональному виду будет обратной к матрице перехода к новому базису в F.

Отсюда получается теорема Жордана: Пусть $\mathbb{K} = \mathbb{C}$. Тогда неприводимыми будут только линейные многочлены вида $\lambda - \lambda_i$. Следовательно,

$$V \cong \mathbb{K}[x]\Big/\big((\lambda-\lambda_1)^{k_1}\big) \oplus \dots \oplus \mathbb{K}[x]\Big/\big((\lambda-\lambda_s)^{k_s}\big) = \langle e_1, \dots, e_s\rangle.$$

Векторный базис каждой жордановой клетки — $\big\{e_i, (\lambda-\lambda_i)e_i, \dots, (\lambda-\lambda_i)^{k_i-1}e_i\big\}$. Вид матрицы в силу единственности разложения определён однозначно с точностью до перестановки клеток.

3.4. Прямые произведения колец (алгебр) и модулей над ними

3.4.1. Прямые произведения колец

Пусть R — кольцо с 1, $I_1, \dots, I_s$ — его идеалы.

Определение. Кольцо R есть *прямое произведение* $I_1, \dots, I_s$, если R как абелева группа есть прямая сумма: $R = I_1 \oplus \dots \oplus I_s$. Обозначение: $R = I_1 \times \dots \times I_s$.

Из определения следует, что $I_i \cap I_j = \{0\}$. Если $x_i \in I_i$, $x_j \in I_j \Rightarrow x_ix_j \in I_i \cap I_j \Rightarrow x_ix_j = 0$. Значит, произведение элементов прямого произведения — покомпонентное:

$$x = x_1 + \dots + x_s, \quad y = y_1 + \dots + y_s \;\Rightarrow\; xy = x_1y_1 + \dots + x_sy_s. \tag{1}$$

Представим единицу в виде суммы: $1 = e_1 + \dots + e_s$, где $e_i \in I_i$. Тогда $x_i = x_ie_i = e_ix_i$, т. е. элементы e_i являются единицами для соответствующих подгрупп (однако I_i будут всего лишь подгруппами по сложению, а не подкольцами в R, так как $e_i \neq 1$). Заметим также, что $e_i^2 = e_i$, а $e_ix_j = x_je_i = 0$, если $i \neq j$. Таким образом, получаем свойства системы элементов e_i:

1° $e_i^2 = e_i$ (идемпотентность);
2° $e_ie_j = 0$, $i \neq j$ (ортогональность);
3° $e_i + \dots + e_s = 1$ (полная система);
4° $e_i \in Z(R)$.

Наоборот, если задана полная система ортогональных идемпотентов, то $I_i := e_iR = Re_i$ — идеал в R, и тогда $R = I_1 \oplus \dots \oplus I_s$.

Теперь определим внешнее произведение. Рассмотрим декартово произведение $R = R_1 \times \dots \times R_s$, введём операции (покомпонентно). Рассмотрим $I_i = \{(0, \dots, 0, x_i, 0, \dots, 0)\}$, где $x_i \in R$. Очевидно, что I_i будет идеалом. Значит, можно не различать внешнее и внутреннее произведения.

Пример 4.1. $R = \mathbb{K}[x]/(f)$, $f = g_1 \dots g_s$, и $(g_i, g_j) = 1$ для $i \neq j$. Рассмотрим кольца $R_i := \mathbb{K}[x]/(g_i)$. Тогда $(f) \subseteq (g_i)$. Рассмотрим отображения $\varphi_i\colon \mathbb{K}[x] \to R_i$. Построим отображение $\varphi\colon \mathbb{K}[x] \to R_1 \times \dots \times R_s$, заданное по правилу $\varphi(h) := \big(\varphi_1(h), \dots, \varphi_s(h)\big)$. Каждому многочлену сопоставим набор его классов вычетов по модулю g_i. По китайской теореме об остатках оно будет сюръективным, так как для любого набора остатков найдётся элемент, которой при делении на заданный набор элементов даёт эти остатки. А тогда по теореме о гомоморфизме $\mathbb{K}[x]/\operatorname{Ker}\varphi \cong R_1 \times \dots \times R_s$. Но ядро состоит в точности из тех многочленов, которые делятся на каждый из g_i, т. е. $\operatorname{Ker}\varphi = (f)$. Значит, $R \cong \prod\limits_{i=1}^{s} R_i$.

Пример 4.2. Множество блочно-диагональных матриц над полем $\mathbb{K}$ образует алгебру. Идеалами, очевидно, будут матрицы, в которых в одном из блоков стоит произвольная подматрица, а все остальные блоки нулевые. Вся алгебра будет произведением таких идеалов.

Утверждение 3.10. *Центр прямого произведения колец равен произведению их центров.*

□ Пусть $R = R_1 \times \ldots \times R_s,\ x = (x_1, \ldots, x_s),\ y = (y_1, \ldots, y_s)$. Умножение покомпонентное, следовательно, $xy = yx \Leftrightarrow x_i y_i = y_i x_i \,\forall\, i$. Это и означает, что $Z(R) = Z(R_1) \times \ldots \times Z(R_s)$. ■

Утверждение 3.11. *Дан модуль M над прямым произведением колец $R = R_1 \times \ldots \times R_s$. Тогда M однозначно разлагается в прямую сумму $M = M_1 \oplus \ldots \oplus M_s$, где M_i — модуль над R_i, и $y_j M_i = 0$ для $\forall\, y_j \in R_j$ при $i \neq j$.*

□ В силу наличия прямого произведения колец имеем разложение для единицы: $1 = e_1 + \ldots + e_s$, где e_i — единицы в R_i. Положим $M_i = e_i M$. Покажем, что M_i будут подмодулями. Поскольку $e_i \in Z(R)$, то для $\forall\, r \in R$, $\forall\, x_i = e_i x$, где $x \in M$, имеем $r x_i = r e_i x = e_i r x \in M_i$. Если $x_i \in M_i$, то $x_i = e_i x$, и $e_i x_i = e_i^2 x = e_i x$, т. е. M_i — подмодуль. Пусть $y_j \in R_j,\ x_i = e_i x \in M_i$. Тогда при $j \neq i$ получаем, что $y_i x_i = \underbrace{y_i e_i}_{0} x = 0$, и следовательно, $M_i \cap \sum\limits_{i \neq j} M_j = \{0\}$. Теперь представим любой элемент $x \in M$ в виде суммы. Имеем $x = 1 \cdot x = (e_1 + \ldots + e_s)x = e_1 x + \ldots + e_s x$. Значит, M есть прямая сумма M_i. ■

Обратно, пусть заданы модули M_i над каждым R_i. Построим из них прямую сумму M. Для $\forall\, r_j \in R_j,\ x_i \in M_i$ при $i \neq j$ положим $r_j x_i = 0$. Определим действие $r = (r_1, \ldots, r_s)$ на $x \in M$ так: $r \cdot x_i := r_i x_i$. Тогда $M = M_1 \oplus \ldots \oplus M_s$.

Следствие 3.3. *Пусть задан простой модуль над прямым произведением. Тогда он совпадает с модулем над одним из множителей.*

3.4.2. Модули над конечномерными алгебрами

Утверждение 3.12. *Пусть R — конечномерная алгебра над $\mathbb{K}$, и V — конечнопорождённый R-модуль. Тогда V — конечномерное векторное пространство.*

□ Пусть $V = \langle e_1, \ldots, e_n \rangle_R$. Рассмотрим свободный модуль $F = \langle u_1, \ldots, u_s \rangle$. Имеем $F \cong R \oplus \ldots \oplus R$ (s штук). Представим V как фактормодуль F/Q. Модуль F конечномерный $\Rightarrow V$ также конечномерный. ■

Пусть $R = \langle e_1, \ldots, e_k \rangle_{\mathbb{K}}$ — векторное пространство. Введём умножение на базисных векторах (превратим R в алгебру) по формулам $e_i e_j = \sum\limits_{k=1}^{n} c_{ij}^k e_k$. Построим модуль V над R. Для этого зададим действие элементов $r \in R$ на элементы $x \in V$ (линейные операторы) $\rho_r(x) = rx$. Достаточно задать такие линейные операторы для базиса: $\rho_i(x) = e_i x$, где $\rho_i = \rho_{e_i}$. При этом произведение элементов алгебры должно соответствовать произведению операторов: $\rho_i \rho_j = \sum\limits_{k=1}^{n} c_{ij}^k \rho_k$, и единице соответствует тождественный оператор $\rho_e = \mathcal{E}$. Таким образом, модуль V над алгеброй R — это векторное пространство и семейство линейных операторов. Фактически при задании модуля рассматривается гомоморфизм из R в алгебру линейных операторов $\mathrm{Lin}(V)$, т. е. *линейное представление* R.

Рассмотрим гомоморфизм R-модулей $\varphi\colon V \to W$, т. е. линейное отображение модулей как векторных пространств, перестановочное с умножением на элементы из R, т. е. $\varphi(rx) = r\varphi(x)$. Пусть ρ_r и $\widetilde{\rho}_r$ — операторы умножения на r в модулях V и W соответственно. Перестановочность ρ и φ достаточно проверять только для базисных элементов. Выберем базис в модулях: $V = \langle v_1, \ldots, v_n \rangle,\ W = \langle w_1, \ldots, w_n \rangle$. Пусть T — матрица φ в этих базисах, A_i — матрица ρ_i относительно базиса V, а B_i — матрица $\widetilde{\rho}_i$ относительно базиса W. Получаем, что матрицы B_i и A_i должны быть сопряжены одной и той же матрицей T: Для $\forall\, x\ B_i T x = T A_i x \ \Rightarrow\ B_i T = T A_i \ \Rightarrow\ B_i = T A_i T^{-1}$. Рассмотрим частный случай: $V = W$, и выбрано 2 разных базиса. Тогда матрицы операторов на V при переходе к другому базису изменяются при помощи сопряжения (хорошо известное утверждение из линейной алгебры).

