Алгебра (материал дополняется)

(Ещё не)алгебраист

Содержание

1. Теория групп

1.1. **Теоремы Коши и Силова.**

Теорема 1.1.1 (Коши)**.** *Пусть G — конечная группа, p — простое число и p делит порядок G. Тогда в группе G найдётся элемент порядка p.*

Доказательство.

Докажем индукций по порядку $n = |G|$ группы G.

База: $n = p$. В этом случае $G \cong \mathbb{Z}/p\mathbb{Z}$ и в ней имеется элемент порядка p.

Шаг. Пусть для всех порядков, меньших n и кратных p утверждение доказано.

Если группа G абелева, то возьмём произвольный неединичный элемент $g \in G$. Если порядок g делится на p, то некоторая степень элемента g будет являться искомым элементом порядка p. Иначе рассмотрим факторгруппу $G/\langle g\rangle$. Её порядок меньше n и делится на p, поэтому по предположению индукции в $G/\langle g\rangle$ найдётся элемент h порядка p. Тогда его произвольный прообраз $h' \in G$ является элементом порядка, кратного p и снова его степень будет являться искомым элементом.

В случае, когда группа G не абелева воспользуемся формулой

$$|G| = |Z(G)| + \sum_{g\in X} |g^G| = |Z(G)| + \sum_{g\in X} \frac{|G|}{|C_G(g)|},$$

где X — множество уникальных представителей классов сопряжённости группы G, состоящих хотя бы из двух элементов. Если порядок центра делится на p, то нужный элемент лежит там по индукционному предположению. Иначе найдётся такой представитель $g \in X$, что число $\frac{|G|}{|C_G(g)|}$ не делится на p. Тогда порядок подгруппы централизаторов $C_G(g)$ кратен p. Так как g не лежит в центре, то эта подгруппа имеет меньший порядок, чем n, и в ней по индукционному предположению найдётся элемент порядка p. □

Пусть G — конечная группа, p — простое число и $|G| = p^k m$, где m взаимно просто с p. Подгруппа $H \leqslant G$, порядок которой равен p^k называет силовской p-подгруппой группы G.

Теорема 1.1.2 (Силов)**.** *Пусть G — конечная группа, p — простое число и $|G| = p^k m$, где m не кратно p. Тогда*

1. *для каждого i от 1 до k существует подгруппа порядка p^i в группе G;*
2. *для всех i, кроме k, всякая подгруппа порядка p^i вложена в подгруппу порядка p^{i+1};*
3. *все подгруппы порядка p^k в группе G сопряжены;*
4. *количество подгрупп порядка p^k сравнимо с 1 по модулю p и делит число m.*

Доказательство.

[1, существование]

Пусть $|G| = p^k m$. Пусть $\mathcal{X}$ — множество всех подмножеств мощности p^i из G. Тогда

$$|\mathcal{X}| = C_{p^k m}^{p^i} = \frac{(p^k m)!}{p^i!(p^k m - p^i)!} = \frac{p^k m}{p^i} \prod_{j=1}^{p^i-1} \frac{p^k m - j}{j}.$$

Если $X \in \mathcal{X}$ и $g \in G$, то $gM = \{gm \mid m \in M\} \in \mathcal{M}$. Так что G действует на $\mathcal{M}$ левыми сдвигами. В формуле, выражающей мощность $\mathcal{X}$ ни один множитель в произведении справа не делится на p, поэтому наибольшая степень p, делящая $|\mathcal{X}|$, — это p^{k-i}. Найдём орбиту $\{X_1, \ldots, X_s\}$, мощность s которой не делится на p^{k-i+1}. Положим

$$G_i = \{g \in G \mid gX_1 = X_i\}, 1 \leqslant i \leqslant s.$$

Множество G_1 — стабилизатор X_1 и, следовательно, подгруппа в G, а G_i — левые смежные классы G по G_1.

Покажем, что подгруппа G_1 имеет требуемый порядок p^i. Действительно, $|G_1| \cdot s = |G| = p^k m$. Так как s не делится на p^{k-i+1}, то $|G_1|$ делится на p^i и поэтому $|G_1| \geqslant p^i$. С другой стороны, возьмём $x \in X_1$. Тогда $G_1 x \subset X_1$. Поскольку $|X_1| = p^i$, то $|G_1| = p^i$.