3.5. Простота и полупростота модулей. Полупростые алгебры

3.5.1. Простые модули

Пусть дан R-модуль V. Рассмотрим подмодуль $L \subset V$. Он является подпространством. Наоборот, подпространство L будет подмодулем, если оно инвариантно относительно всех операторов из R, т. е. $\rho_r(L) \subseteq L \Leftrightarrow \forall\, x \in L,\ r \in R$ выполнено $rx \in L$. Это свойство достаточно проверять на базисных операторах ρ_i.

Определение. Если существует подпространство, инвариантное относительно всех операторов ρ_i, то пространство называется *приводимым*.

На матричном языке свойство приводимости выглядит так: существует матрица перехода к новому базису,

в котором матрицы всех операторов имеют общий угол нулей:

$$B_i = \left(\begin{array}{c|c} * & * \\ \hline 0 & * \end{array}\right).$$

Определение. Модуль называется *полупростым* (*вполне приводимым*), если он является прямой суммой простых.

Лемма 3.13 (Эквивалентное условие полупростоты модуля). *Конечномерный модуль V над конечномерной алгеброй R является полупростым $\Leftrightarrow$ для любого подмодуля $L \subset V$ существует подмодуль $L' \subset V$, такой, что $V = L \oplus L'$.*

□ Справа налево докажем по индукции по размерности подмодулей. Имеем $V = L \oplus L'$. Пусть один из подмодулей (для определённости L) не простой. Докажем, что L также расщепляется в прямую сумму. Пусть $M \subset L$. Тогда по условию $V = M \oplus M'$. Покажем, что $L = M \oplus (L \cap M')$. Очевидно, что $M \oplus (L \cap M') \subseteq L$, остаётся показать обратное включение. Пусть $x \in L \;\Rightarrow\; x = x_1 + x_2$, где $x_1 \in M,\ x_2 \in M'$. Тогда $x_2 = x - x_1 \in L \;\Rightarrow\; x_2 \in (L \cap M')$. Поскольку модули L и L' имеют меньшую размерность, то они предположению индукции обладают свойством отщепляемости.

Обратно: пусть $V = V_1 \oplus \ldots \oplus V_s$, где V_i — простые подмодули, L — некоторый подмодуль в V. Если $V_i \subset L$ для всех i, то тогда $L = V$ и доказывать нечего. Пусть нашлось $i\colon V_i \not\subseteq L$. Тогда $L \cap V_i = \{0\}$, так как пересечение $L \cap V_i$ есть подмодуль в V_i, а V_i — простой. Следовательно, можно рассмотреть прямую сумму $L \oplus V_i$. Если $L \oplus V_i \neq V$, то повторяем процедуру отщепления. Рано или поздно всё закончится, так как модуль конечномерный. ■

Следствие 3.4. *Подмодуль или фактормодуль полупростого модуля является полупростым.*

□ Для подмодулей справедливость утверждения обеспечивается леммой. Докажем для фактормодулей. Пусть $L \subset V,\ L'' = V/L$. Вследствие полупростоты V найдётся подмодуль $L' \subset V\colon\ V = L \oplus L'$. Но тогда $V/L \cong L'$. Так как L' — подмодуль полупростого модуля, то он сам полупростой, а значит, V/L полупростой. ■

3.5.2. Полупростые алгебры

Определение. Конечномерная алгебра называется *полупростой (слева)*, если как левый модуль над собой она является полупростым модулем.

Определение. *Минимальный* левый идеал — ненулевой идеал, не содержащий ненулевых подидеалов.

Рассмотрим алгебру R как левый модуль над собой. Пусть она полупроста, т. е. $R = I_1 \oplus \ldots \oplus I_s$. Тогда простые подмодули I_i, очевидно, будут левыми идеалами. Наоборот, алгебра R — полупроста слева, если она является прямой суммой своих минимальных левых идеалов.

Утверждение 3.14. *Любой конечномерный модуль V над полупростой алгеброй R является полупростым.*

□ Модуль V конечномерен $\Rightarrow$ имеет конечную систему порождающих, а значит, может быть представлен как $V = F/Q$, где $F = \langle e_1, \ldots, e_k \rangle_R = R \oplus \ldots \oplus R$ — свободный модуль. Если R полупроста, то и F разлагается в прямую сумму простых, т. е. является полупростым. А значит, и F/Q по следствию также полупростой. ■

Утверждение 3.15. *Всякая простая конечномерная алгебра R является полупростой.*

□ Алгебра R конечномерна $\Rightarrow$ в ней есть минимальные левые идеалы (см. определение идеала в алгебре). Пусть I — некоторый минимальный левый идеал в R. Пусть $x \in I,\ r \in R$. Рассмотрим отображение $f\colon x \mapsto xr$, т. е. $f\colon I \to Ir$ — эпиморфизм. Поскольку Ir — левый идеал, то f будет гомоморфизмом левых модулей (простых). Тогда его ядро либо нулевое, либо совпадает с I, так как в I нет нетривиальных подмодулей. Значит, либо $Ir \cong I$, либо $Ir = 0$. Теперь рассмотрим все такие идеалы вида Ir_i для всех $r_i \in R$ и их сумму

$$J := \sum_{r_i \in R} Ir_i = \{r \in R\colon\ \exists\, x_i \in I,\ r_i \in R\,(i = 1, \ldots, s)\colon\ r = x_1 r_1 + \ldots + x_s r_s\}.$$

Это множество будет двусторонним ненулевым идеалом, содержащим I, так как I — левый идеал, и умножение слева ничего не меняет, а при умножении справа снова получается элемент такого же вида. Но алгебра простая, и нетривиальных идеалов там нет, а значит, $J = R$. В частности, есть разложение для единицы: $1 = x_1 r_1 + \ldots + x_s r_s$. Рассмотрим сумму $Ir_1 + \ldots + Ir_s$. Она содержит единицу, а следовательно совпадает с R.

Теперь рассмотрим внешнюю прямую сумму $V := Ir_1 \oplus \ldots \oplus Ir_s$. Она будет полупростым модулем (суммой простых). Построим гомоморфизм $g\colon V \to R$ по формуле $g(y_1, \ldots, y_s) = y_1 + \ldots + y_s$, где $y_i = x_i r_i,\ x_i \in I$. Он будет эпиморфизмом левых модулей, а тогда по теореме о гомоморфизме $R \cong V/\operatorname{Ker} g$. Тогда по следствию леммы R будет полупростой. ■

Замечание. Пусть все слагаемые в разложении модуля V между собой изоморфны I. Тогда, так как по теореме Жордана – Гёльдера разложение в прямую сумму простых модулей однозначно с точностью до изоморфизма, то любой подмодуль и фактормодуль в V также однозначно разлагается в прямую сумму модулей, изоморфных I. Значит, R будет прямой суммой минимальных левых идеалов, изоморфных I.

Утверждение 3.16. *Пусть R — полупростая алгебра, $R = I_1 \oplus \ldots \oplus I_s$, где I_i — минимальные левые идеалы. Тогда любой неприводимый R-модуль V изоморфен одному из I_i.*

□ Модуль V порождается одним своим элементом. В самом деле, если бы порождающих было больше, то тогда в V существовал бы нетривиальный подмодуль, порождённый одним из них. Пусть $V = Rx_0$, где $0 \neq x_0 \in V$. Рассмотрим эпиморфизм $f\colon R \to V\colon f(r) = rx_0$. Тогда $V \cong R/\operatorname{Ker} f$. Поскольку R полупроста, то $R = \operatorname{Ker} f \oplus I$, где I — некоторый её идеал. Следовательно, $I \cong R/\operatorname{Ker} f \cong V$. Но так как $\operatorname{Ker} f$ — подмодуль полупростого модуля, то он сам полупростой, т. е. $\operatorname{Ker} f = I'_1 \oplus \ldots \oplus I'_{k-1}$, где I'_i — минимальные левые идеалы. Значит, $R = I'_1 \oplus \ldots \oplus I'_{k-1} \oplus I$. В силу однозначности разложения $k = s$ и слагаемые изоморфны (с точностью до перестановки). Следовательно, $\exists\, j\colon V \cong I \cong I_j$. ■

Следствие 3.5. *Над простой конечномерной алгеброй все простые модули между собой изоморфны.*

Пример 5.1. Пусть $R = \mathbf{M}_n(\mathbb{K})$ (полная матричная алгебра), и $V = \mathbb{K}^n$. Модуль V будет неприводимым, так как не существует подпространства, инвариантного относительно всех операторов. Рассмотрим множество матриц I_j, у которых j-тый столбец — произвольный, а все остальные столбцы нулевые. Очевидно, что это левый идеал алгебры, кроме того, он будет минимальным. Имеем $I_j \cong \mathbb{K}^n$, $\mathbf{M}_n(\mathbb{K}) = I_1 \oplus \ldots \oplus I_n$. Значит, алгебра $\mathbf{M}_n(\mathbb{K})$ полупростая.

Задача 3.1. *Доказать, что если над полупростой алгеброй все неприводимые модули между собой изоморфны, то она простая.*

3.6. Кольцо (алгебра) эндоморфизмов модулей

3.6.1. Основные понятия

Определение. *Эндоморфизмом* модуля называется его гомоморфизм на себя.