[2, вложенность]

Пусть p^{i+1} делит $|G|$, P — подгруппа порядка p^i из G, $\mathcal{P}$ — класс подгрупп, сопряжённых с P элементами из G. Мы знаем, что $|\mathcal{P}| = |G : N_G(P)|$.

Если $|\mathcal{P}|$ не делится на p, то $|N_G(P)|$ делится на p^{i+1}, а потому по первой части пункта 1 теоремы в $N_G(P)/P$ существует подгруппа P^*/P порядка p. Тогда P^* — требуемая подгруппа G.

Пусть теперь $|\mathcal{P}|$ делится на p. Группа P действует на $\mathcal{P}$ сопряжениями, причём мощности орбит делят $|P|$, а потому имеют вид $p^{k_j}, k_j \geqslant 0$. Имеется по крайней мере одна одноэлементная орбита $\{P\}$ и $|\mathcal{P}|$ делится на p. Поэтому непременно найдётся и другая одноэлементная орбита $\{Q\}$. Но это означает, что P нормализует Q, поэтому PQ есть подгруппа и, более того, p-подгруппа. Последнее следует из того, что $|PQ| = |Q| \cdot |PQ/Q|$ и того, что $PQ/Q \simeq P/P \cap Q$. Применяя к PQ то сопряжение группы G, которое переводит Q в P, мы получим p-подгруппу $P'P$, содержащую P в качестве собственной нормальной подгруппы. Снова по первой части теоремы в $P'P/P$ найдётся подгруппа P^*/P порядка p, тогда P^* — требуемая подгруппа.

[3, 4]

Пусть S — непустое множество подгрупп порядка p^k, инвариантное относительно действия группы G сопряжениями. Покажем, что порядок S сравним с 1 по модулю p.

Действительно, пусть $H \in S$ — подгруппа порядка p^k. Рассмотрим действие H на S сопряжениями. Порядок всякой орбиты делит p^k. Тогда либо порядок орбиты делится на p, либо она состоит ровно из одной подгруппы. Если $\{H'\}$ — одноэлементная орбита, то H нормализует H'. Тогда группа HH' содержится в $N_G(H')$ и H' нормальна в HH'. Отсюда $|HH'| = |H'| \cdot |HH'/H'| = |H'| \cdot |H/H \cap H'|$ является степенью числа p. Так как p^k — набольшая степень p, делящая порядок G, то $H = HH' = H'$. Таким образом, одноэлементная орбита ровно одна и $|S| \equiv 1 \pmod p$.

Из доказанного следует, что множеств подгрупп порядка p^k, инвариантных относительно сопряжения, не может быть двух. Иначе порядок объединения двух инвариантных подмножеств не был бы сравним с 1 по модулю p. Тогда все подгруппы порядка p^k сопряжены, их количество сравнимо с 1 по модулю p и делит порядок группы G.

$\square$

1.2. **Простые группы.** Группа называется простой, если в ней нет собственных нормальных подгрупп.

Теорема 1.2.1. *Группы A_n при $n \neq 4$ просты.*

Доказательство. [1] Группы A_1, A_2, A_3 имеют порядки 1, 1, 3 соответственно, а потому просты.

Группа A_4 содержит четверную группу Клейна $V_4 = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}$, которая нормальна в A_4. Следовательно, A_4 не проста.

Таким образом, теорему необходимо доказать при $n \geqslant 5$.

Дальнейшее доказательство теоремы опирается на ряд следующих вспомогательных утверждений.

Теорема 1.2.2. *Группа A_n порождается тройными циклами.*

Доказательство. Мы знаем, что каждая подстановка есть произведение циклов длины 2 (транспозиций). Так как подстановки в A_n чётны, то они равны произведению чётного числа транспозиций. Рассмотрим различные (по числу общих символов) варианты произведения двух соседних транспозиций:
$(ij)(kl) = (ijk)(jkl)$, если i, j, k, l все различны (нуль общих символов),
$(ij)\,(jk) = (ijk)$, если i, j, k различны (один общий символ), и, наконец,
$(ij)\,(ij) = 1$.