Пусть R — кольцо или алгебра, V, W — R-модули. Рассмотрим множество гомоморфизмов $\operatorname{Hom}(V, W)$. Введём на нём операцию сложения: $(f + g)(x) := f(x) + g(x)$. Очевидно, что это корректно. Значит, $\operatorname{Hom}(V, W)$ есть абелева группа по сложению. Если R — алгебра над $\mathbb{K}$, то зададим умножение на элементы поля: $(\lambda f)(x) := \lambda f(x)$, и группа гомоморфизмов превращается в векторное пространство над $\mathbb{K}$.

Теперь рассмотрим $\operatorname{End}(V) := \operatorname{Hom}(V, V)$. В таком множестве можно ввести ещё одну операцию — композицию (умножение). Значит, $\operatorname{End}(V)$ — кольцо. Оно и называется кольцом эндоморфизмов модулей.

Замечание. Эндоморфизм — аналог линейного оператора в векторном пространстве.

Если R — алгебра, то $\operatorname{End}(V)$ становится алгеброй. Можно считать, что $\mathbb{K} \subset \operatorname{End}(V)$, так как можно отождествить скалярные операторы с умножением на числа. Очевидно, что $\mathbb{K} \subset Z(\operatorname{End}(V))$.

Пусть V — конечномерный R-модуль, где R — алгебра над $\mathbb{K}$. Рассмотрим алгебру всех $\mathbb{K}$-линейных операторов $\operatorname{Lin}(V)$. Имеем $\operatorname{End}(V) \subset \operatorname{Lin}(V)$. Как уже говорилось, можно рассматривать элементы из R как линейные операторы. По определению гомоморфизма должно выполняться свойство $f(rx) = rf(x)$, а значит, эндоморфизмы — это те операторы, которые коммутируют с операторами из R.

3.6.2. Лемма Шура

Будем рассматривать гомоморфизмы простых модулей.

Лемма 3.17 (Шура). *Пусть R — конечномерная алгебра над $\mathbb{K}$, и V, W — простые R-модули. Тогда:*
1° *$f \in \operatorname{Hom}(V, W) \Rightarrow$ f либо нулевой, либо изоморфизм;*
2° *Любой эндоморфизм V является автоморфизмом, и $\operatorname{End}(V)$ — алгебра с делением;*
3° *Если $\mathbb{K} = \mathbb{C}$, то любой эндоморфизм простого модуля скалярен, т. е. $\operatorname{End}(V) = \mathbb{C}$.*

□ **1°** Ядро эндоморфизма — подмодуль, а V простой модуль, значит, либо $\operatorname{Ker} f = \{0\}$, либо $\operatorname{Ker} f = V$. В первом случае получаем, что f — инъекция. $\operatorname{Im} f \subseteq W$, $\operatorname{Im} f \neq \{0\} \Rightarrow \operatorname{Im} f = W$, так как W простой модуль.

2° Очевидно: любой изоморфизм на себя (т. е. автоморфизм) обратим, и значит, $\operatorname{End}(V)$ — алгебра с делением.

3° Можно сослаться на теорему о том, что все конечномерные алгебры с делением над $\mathbb{C}$ совпадают с $\mathbb{C}$. Но не будем «стрелять из пушки по воробьям» и докажем это по-другому. Пусть $f \in \operatorname{End}(V)$. У него есть собственное значение λ, так как $\mathbb{K} = \mathbb{C}$. Если $f = \lambda\mathcal{E}$, то всё ясно, а если нет, то тогда оператор $f - \lambda\mathcal{E} \neq 0$ также будет эндоморфизмом. Тогда $\operatorname{Ker}(f - \lambda\mathcal{E})$ — подмодуль в V, но вследствие простоты это либо $\{0\}$, либо весь модуль V. ■

3.6.3. Кольцо эндоморфизмов прямой суммы модулей

Пусть $V = V_1 \oplus \ldots \oplus V_n$. Рассмотрим эндоморфизм $f\colon V \to V$. Пусть мы уже знаем, как устроены $\operatorname{Hom}(V_i, V_j)$. Тогда достаточно задать f на прямых слагаемых. Пусть $x = (x_1, \ldots, x_n) \in V$, $f(x) = (y_1, \ldots, y_n)$, где $y_i \in V_i$. $f\big((0, \ldots, x_j, \ldots, 0)\big) = (y_{1j}, \ldots, y_{nj})$. Рассмотрим $f_{ij}\colon V_j \to V_i$. Эти гомоморфизмы можно рассматривать как гомоморфизмы всего модуля, если считать, что $f_{ij}\big((x_1, \ldots, x_n)\big) = (0, \ldots, y_{ij}, \ldots, 0)$. Если мы зададим f_{ij} для

всех i и j, то тогда мы зададим и весь эндоморфизм f. Пусть $x = x_1 + \ldots + x_n$, тогда $f(x) = f(x_1) + \ldots + f(x_n)$. Каждый «элементарный» гомоморфизм f_{ij} отображает V_j в V_i, а всё остальное переводит в 0. Значит,

$$f = \sum_{i,j=1}^{n} f_{ij} = \begin{pmatrix} f_{11} & \ldots & f_{1n} \\ & & \\ f_{n1} & \ldots & f_{nn} \end{pmatrix}.$$

При таком задании f_{ij} сумме эндоморфизмов соответствует сумма, а композиции — произведение матриц:

$$f_{ij} \cdot g_{kl} = \begin{cases} 0, \ j \neq k; \\ (f \circ g)_{il}, \ j = k. \end{cases}$$

Значит, можно отождествить элементы кольца эндоморфизмов прямой суммы модулей с матрицами из f_{ij}.

3.7. Основная теорема о полупростой алгебре над $\mathbb{C}$

3.7.1. Гомоморфизмы полупростых модулей

Рассмотрим частный случай: V — полупростой R-модуль, а R — алгебра над $\mathbb{C}$. Разложим V на простые и сгруппируем изоморфные слагаемые в блоки:

$$V = (\underbrace{V_1 \oplus \ldots \oplus V_{n_1}}_{n_1}) \oplus (\underbrace{V_{n_1+1} \oplus \ldots \oplus V_{n_1+n_2}}_{n_2}) \oplus \ldots \oplus V_s.$$

Пусть $\varphi_{ij} \in \mathrm{Hom}(V_j, V_i)$. Тогда, по лемме Шура, если V_j и V_i в одном блоке, то $\mathrm{Hom}(V_i, V_j) \cong \mathbb{C}$ (только умножение на скаляры), а если в разных, то $\mathrm{Hom}(V_i, V_j) = \{0\}$. Значит, матрицы из алгебры эндоморфизмов будут иметь следующий блочный вид:

$$\begin{pmatrix} \mathbf{M}_{n_1}(\mathbb{C}) & & & 0 \\ n_1 \times n_1 & & & \\ & \mathbf{M}_{n_2}(\mathbb{C}) & & \\ & n_2 \times n_2 & & \\ & & \ddots & \\ 0 & & & \mathbf{M}_{n_s}(\mathbb{C}) \\ & & & n_s \times n_s \end{pmatrix}$$

Получается следующее

Утверждение 3.18. *Алгебру эндоморфизмов полупростого модуля можно отождествить с прямым произведением полных матричных алгебр* $\mathbf{M}_{n_1}(\mathbb{C}) \times \ldots \times \mathbf{M}_{n_s}(\mathbb{C})$.

3.7.2. Основная теорема и её следствия

Теорема 3.19. *Полупростая алгебра R над $\mathbb{C}$ изоморфна прямому произведению полных матричных алгебр.*

□ Рассмотрим алгебру как левый модуль над собой. Представим её как прямую сумму минимальных левых идеалов, сгруппировав их в блоки:

$$R = (\underbrace{V_1 \oplus \ldots \oplus V_{n_1}}_{n_1}) \oplus (\underbrace{V_{n_1+1} \oplus \ldots \oplus V_{n_1+n_2}}_{n_2}) \oplus \ldots \oplus V_{n_k}, \ \dim R = n.$$

Из предыдущего утверждения следует, что $\mathrm{End}_R(R) = \mathbf{M}_{n_1}(\mathbb{C}) \times \ldots \times \mathbf{M}_{n_k}(\mathbb{C})$. Теперь построим изоморфизм алгебр между R и $\mathrm{End}_R(R)$. Сопоставим каждому элементу алгебры $r \in R$ эндоморфизм $\varphi_r(x) := xr$. Проверим, что это действительно эндоморфизм: $\varphi_r(x_1 + x_2) = (x_1 + x_2)r = x_1r + x_2r = \varphi_r(x_1) + \varphi_r(x_2)$, и $\varphi_r(\lambda x) = (\lambda x)r = \lambda(xr) = \lambda\varphi_r(x)$. Таким образом, получается отображение $\mu\colon R \to \mathrm{End}_R(R)$. Покажем, что оно биективно. Инъективность: если $r \neq 0$, то $\varphi_r(1) = r \Rightarrow \varphi_r \neq 0$. Сюръективность: возьмём любой эндоморфизм $\varphi \in \mathrm{End}_R(R)$, положим $r := \varphi(1)$. Тогда, пользуясь тем, что φ — эндоморфизм левых модулей и он перестановочен с умножением на элементы из R, получаем, что $\varphi(x) = \varphi(x \cdot 1) = x\varphi(1) = xr = \varphi_r(x)$, т. е. любому эндоморфизму соответствует некоторый φ_r. Биективность доказана. Остается построить изоморфизм алгебр R и $\mathrm{End}_R(R)$. Первым кандидатом на роль изоморфизма является само отображение μ, но беда в том, что если $r_1, r_2 \in R$, то

$$\varphi_{r_1r_2}(x) = x(r_1r_2) = (xr_1)r_2 = \varphi_{r_1}(x)r_2 = \varphi_{r_2}(\varphi_{r_1}(x)) = (\varphi_{r_1} \circ \varphi_{r_2})(x).$$

Перемножение происходит в обратном порядке: $\mu(r_1r_2) = \mu(r_2)\mu(r_1)$. Значит, μ не является изоморфизмом алгебр. Теперь «подправим» наше отображение, вспомнив, что произведение транспонированных матриц есть

транспонированное произведение в обратном порядке. Пусть T — отображение транспонирования. Тогда $(T \circ \mu)$ уже будет изоморфизмом алгебр, откуда и следует, что $R \cong \mathbf{M}_{n_1}(\mathbb{C}) \oplus \ldots \oplus \mathbf{M}_{n_k}(\mathbb{C})$. ■

Сформулируем следствия теоремы. R — полупростая алгебра над $\mathbb{C}$. Имеем $R \cong \mathbf{M}_{n_1}(\mathbb{C}) \times \ldots \times \mathbf{M}_{n_k}(\mathbb{C})$. Тогда:

Следствие 3.6. *Если V — простой модуль над R, то он будет модулем над одним из сомножителей $\mathbf{M}_{n_i}(\mathbb{C})$ для некоторого i. Все простые модули над $\mathbf{M}_n(\mathbb{C})$ изоморфны минимальному левому идеалу, состоящему из матриц, у которых все столбцы, кроме одного, нулевые. Таким образом, если есть k блоков, то есть k попарно неизоморфных модулей V над блоками, и $\dim_{\mathbb{C}} V = n_i$, где n_i — размер блока.*

Следствие 3.7. *Размерность полупростой алгебры над $\mathbb{C}$ равна сумме квадратов размерностей простых модулей над ней, т. е. $\dim_{\mathbb{C}} R = n_1^2 + \ldots + n_k^2 = \dim \mathbf{M}_{n_1}(\mathbb{C}) + \ldots + \dim \mathbf{M}_{n_k}(\mathbb{C})$.*

Следствие 3.8. *Имеем $Z(R) = Z(M_{n_1}(\mathbb{C})) \times \ldots \times Z(M_{n_k}(\mathbb{C}))$. Центр образован скалярными матрицами $\Rightarrow Z(R) = \mathbb{C}^k$, и $\dim_{\mathbb{C}} Z(R) = k$, где k – число блоков. Следовательно, число неизоморфных простых модулей над полупростой комплексной алгеброй равно размерности её центра.*

Следствие 3.9. *Если полупростая алгебра над $\mathbb{C}$ коммутативна, то все простые модули над ней одномерны. Верно также и обратное утверждение.*

□ Пусть задана совокупность коммутирующих линейных операторов $\{\mathcal{A}_i\}$ на комплексном конечномерном векторном пространстве. Докажем, что у них есть общий собственный вектор, т. е. общее одномерное инвариантное подпространство. Проведём индукцию по $n := \dim V$. Если $n = 1$, доказывать нечего. Пусть всё доказано для размерности меньше n. Если все операторы скалярные, то всё ясно. Пусть есть какой-то нескалярный оператор, для определённости $\mathcal{A}_1$, и λ — его собственное значение. Рассмотрим его собственное подпространство $V_\lambda = \operatorname{Ker}(\mathcal{A} - \lambda\mathcal{E})$. Очевидно, оно ненулевое и не совпадает со всем пространством. Покажем, что оно инвариантно относительно всех $\mathcal{A}_i$. Пусть $x \in V_\lambda$. Тогда $\mathcal{A}_1(\mathcal{A}_i(x)) \overset{\text{комм.}}{=\!=} \mathcal{A}_i(\mathcal{A}_1(x)) = \mathcal{A}_i(\lambda x) = \lambda\mathcal{A}_i(x)$, т. е. λ будет собственным значением для всех $\mathcal{A}_i$. Имеем $\dim V_\lambda < n \Rightarrow$ можно применить предположение индукции. Значит, все простые модули одномерны. ■

4. Линейные представления групп

4.1. Основные понятия

4.1.1. Понятие линейного представления

Определение. Пусть G — группа, V — конечномерное векторное пространство над полем $\mathbb{K}$. *Линейным представлением* группы G называется гомоморфизм $\rho\colon G \to \mathbf{GL}(V)$.

Линейное представление является частным случаем действия группы на векторном пространстве V. Однако каждому элементу группы в данном случае сопоставляется не произвольное биективное отображение V в себя, а линейный оператор. Произведению элементов соответствует композиция операторов: $g_1 g_2 \mapsto \rho(g_1 g_2) = \rho(g_1)\rho(g_2)$. Единица переходит в тождественный оператор $\mathcal{E}$.

Пусть в пространстве V выбран какой-то базис: $V = \langle e_1, \ldots, e_n \rangle$. Тогда можно перейти к матричному представлению $\rho\colon G \to \mathbf{GL}_n(\mathbb{K})$.

Определение. *Размерностью представления* называется размерность пространства V.

Определение. Пусть есть 2 представления $\rho_1\colon G \to \mathbf{GL}(V)$ и $\rho_2\colon G \to \mathbf{GL}(W)$. *Гомоморфизмом* линейных представлений называется линейное отображение векторных пространств $\varphi\colon V \to W$, при котором $\varphi\big(\rho_1(g)(x)\big) = \rho_2(g)\big(\varphi(x)\big)$ для $\forall\, g \in G$, т. е. следующая диаграмма коммутативна:

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ {\scriptstyle \rho_1}\downarrow & & \downarrow{\scriptstyle \rho_2} \\ V & \xrightarrow[\varphi]{} & W \end{array}$$

Определение. Гомоморфизм φ линейных представлений ρ_1 и ρ_2 называется *изоморфизмом* в том случае, когда он является изоморфизмом векторных пространств. В этом случае говорят, что представления *эквивалентны*.

Выясним, что означает эквивалентность представлений ρ_1 и ρ_2 в терминах матриц. Пусть $V = \langle e_1, \ldots, e_n \rangle$, и $W = \langle f_1, \ldots, f_n \rangle$. Пусть C — матрица изоморфизма φ, а $\rho_1(g)$ и $\rho_2(g)$ — матрицы операторов в соответствующих базисах. Тогда, по определению изоморфизма,

$$\rho_2(g)C = C\rho_1(g) \Leftrightarrow \rho_2(g) = C\rho_1(g)C^{-1} \;\; \forall\, g \in G.$$

Таким образом, матрицы всех операторов, соответствующих элементам группы, должны быть подобны, и (что самое важное) сопрягающая матрица одна для всех элементов группы.

4.1.2. Приводимость представлений

Определение. Линейное представление называется *приводимым*, если существует нетривиальное подпространство $W \subset V$, являющееся инвариантным относительно $\rho(g)$ для всех $g \in G$. В этом случае индуцируется представление на пространстве W. Если такого подпространства нет, представление *неприводимо*.

На матричном языке приводимость означает, что если выбрать базис $V = \langle e_1, \dots, e_k, e_{k+1}, \dots, e_n \rangle$, такой, что $W = \langle e_1, \dots, e_k \rangle$, то у всех операторов $\rho(g)$ будет общий угол нулей.

Замечание. Иногда для краткости пишут $\rho(g)(x) = gx$.

Если $G = \{g_1, \dots, g_m\}$, то очевидно, что представление неприводимо $\Leftrightarrow \ \langle g_1 x, \dots, g_m x \rangle_{\mathbb{K}} = V$.

Определение. Линейное представление ρ называется *вполне приводимым (полупростым)*, если оно разлагается в прямую сумму неприводимых, то есть $V = V_1 \oplus \dots \oplus V_s$, где V_i — инвариантные подпространства относительно $\rho(g)$ для всех $g \in G$. Обозначение: $\rho = \rho_1 \oplus \dots \oplus \rho_s$.

Вполне приводимость означает, что матрицы $\rho(g)$ в подходящем базисе будут блочно-диагональными, и в каждом блоке стоит матрица ограничения представления $\rho_i := \rho\Big|_{V_i}$ на подпространство V_i.

4.1.3. Примеры линейных представлений

Пример 1.1. Рассмотрим линейное представление бесконечной циклической группы $\rho\colon \langle a \rangle_\infty \to \mathbf{GL}(V)$. Достаточно задать одну невырожденную матрицу $\rho(a)$. Очевидно, два представления будут эквивалентными $\Leftrightarrow$ матрицы для порождающих элементов подобны, т. е. обладают одинаковой жордановой формой.

Пример 1.2. $G = \langle a \rangle_n$. В этом случае опять достаточно задать матрицу для порождающего элемента, такую, что $\rho(a)^n = \mathcal{E}$. Аннулирующим для оператора $\rho(a)$ будет многочлен $t^n - 1$, а значит, над полем $\mathbb{C}$ матрица диагонализируема, и все жордановы клетки будут одномерными, так как у многочлена нет кратных корней.

Замечание. Над полем $\mathbb{C}$ все конечномерные представления будут вполне приводимыми.

Пример 1.3. Пусть G — свободная группа с базисом $x_1, \dots, x_n$. На порождающих элементах представление можно задавать произвольным образом. Представления эквивалентны, если $\rho_2(x_i) = C\rho_1(x_i)C^{-1}$, $i = \overline{1, n}$.