Таким образом, сгруппировав транспозиции по две, мы сможем представить произведение четного числа транспозиций как произведение циклов длины 3. $\square$

Лемма 1.2.3. *Пусть N нормальная подгруппа в A_n, $n \geqslant 5$. Если N содержит тройной цикл $(ijk) \in N$, то $N = A_n$.*

Доказательство. Возьмём произвольный тройной цикл (abc), возьмём подстановку $\sigma = \begin{pmatrix} i & j & k & u & v & \dots \\ a & b & c & u' & v' & \dots \end{pmatrix}$, такую что $u', v' \neq a, b, c$ и $u', v' \in \{i, j, k, u, v\}$, далее все элементы переходят в себя. При необходимости меняем u', v' местами: одна из таких подстановок будет чётной, выберем ее. Получаем $\sigma\,(ijk)\,\sigma^{-1} = (abc) \in N$, так как $N \lhd A_n$. Следовательно, подгруппе N принадлежат все тройные циклы. Отсюда (по предыдущей лемме) $N = A_n$. $\square$

Лемма 1.2.4. *Если $N \lhd A_n$ и содержит подстановку σ, у которой в разложении на независимые циклы встречается цикл длины $\geqslant 4$, то $N = A_n$.*

---

[1] Сделано на основе лекций по алгебре, читавшихся в Красноярском государственном университете

Доказательство. Пусть $\sigma = (ijkl\ldots)\ldots \in N$. Тогда $\tau = \underbrace{(ijk)\sigma(ijk)^{-1}}_{\in N}\underbrace{\sigma^{-1}}_{\in N} = (ijl) \in N$, то есть N содержит цикл длины 3. Следовательно (по лемме о порождении A_n), $N = A_n$. $\square$

Лемма 1.2.5. *Если $N \lhd A_n$ и содержит подстановку σ, у которой в разложении на независимые циклы встречается цикл длины $\geqslant 3$, а также еще какие-либо нетривиальные циклы, то $N = A_n$.*

Доказательство. Пусть $\sigma = (ijk)(lm\ldots)\ldots \in N$. Тогда $\tau = \underbrace{(jkl)\sigma(jkl)^{-1}}_{\in N}\underbrace{\sigma^{-1}}_{\in N} = (iljkm) \in N$. Следовательно (по предыдущей лемме), $N = A_n$. $\square$

Лемма 1.2.6. *Если $N \lhd A_n$ ($n \geqslant 5$) и содержит подстановку σ, у которой в разложении на независимые циклы содержатся только циклы длины 2, то $N = A_n$.*

Доказательство. Если $\sigma = (ij)\,(ab)$, то, так как у нас не менее пяти символов, $\exists c \notin \{i, j, a, b\}$. Тогда $\tau = (ijc)\,\sigma\,(ijc)^{-1}\,\sigma^{-1} = (icj) \in N$, следовательно (по лемме 1.2.3), $N = A_n$.

Если $\sigma = (ij)\,(ab)\,(uv)\,(pq)\ldots$, то $(ja)(bu)\sigma(bu)\,(ja)\,\sigma^{-1} = (iub)\,(jav) \in N$, следовательно (по предыдущей лемме), $N = A_n$. $\square$

Теперь, собственно, докажем теорему 1.2.1. Возьмём произвольную нетривиальную подстановку $\sigma \in N$. Она удовлетворяет условию одной из предыдущих лемм, следовательно $N = A_n$. Теорема доказана. $\square$

1.3. **Полупрямое произведение групп.**

Теорема 1.3.1. *Следующие утверждения о группах G, N и H эквивалентны:*

(1) *имеется расщепляющаяся точная последовательность*

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r] & G \arrow[r] & H \arrow[l, bend right, dashed, "s"'] \arrow[r] & 1; \end{tikzcd}$$

(2) *в группе G имеются подгруппы N' и H', изоморфные N и H, соответственно, такие, что $N' \lhd G$, $N'H' = G$ и $N' \cap H' = \{e\}$;*

(3) *существует такой гомоморфизм $\varphi\colon H \to \mathrm{Aut}\,(N)$, что группа G изоморфна группе пар $(n, h) \in N \times H$ с умножением заданным по правилу $(n_1, h_1)(n_2, h_2) = (n_1\varphi(h_1)(n_2), h_1h_2)$.*

Доказательство.