Рассмотрим более общий случай. Пусть группа G порождается элементами $a_1, \dots, a_n$. Чтобы задать линейное представление, нужно определить $\rho(a_1), \dots, \rho(a_n)$, и при этом должны выполняться определяющие соотношения, т. е. если $a_{i_1}^{\varepsilon_1} \dots a_{i_s}^{\varepsilon_s} = e$, то тогда $\rho(a_{i_1})^{\varepsilon_1} \dots \rho(a_{i_s})^{\varepsilon_s} = \mathcal{E}$.

4.1.4. Связь модулей с линейными представлениями групп

Убедимся в том, что линейное представление — частный случай модуля над алгеброй. Пусть $G = \{g_1, \dots, g_n\}$, $\mathbb{K}$ — поле. Рассмотрим групповую алгебру $\mathbb{K}G = \langle g_1, \dots, g_n \rangle = \left\{ \sum\limits_{g \in G} a_g g \mid a_g \in \mathbb{K} \right\}$, т. е. n-мерное векторное пространство над $\mathbb{K}$, у которого базисные векторы формально занумерованы элементами группы. Рассмотрим модуль V над $\mathbb{K}G$. Зададим умножение в модуле на элементы алгебры, т. е. действие $r \in \mathbb{K}G$ на $x \in V$. Для этого зададим умножение на базисных векторах: для $r = g \in G$ и $x \in V$ определим линейный оператор $\rho(g)(x) = gx$. Наоборот, пусть задано представление $\rho\colon G \to \mathbf{GL}(V)$. Чтобы задать умножение $r \cdot x$, достаточно задать его на базисных элементах: $gx = \rho(g)(x)$. При этом произведение базисных элементов переходит в произведение операторов, поэтому аксиомы модуля выполняются автоматически: $(\sum a_g g)x \overset{\text{дистр.}}{=\!=} \sum a_g \rho(g)x$.

Таким образом, мы видим, что рассмотрение линейных представлений равносильно рассмотрению модулей. В частности, практически одинаковым оказывается понятие гомоморфизма, приводимости, и т. д.

4.2. Основные теоремы о линейных представлениях

4.2.1. Лемма Шура для линейных представлений. Теорема Машке

Переформулируем лемму Шура для линейных представлений.

Лемма 4.1. *Пусть V, W — неприводимые линейные представления группы G над полем $\mathbb{C}$. Тогда любой гомоморфизм $\varphi\colon V \to W$ либо изоморфизм, либо нулевой. Гомоморфизм неприводимого комплексного представления в себя является скалярным (Матрица, коммутирующая со всеми операторами, может быть только скалярной).*

Теорема 4.2 (Машке). *Пусть G — конечная группа порядка n, $\mathbb{K}$ — поле и $\operatorname{char}\mathbb{K}$ не является делителем порядка группы (в частности, $\operatorname{char}\mathbb{K} = 0$). Тогда групповая алгебра $\mathbb{K}G$ полупроста.*

□ Покажем, что любой конечномерный модуль V над $\mathbb{K}G$ обладает свойством отщепляемости, т. е. если существует инвариантное подпространство $L \subset V$, то существует и дополнительное инвариантное подпространство L' такое, что $V = L \oplus L'$. Это равносильно тому, что существует гомоморфизм модулей $\pi\colon V \to L$, являющийся проекцией на L, т. е. $\pi(x) = x$, если $x \in L$. Если мы найдём такой гомоморфизм, то положим $L' := \operatorname{Ker}\pi$ и утверждение будет доказано. В самом деле, покажем, что $V = \operatorname{Im}\pi \oplus \operatorname{Ker}\pi$. Проектор — это такой оператор π, что $\pi^2(x) = \pi(x)$. Запишем тождество $x = \pi(x) + x - \pi(x)$. Поскольку $\pi(x - \pi(x)) = \pi(x) - \pi^2(x) = \pi(x) - \pi(x) = 0$, то $x - \pi(x) \in \operatorname{Ker}\pi$. Таким образом, вектор разлагается в сумму $\pi(x) \in \operatorname{Im}\pi$ и $x - \pi(x) \in \operatorname{Ker}\pi$. Пересечение ядра с образом нулевое, поэтому сумма прямая.

Построим проекцию на L, являющуюся гомоморфизмом модулей. Пусть $\widetilde{\pi}\colon V \to L$ — произвольная проекция на L, при которой элементы из L отображаются тождественно. Построим отображение $\pi(x) := \frac{1}{n}\sum\limits_{g\in G} g\widetilde{\pi}(g^{-1}x)$. Коэффициент $\frac{1}{n}$ имеет смысл, так как $\operatorname{char}\mathbb{K} \nmid n$ и в поле $\mathbb{K}$ число $n \cdot 1$ не равно 0 и, стало быть, обратимо. Покажем, что π является гомоморфизмом модулей, а именно, $\pi(hx) = h\pi(x)$. В самом деле,

$$\pi(hx) = \frac{1}{n}\sum_{g\in G} g\widetilde{\pi}(g^{-1}hx) = \frac{1}{n}\sum_{g\in G} h(h^{-1}g)\widetilde{\pi}\big((g^{-1}h)x\big) \overset{\text{дистр.}}{=\!=} h\cdot\frac{1}{n}\sum_{g\in G}(h^{-1}g)\widetilde{\pi}\big((h^{-1}g)^{-1}x\big). \tag{1}$$

Если g при суммировании пробегает всю группу, то и $h^{-1}g$ также пробегает всю группу. Значит, (1) равно $h\pi(x)$. Теперь проверим, что это проекция на L. Если $x \in L$, то и $g^{-1}x \in L$, так как L инвариантное подпространство. Но тогда и $\widetilde{\pi}(g^{-1}x) \in L$, а значит, и $g\widetilde{\pi}(g^{-1}x) \in L$. Кроме того,

$$\pi(x) = \frac{1}{n}\sum_{g\in G} g\underbrace{\widetilde{\pi}(g^{-1}x)}_{g^{-1}x} = \frac{1}{n}\sum_{g\in G} gg^{-1}x = \frac{1}{n}\underbrace{\sum x}_{nx} = x.$$

■

4.2.2. Ортогональные и унитарные представления

Пусть V — векторное пространство над полем $\mathbb{R}$ или $\mathbb{C}$. Введём скалярное произведение (евклидово или эрмитово).

Определение. Представление называется *ортогональным* (соответственно, для $\mathbb{C}$ – *унитарным*), если все операторы $\rho(g)$ ортогональны (унитарны).

Пользуясь этим понятием, можно легко доказать теорему Машке для полей $\mathbb{R}$ и $\mathbb{C}$. Рассмотрим случай $\mathbb{K} = \mathbb{C}$. Покажем, что можно ввести такое скалярное произведение, относительно которого линейное представление будет унитарным. Сначала введём обычное эрмитово произведение $(x, y) = \sum\limits_{i=1}^{n} \overline{x_i}y_i$. Построим новое скалярное произведение $\langle x, y\rangle := \frac{1}{n}\sum\limits_{g\in G}(gx, gy)$. Ясно, что это также невырожденная эрмитова форма. Тогда любое представление будет унитарным, поскольку если $h \in G$, то

$$\langle hx, hy\rangle = \frac{1}{n}\sum(ghx, ghy) = \frac{1}{n}n\,\langle x, y\rangle = \langle x, y\rangle \tag{2}$$

(здесь gh также пробегает всю G).

Теперь доказательство теоремы Машке тривиально: если есть инвариантное подпространство относительно ортогонального (унитарного) оператора, то ортогональное дополнение также инвариантно, а этот факт был доказан в курсе линейной алгебры.

Задача 4.1. *Доказать обратную теорему Машке: если групповая алгебра полупроста, то* $\operatorname{char}\mathbb{K} \nmid |G|$. *Идея решения: от противного, пусть* $\operatorname{char}\mathbb{K}$ *делит порядок группы. Нужно рассмотреть алгебру* $\mathbb{K}G$ *как модуль над собой и доказать, что подпространство* $L := \left\langle \sum\limits_{g\in G} g \right\rangle$ *не отщепляется.*

4.2.3. Свойства линейных представлений. Регулярное представление

Дано представление $\rho\colon G \to \mathbf{GL}(V)$, где V — векторное пространство над $\mathbb{C}$. Перечислим его свойства.

Утверждение 4.3. *Любое комплексное представление вполне приводимо (уже доказывалось).*

Определение. *Регулярным представлением* группы G называется представление Λ на групповой алгебре $\mathbb{K}G$, заданное по правилу $\Lambda(h)(\sum\limits_{g\in G} a_g g) = \sum\limits_{g\in G} a_g hg$.

Разложим групповую алгебру (а вместе с ней и регулярное представление) на неприводимые и сгруппируем изоморфные слагаемые в блоки:

$$\mathbb{K}G = (\underbrace{V_1 \oplus \ldots \oplus V_{n_1}}_{n_1}) \oplus (\underbrace{V_{n_1+1} \oplus \ldots \oplus V_{n_1+n_2}}_{n_2}) \oplus \ldots \oplus (\underbrace{V_{n_1+\ldots+n_{s-1}} \oplus \ldots \oplus V_{n_1+\ldots+n_s}}_{n_s}).$$

Утверждение 4.4. *Любое неприводимое представление входит в регулярное представление.*[1]

□ Пусть $\Lambda : G \to \mathbf{GL}(\mathbb{K}G)$ — регулярное представление группы G, и $\rho\colon G \to \mathbf{GL}(V)$ — произвольное неприводимое представление. Фиксируем вектор $x \in V$. Рассмотрим линейное отображение $\varphi_x\colon \mathbb{K}G \to V$, заданное по правилу $\sum\limits_{g\in G} a_g g \overset{\varphi_x}{\longmapsto} \sum\limits_{g\in G} a_g \rho(g)x$. Покажем, что φ_x — гомоморфизм линейных представлений. Имеем

$$\varphi_x\big(\Lambda(h)(\sum_{g\in G} a_g g)\big) \overset{\text{def}}{=} \varphi_x\big(\sum_{g\in G} a_g hg\big) = \sum_{g\in G} a_g \rho(hg)x = \rho(h)\big(\sum_{g\in G} a_g \rho(g)x\big) = \rho(h)\cdot\varphi_x\big(\sum_{g\in G} a_g g\big).$$

Заметим также, что $\varphi_x(e) = \rho(e)(x) = \mathcal{E}x = x$. Рассмотрим произвольный гомоморфизм представлений $\varphi\colon \Lambda \to \rho$. Тогда найдётся $x \in V$, для которого $\varphi = \varphi_x$. В самом деле, положим $x := \varphi(e)$. Тогда для базисных элементов имеем $\varphi(g) = \varphi(g\cdot e) = \varphi(\Lambda(g)e) = \rho(g)\varphi(e) = \rho(g)x = \varphi_x(g)$, т. е. никаких других гомоморфизмов, кроме φ_x, тут быть не может. Далее, применяя первое утверждение леммы Шура, получаем, что всякое неприводимое представление изоморфно подпредставлению регулярного представления. ■

Следствие 4.1. *Кратность вхождения неприводимого представления в регулярное представление равна его размерности:* $\sum\limits_{i=1}^{s} n_i^2 = \dim \mathbb{K}G = |G|$.

Утверждение 4.5. *Число неприводимых комплексных представлений равно размерности центра групповой алгебры и равно числу классов сопряжённости группы.*

□ Очевидно, что элемент лежит в центре алгебры тогда и только тогда, когда он коммутирует с базисом, т. е. если $x = \sum\limits_{g\in G} a_g g$, то $x \in Z(\mathbb{C}G) \Leftrightarrow hx = xh \ \forall\, h \in G$. А это значит, что $hxh^{-1} = x \Leftrightarrow \sum\limits_{g\in G} a_g hgh^{-1} = \sum\limits_{g\in G} a_g g$. Таким образом, у вектора должны быть одинаковые координаты при сопряжённых базисных элементах. Поэтому можно сгруппировать сопряжённые элементы из каждого класса и вынести их за скобки. Следовательно, каждый базисный вектор центра — это сумма элементов в некотором классе сопряжённости. По следствию 3.8 основной теоремы число неизоморфных неприводимых модулей (а вместе с тем и число неприводимых представлений) равно размерности центра алгебры. ■

4.3. Линейные комплексные представления различных классов групп

4.3.1. Представления абелевых групп

Здесь и далее предполагаем, что $\mathbb{K} = \mathbb{C}$. Всякое неприводимое комплексное представление абелевой группы будет одномерным, т. е. $\chi\colon G \to \mathbf{GL}_1(\mathbb{C}) = \mathbb{C}^*$. Эквивалентность представлений в силу коммутативности $\mathbb{C}^*$ есть обычное равенство. Разложим группу на циклические: $G = \langle a_1\rangle_{n_1} \times \ldots \times \langle a_k\rangle_{n_k}$. Зададим представление на порождающих: $\chi(a_i) \in \mathbb{C}^*,\ a_i^{n_i} = 1 \Rightarrow \chi(a_i)^{n_i} = 1$, т. е. $\chi(a_i)$ — корни n_i-той степени из 1. Для каждого a_i есть n_i возможностей, поэтому всего $n_1 \ldots n_k = n = |G|$ различных гомоморфизмов χ. Разложим регулярное представление абелевой группы на неприводимые. Построим одномерные подпространства, являющиеся собственными для всех операторов. Для каждого χ рассмотрим вектор $v_\chi := \sum\limits_{g\in G} \chi(g^{-1})g \in \mathbb{C}G$. Он будет собственным, т. к.

$$hv_\chi = \sum_{g\in G} \chi(g^{-1})hg = \sum_{g\in G} \chi(h)\chi(g^{-1}h^{-1})hg = \chi(h)\sum_{g\in G} \chi\big((hg)^{-1}\big)(hg) = \chi(h)v_\chi,$$

и $\chi(h)$ — будет собственным значением. Проверка линейной независимости предоставляется читателю в качестве элементарного упражнения. Таким образом, $\mathbb{C}G$ является прямой суммой n собственных подпространств.

4.3.2. Одномерные представления произвольной конечной группы

Пусть G — конечная группа, $\chi\colon G \to \mathbb{C}^*$ — её одномерное представление. Тогда $G/\operatorname{Ker}\chi = \operatorname{Im}\chi \subset \mathbb{C}^*$ — абелева группа. Значит, она содержит коммутант G' группы G. Рассмотрим образ смежного класса gG' при гомоморфизме χ. Имеем $gG' \subseteq g\operatorname{Ker}\chi \Rightarrow \chi(gG') \subset \chi(g\operatorname{Ker}\chi) = \chi(g)$. Вывод: гомоморфизмы χ находятся в биективном соответствии с гомоморфизмами $G/G' \to \mathbb{C}^*$, и число одномерных комплексных представлений равно $|G/G'|$.

Задача 4.2. *Доказать, что у неабелевых групп существуют неприводимые многомерные представления.*

[1] На лекциях это утверждение не доказывалось. (Прим. наб.)

4.3.3. Линейные представления групп $\mathbf{D}_n$, $\mathbf{Q}_8$, $\mathbf{S}_n$, $\mathbf{A}_n$

Рассмотрим группу диэдра $\mathbf{D}_n$. Имеем $\mathbf{D}_n = \langle a, b\rangle$, где a — поворот, а b — симметрия. Определяющие соотношения: $a^n = e, b^2 = e, bab = a^{-1}$. Пусть n нечётно. Тогда $|\mathbf{D}_n/\mathbf{D}'_n| = 2$, т. е. существует 2 одномерных представления. Группа диэдра естественным образом действует на плоскости, поэтому положим $\rho(b) = b$, $\rho_k(a) = a^k$ при $k = 1, \ldots, \frac{n-1}{2}$. Соотношения, очевидно, выполняются. Такие представления неприводимы, поскольку собственный вектор симметрии имеет вещественные координаты, а собственный вектор поворота — нет, и значит, не может быть общих собственных векторов (т. е. одномерных инвариантных подпространств). Построенные представления будут неэквивалентными, так как $\rho_k(a)$ и $\rho_m(a)$ при $k \neq m$ имеют разные собственные значения, а потому матрицы не могут быть подобными. Итого получилось $2 + 2^2\frac{n-1}{2} = 2n = |\mathbf{D}_n|$. Значит, это все неприводимые представления группы $\mathbf{D}_n$ при нечётном n. В случае $n = 2k$ имеем $|\mathbf{D}_n/\mathbf{D}'_n| = 4$. Поступим аналогично, только число в данном случае $k = 1, \ldots, \frac{n-2}{2}$. Всего $4 + 2^2\frac{n-2}{2} = 2n$. Значит, это все представления.

Теперь рассмотрим группу $\mathbf{S}_3$. Можно было бы свести задачу к предыдущей, заметив, что $\mathbf{S}_3 \cong \mathbf{D}_3$. Но поступим по-другому. Имеем $|\mathbf{S}_3/\mathbf{S}'_3| = 2$. Значит, есть ещё одно двумерное представление. Пусть $V = \langle e_1, e_2, e_3\rangle$. Зададим представление (так называемое мономиальное представление), переставляющее базисные векторы, т.е если $\pi \in \mathbf{S}_3$, то $\pi e_i = e_{\pi(i)}$. Рассмотрим подпространство $L := \langle e_1 + e_2 + e_3\rangle$. Оно, очевидно, будет инвариантным. Ортогональное дополнение к нему $\langle e_1 + e_2 + e_3\rangle^\perp$ будет также инвариантным и неприводимым.

Перечислим неприводимые представления группы $\mathbf{Q}_8$. Вспомним, что $\mathbf{Q}_8 \subset \mathbb{H}$, $\mathbb{C} \subset \mathbb{H}$. Рассмотрим $\mathbb{H}$ как векторное пространство над $\mathbb{C}$ и зададим умножение на скаляры: $\lambda \cdot x := x\lambda$ для $\forall\, \lambda \in \mathbb{C}$, $x \in \mathbb{H}$. Представление зададим так: пусть $g \in \mathbf{Q}_8$, тогда положим $\rho(g)(x) = gx$ (обычное умножение слева). Это будет линейный оператор, так как $\rho(g)(\lambda \cdot x) = \rho(g)(x\lambda) = g(x\lambda) = (gx)\lambda = \lambda \cdot \big(\rho(g)(x)\big)$. Это представление двумерно, теперь покажем, что оно неприводимо. Допустим противное, пусть существует нетривиальное инвариантное подпространство. Тогда, так как $\langle \mathbf{Q}_8\rangle = \mathbb{H}$, то оно было бы инвариантным и относительно всех элементов из $\mathbb{H}$, т. е. это был бы левый идеал, а в алгебре с делением он совпадает со всей алгеброй. Поскольку $|\mathbf{Q}_8/\mathbf{Q}'_8| = 4$, то будет 4 одномерных представления. Получаем $4 + 2^2 = 8 = |\mathbf{Q}_8|$, т. е. перечислены все представления.

Рассмотрим представления группы $\mathbf{A}_n$. Пусть $V = \langle e_1, \ldots, e_n\rangle_{\mathbb{C}}$. Рассмотрим мономиальное представление, переставляющее базисные векторы. Как и в случае $\mathbf{S}_3$, оно приводимо и инвариантным подпространством будет $\langle e_1 + \ldots + e_n\rangle$. Покажем, что ортогональное дополнение $L := \langle e_1 + \ldots + e_n\rangle^\perp$ будет инвариантным и для $\mathbf{A}_n$. Имеем $L = \{x = (x_1, \ldots, x_n)\colon \sum x_i = 0\}$. Пусть $n \geqslant 4$. Докажем, что из любого ненулевого вектора путём перестановок координат можно получить базис L. Ясно, что если у вектора x больше трёх ненулевых координат, то можно тройным циклом переставить какие-то 3 из них и затем вычесть результат из исходного вектора, после чего останется только 3 ненулевых координаты. Поэтому без ограничения общности можно считать, что $x = (x_1, x_2, x_3, 0, \ldots, 0)$. Если одна из первых трёх координат (для определённости x_3) равна 0, то $x_1 = -x_2$ и можно построить набор векторов

$$
\begin{aligned}
u_1 &= (1, -1, \ \ 0, \ \ 0, \ \ 0, \ \ \ldots \ \ 0, \ \ 0)\\
u_2 &= (0, \ \ 1, -1, \ \ 0, \ \ 0, \ \ \ldots \ \ 0, \ \ 0)\\
u_3 &= (0, \ \ 0, \ \ 1, -1, \ \ 0, \ \ \ldots \ \ 0, \ \ 0)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
u_n &= (0, \ \ 0, \ \ 0, \ \ 0, \ \ 0, \ \ \ldots \ \ 1, -1)
\end{aligned}
$$

Они, как легко видеть, образуют базис L. А если все три координаты ненулевые, то рассмотрим вектор $y = (123) \cdot x = (x_3, x_1, x_2, 0, \ldots, 0)$. Если x и y линейно независимы, то вектора u_1 и u_2 содержатся в их линейной оболочке и можно, как и в первом случае, построить базис L. Если же x и y линейно зависимы, то тогда имеем $\begin{vmatrix} x_2 & x_3 \\ x_1 & x_2 \end{vmatrix} = x_2^2 - x_1x_3 = 0$. Рассмотрим ещё 2 вектора: $(12)(34) \cdot x = (x_2, x_1, 0, x_3, \ldots, 0)$, и $(234) \cdot x = (x_1, 0, x_2, x_3, 0, \ldots, 0)$. Они линейно независимы, так как $\begin{vmatrix} x_2 & x_3 & 0 \\ x_1 & 0 & x_3 \\ 0 & x_2 & x_3 \end{vmatrix} = -x_1x_3^2 - x_2^2x_3 = -2x_1x_3^2 \neq 0$. Далее рассуждения аналогичны. Итак, получаем, что ограничение мономиального представления на подпространство L неприводимо.

Отдельно разберём случай $n = 4$. Для группы $\mathbf{A}_4$ имеем $|\mathbf{A}_4/\mathbf{A}'_4| = 3$. Выше было построено неприводимое представление размерности $n - 1$, значит, в нашем случае $3 + 3^2 = 12 = |\mathbf{A}_4|$, т. е. это все неприводимые представления. Для группы $\mathbf{S}_4$ имеем 2 одномерных представления, так как $|\mathbf{S}_4/\mathbf{S}'_4| = 2$. Пусть ρ — мономиальное представление. Построим по нему ещё одно неприводимое представление. Положим $\rho'(\pi)(x) = (\operatorname{sgn}\pi)\rho(\pi)(x)$. Неприводимость следует из того, что при ограничении на подгруппу $\mathbf{A}_4$ получается обычное мономиальное представление. Покажем, что $\rho' \nsim \rho$. Допустим противное, т. е. что $\rho'(\pi) = C^{-1}\rho(\pi)C$ для $\forall\, \pi \in \mathbf{S}_4$. В частности, что должно быть верно для $\pi \in \mathbf{A}_4$, но в $\mathbf{A}_4$ ρ' совпадает с ρ, а потому C — скалярная матрица. Значит, $\rho'(\pi) = \rho(\pi)$

для $\forall\,\pi \in \mathbf{S}_4$, а это не так, если π — нечётная перестановка. Чтобы найти ещё одно двумерное представление, воспользуемся следующим обстоятельством. Если есть эпиморфизм групп $f\colon G \to H$, и ρ — неприводимое представление группы H, то есть и неприводимое представление $\widetilde{\rho}$ группы G той же размерности, которое можно определить по правилу $\widetilde{\rho}(g) := \rho(f(g))$. В случае группы S_4 имеем $\mathbf{V}_4 \lhd \mathbf{S}_4$, и $\mathbf{S}_4/\mathbf{V}_4 \cong \mathbf{S}_3$, поэтому можно рассмотреть эпиморфизм $f\colon \mathbf{S}_4 \to \mathbf{S}_3$ и получить искомое представление. Итого получается $2 + 2 \cdot 3^2 + 2^2 = 24$, т. е. ровно столько, сколько нужно.

4.3.4. Неприводимые комплексные представления и нормальные подгруппы простого индекса

Пусть $H \lhd G$, и $(G : H) = p$ — простое число. Тогда имеем $G/H = \langle aH \rangle_p$, $a^p = b \in H$, и любой элемент группы G записывается в виде $g = a^k \cdot h$, где $h \in H$. Пусть дано множество всех попарно неизоморфных неприводимых представлений группы H: $\mathcal{M} := \{\rho_1, \ldots, \rho_s\}$, и $\mathcal{M} \ni \rho\colon H \to \mathbf{GL}(V)$. Определим действие G на этом множестве: $\rho_g(h) := \rho(g^{-1}hg)$ для $\forall\, g \in G$. Если элемент g лежит в H, то $\rho_g(h) = \rho(g)^{-1}\rho(h)\rho(g)$ для $\forall\, h \in H$, т. е. $\rho_g \sim \rho$. Значит, $H \subseteq \mathrm{St}(\rho)$. Поскольку $(G : H)$ — простое число, то промежуточных подгрупп между G и H нет. Поэтому возможно только 2 случая: $\mathrm{St}(\rho) = G$ и $\mathrm{St}(\rho) = H$.

В первом случае покажем, что можно продолжить представление ρ до представления всей группы G. Для этого достаточно задать $\rho(a)$, и при этом должны выполняться условия:

1° $\rho(a)^p = \rho(b)$;

2° $\rho(\underbrace{a^{-1}ha}_{\in H}) = \rho(a)^{-1}\rho(h)\rho(a)$ для любого $h \in H$.

Они же будут и достаточными условиями, поскольку если $g = a^k h$, то $\rho(g) = \rho(a)^k\rho(h)$ и свойства гомоморфизма легко проверяются. Поскольку $\mathrm{St}(\rho) = G$, то при действии любого элемента (в частности, элемента a) ρ остаётся на месте, т. е. $\rho_a \sim \rho$. Поэтому $\rho_a(h) = \rho(a^{-1}ha) = C^{-1}\rho(h)C$ для $\forall\, h \in H$. По индукции очевидным образом получаем, что $\rho(a^{-k}ha^k) = C^{-k}\rho(h)C^k$. Вспоминая, что $a^p = b$, получаем, что при $k = p$ имеем $\rho(b^{-1}hb) = C^{-p}\rho(h)C^p$. Так как $b \in H$, то $\rho(b^{-1}hb) = \rho(b)^{-1}\rho(h)\rho(b)$. Отсюда

$$C^p\rho(b)^{-1}\rho(h)\rho(b)C^{-p} = \rho(h) \;\Leftrightarrow\; \big[C^p\rho(b)^{-1}\big]\rho(h)\big[C^p\rho(b)^{-1}\big]^{-1} = \rho(h).$$

Но представление ρ неприводимо, и по лемме Шура $C^p\rho(b)^{-1}$ — скалярная матрица. Пусть $C^p\rho(b)^{-1} = \lambda^{-1}E$, где λ — некоторое комплексное число. Тогда $\rho(b) = (\sqrt[p]{\lambda}C)^p$. Вспомним теперь про равенство $\rho(a^{-1}ha) = C^{-1}\rho(h)C$. От умножения матрицы на ненулевой скаляр ничего не изменится, поэтому можно считать, что $C^p = \rho(b)$. Положим $\rho(a) = C$ и тем самым получим продолжение представления, но не единственное: пусть $\xi_0, \ldots, \xi_{p-1}$ — корни из 1 p-й степени. Тогда получаем p представлений: $\rho_i(a) = \xi_i C$. Остаётся показать, что они неэквивалентны. От противного: пусть $\rho_i \sim \rho_j$ при $i \neq j$. Тогда $\rho_i(g) = C^{-1}\rho_j(g)C$ для всех $g \in G$. В частности, это должно быть верно для $g \in H$, но в этом случае, очевидно, $\rho_i(g) = \rho(g)$. Значит, $\rho(g) = C^{-1}\rho(g)C$ для $\forall\, g \in H$, следовательно, C — скалярная матрица. Значит, $\rho_i(g) = \rho_j(g)$ для любого $g \in G$, но это неверно, если подставить $g = a$: справа и слева от знака равенства будут стоять различные корни из единицы. Случай 1 разобран.

Пусть теперь $\mathrm{St}(\rho) = H$. Тогда орбита ρ состоит из элементов $\rho, \rho_a, \rho_{a^2}, \ldots, \rho_{a^{p-1}}$. Возьмём p экземпляров пространства V и построим внешнюю прямую сумму $W := V_0 \oplus \ldots \oplus V_{p-1}$. На каждом из V_i рассмотрим представление ρ_{a^i} подгруппы H. Определим представление $\widetilde{\rho}\colon H \to \mathbf{GL}(W)$:

$$\widetilde{\rho}(h) := \begin{pmatrix} \rho(h) & & & 0 \\ & \rho_a(h) & & \\ & & \ddots & \\ 0 & & & \rho_{a^{p-1}}(h) \end{pmatrix}$$

Теперь зададим продолжение $\widetilde{\rho}$ на группу G, т. е. $\rho(a)$:

$$\widetilde{\rho}(a) := \begin{pmatrix} 0 & & & 0 & \rho(b) \\ E & 0 & & & 0 \\ & E & 0 & & \\ & & \ddots & 0 & \vdots \\ 0 & & & E & 0 \end{pmatrix}$$

Оно осуществляет циклический сдвиг подпространств: $V_0 \mapsto V_1$, $V_1 \mapsto V_2, \ldots$ Проверка условий **1°** и **2°** выполняется «в лоб» умножением матриц. Докажем, что получилось неприводимое представление $\widetilde{\rho}\colon G \to \mathbf{GL}(W)$. Пусть L — инвариантное подпространство в W. Тогда L будет инвариантным и относительно H. Разложим его на неприводимые: $L = L_1 \oplus \ldots \oplus L_k$ (относительно H). Докажем, что любое из L_i совпадает с одним из V_j.

Рассмотрим проекции L_i на V_j для всех j. Очевидно, они все не могут одновременно быть нулевыми. Тогда эти проекции будут ненулевыми гомоморфизмами неприводимых представлений, а по лемме Шура они должны быть изоморфизмами. Таким образом, $L = V_0 \oplus \ldots \oplus V_k$. Если $k \neq p-1$, то L, очевидно, не будет инвариантным подпространством (поскольку под действием $\widetilde{\rho}(a)$ переставляются *все* V_i). Значит, $L = W$.

Покажем, что так получаются все неприводимые представления G. Пусть в множестве $\mathcal{M}$ представления $\rho_1, \ldots, \rho_k$ имеют одноэлементные орбиты (случай 1) и их размерности соответственно $n_1, \ldots, n_k$, а остальные $\rho_{k+1}, \ldots, \rho_s$ имеют орбиты из p элементов и размерности $n_{k+1}, \ldots, n_s$ соответственно (случай 2). Имеем $\sum n_i^2 = |H|$. Для первых k представлений получаем p неэквивалентных представлений G. Для всех остальных получаем по одному представлению группы G, каждое размерности $p \cdot n_i$. Всего

$$pn_1^2 + \ldots + pn_k^2 + pn_{k+1}^2 + \ldots + pn_s^2 = p\sum n_i^2 = p|H| = |G|. \tag{3}$$

4.4. Характеры линейных представлений

4.4.1. Понятие характера

Определение. Пусть G — конечная группа, $\rho\colon G \to \mathbf{GL}_n(\mathbb{C})$ — матричное представление. *Характером представления* называется функция $\chi_\rho\colon G \to \mathbb{C}$, равная следу оператора $\rho(g)$, т. е. $\chi_\rho(g) := \operatorname{tr}\rho(g)$.

Перечислим основные свойства характеров:

1° Если $\rho_1 \sim \rho_2$, то $\chi_{\rho_1}(g) = \chi_{\rho_2}(g)$, так как след — инвариант линейного оператора.

2° Характеры постоянны на классах сопряжённости:

$$\chi_\rho(h^{-1}gh) = \operatorname{tr}\rho(h^{-1}gh) = \operatorname{tr}\rho(h)^{-1}\rho(g)\rho(h) = \operatorname{tr}\rho(g) = \chi_\rho(g). \tag{4}$$

3° $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$. В самом деле, если $|G| = n$, то $\rho(g)^n = \mathcal{E}$. Тогда все собственные значения $\lambda_1, \ldots, \lambda_n$ оператора $\rho(g)$ — комплексные корни из 1 степени n. Поскольку $\rho(g^{-1}) = \rho(g)^{-1}$, и $\lambda_i^{-1} = \overline{\lambda_i}$ для всех i, а след оператора есть сумма собственных значений, то $\chi(g^{-1}) = \overline{\chi(g)}$.

4° $\chi_{\rho_1\oplus\rho_2}(g) = \chi_{\rho_1}(g) + \chi_{\rho_2}(g)$. Это очевидно, поскольку матрица прямой суммы представлений блочно-диагональная, и след такой матрицы равен сумме следов блоков.

Рассмотрим групповую алгебру $\mathbb{C}G$. Пусть $r = \sum\limits_{g\in G} a_g g \in \mathbb{C}G$. Тогда $\rho(r) = \sum\limits_{g\in G} a_g\rho(g)$ и можно рассмотреть характер представления на всей групповой алгебре: $\chi_\rho(r) = \sum\limits_{g\in G} a_g\chi_\rho(g)$. Он будет линейной функцией на $\mathbb{C}G$.

4.4.2. Основная теорема о характерах

Рассмотрим пространство $\mathcal{X}$ всех комплекснозначных функций на группе G, постоянных на классах сопряжённых элементов. Пусть этих классов s штук и $|G| = n$. Имеем $\dim_{\mathbb{C}}\mathcal{X} = s$. Введём на $\mathcal{X}$ эрмитово скалярное произведение: для $f_1, f_2\colon G \to \mathbb{C}$ положим

$$(f_1, f_2) := \frac{1}{n}\sum_{g\in G}\overline{f_1(g)}f_2(g). \tag{5}$$

Теорема 4.6. *Пусть $\rho_1, \ldots, \rho_s$ — неприводимые представления группы G. Тогда характеры $\chi_i := \chi_{\rho_i}$ образуют ортонормированный базис в $\mathcal{X}$.*

□ Разложим $\mathbb{C}G$ в прямое произведение: $\mathbb{C}G = \mathbf{M}_{n_1}(\mathbb{C}) \times \ldots \times \mathbf{M}_{n_s}(\mathbb{C})$. Выберем нумерацию блоков так, что ρ_i — представление на минимальном левом идеале в $\mathbf{M}_{n_i}(\mathbb{C})$. Тогда $\rho_i = 0$ на $\mathbf{M}_{n_j}$ при $i \neq j$. Рассмотрим регулярное представление $\Lambda\colon G \to \mathbf{GL}(\mathbb{C}G)$. Напомним, что $\Lambda(h)(\sum\limits_{g\in G} a_g g) = \sum\limits_{g\in G} a_g hg$. Найдём характер регулярного представления χ_r. На базисных элементах имеем $\Lambda(h)(g) = hg$. Если $h = e$, то так как матрица элемента e есть единичная матрица размера $n \times n$, получаем, что $\chi_r(h) = n$. Если же $h \neq e$, то $hg \neq g$ (происходит перестановка базисных векторов), и на диагонали будут нули, т. е. $\chi_r(h) = 0$.

Пусть $e = e_1 \oplus \ldots \oplus e_s$, где e_i — единица $\mathbf{M}_{n_i}(\mathbb{C})$, и $e_i = \sum\limits_{g\in G} a_g g$. Найдём коэффициенты a_g. Умножив слева на g^{-1}, преобразуем равенство к виду

$$g^{-1}e_i = a_g + \sum_{h\neq g} a_h g^{-1}h. \tag{6}$$

Отсюда получаем $\chi_r(g^{-1}e_i) = na_g + 0 \;\Rightarrow\; a_g = \frac{1}{n}\chi_r(g^{-1}e_i)$. Но так как $\chi_r = \sum\limits_{i=1}^{s} n_i\chi_i$, то

$$a_g = \frac{1}{n}\sum_{j=1}^{s} n_j\chi_j(g^{-1}e_i). \tag{7}$$

Поскольку $g^{-1}e_i \in \mathbf{M}_{n_i}(\mathbb{C})$, то останется только одно слагаемое, т. е. $a_g = \frac{n_i}{n}\chi_i(g^{-1}e_i)$. Имеем

$$\chi_i(g^{-1}) = \chi_i(g^{-1}e) = \chi_i\big(\sum_{j=1}^{s} g^{-1}e_j\big) = \chi_i(g^{-1}e_i), \tag{8}$$

так как все слагаемые, кроме i-того, равны 0. Окончательно получаем $a_g = \frac{n_i}{n}\chi_i(g^{-1})$, а потому

$$e_i = \frac{n_i}{n}\sum_{g\in G}\chi_i(g^{-1})g. \tag{9}$$

Применим к последнему равенству характер χ_j. Если $i = j$, то

$$\chi_i(e_i) = n_i = \frac{n_i}{n}\sum_{g\in G}\chi_i(g^{-1})\chi_i(g). \tag{10}$$

Поскольку $\rho_i(e_i)$ — единичная матрица со следом n_i, то $\frac{1}{n}\sum\limits_{g\in G}\overline{\chi_i(g)}\chi_i(g) = 1$, то есть $(\chi_i, \chi_i) = 1$. Если же $i \neq j$, то очевидно, что $(\chi_i, \chi_j) = 0$, что и требовалось доказать. ■

Следствие 4.2. *Любое представление определяется своим характером.*

□ Пусть $\rho = \sum\limits_{i=1}^{s} k_i\rho_i$. Тогда $\chi_\rho = \sum\limits_{i=1}^{s} k_i\chi_i$. Имеем $k_i = (\chi_i, \chi_\rho)$. Значит, k_i однозначно определяются. ■

Следствие 4.3. *Представление неприводимо ⇔ скалярный квадрат его характера равен 1.*

□ Очевидно: $(\chi_\rho, \chi_\rho) = \sum\limits_{i=1}^{s} k_i^2 = 1$. Значит, все k_i, кроме одного, равны 0, что и даёт неприводимость. ■