[1 ⇒ 2]

Пусть $i\colon N \to G$ — вложение и $\pi\colon G \to H$ — проекция из точной последовательности. Положим $N' = i(N)$ и $H' = s(H)$. Так как $N' = \ker\pi$, то N' нормальна в G. Имеем $s \circ \pi = \mathrm{Id}_H$ по определению расщепляющейся точной последовательности групп. Тогда $H' \cap N' = H' \cap \ker\pi = \{e\}$. Для всякого элемента $g \in G$ имеем $\pi(s(\pi(g))) = \pi(g)$. Положим $h' = s(\pi(g))$. Тогда $gh'^{-1} \in \ker\pi = N'$ и поэтому $G = N'H'$.

[2 ⇒ 3]

Пусть $f\colon N \to N', g\colon H \to H'$ — изоморфизмы. Зададим $\varphi\colon H \to \mathrm{Aut}\,(N)$ по правилу $\varphi\colon h \mapsto (n \mapsto f^{-1}(g(h)f(n)g(h)^{-1}))$. Обозначим через K группу пар $(n, h) \in N \times H$ с указанным правилом умножения. Положим $k\colon K \to G$ равным $k\colon (n, h) \mapsto f(n)g(h)$. По построению φ отображение k является гомоморфизмом:

$$k\big((n_1, h_1)(n_2, h_2)\big) = k\big((n_1\varphi(h_1)(n_2), h_1h_2)\big) = k\big((n_1f^{-1}(g(h_1)f(n_2)g(h_1)^{-1}), h_1h_2)\big) =$$

$$= f(n_1)g(h_1)f(n_2)g(h_1)^{-1}g(h_1h_2) = f(n_1)g(h_1)f(n_2)g(h_2) = k\big((n_1, h_1)\big)k\big((n_2, h_2)\big).$$

[3 ⇒ 1]

Пусть, как в доказательстве предыдущей импликации K — группа пар $(n, h) \in N \times H$ с указанным правилом умножения и $k\colon K \to G$ — изоморфизм.

Положим $i\colon N \to G$ равным $i\colon n \mapsto k\big((n, e_H)\big)$ и $\pi\colon G \to H$ равным $\pi = \mathrm{pr}_H \circ k^{-1}$, где pr_H — гомоморфизм проекции K на H. Как композиция инъекции и изоморфизма i инъективно, аналогично π сюръективно как композиции изоморфизма и сюръекции. По построению $\mathrm{Im}\, i \subset \ker \pi$. Если $g \in \ker \pi$, то $k^{-1} = (n, e_H)$ для некоторого $n \in N$. Тогда $i(n) = g$, поэтому $\ker \pi \subset \mathrm{Im}\, i$ и последовательность ниже точна:

$$1 \longrightarrow N \xrightarrow{\ i\ } G \xrightarrow{\ \pi\ } H \longrightarrow 1.$$

Положим $s\colon H \to G$ равным $s\colon h \mapsto k\big((e_N, h)\big)$. По построению $\pi \circ s = \mathrm{Id}_H$ и последовательность расщепляется.

□

Для двух групп N и H группа G, удовлетворяющая одному из условий теоремы называется полупрямым произведением групп N и H и обозначается $N \leftthreetimes_\varphi H$ или $N \rtimes_\varphi H$, где $\varphi\colon H \to \mathrm{Aut}\,(N)$ — гомоморфизм из пункта 3. Если φ известно из контекста, то этот индекс опускается.

Теорема 1.3.2. *Пусть $p < q$ — простые числа. Тогда группа G порядка pq является полупрямым произведением $\mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$, где $\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}\,(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$ — гомоморфизм. Более того, либо группа G изоморфна группе $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$, либо p делит $q-1$ и группа G изоморфна группе, заданной образующими и соотношениями как $\langle x, y \mid x^q, y^p, yxy^{-1}x^{-m}\rangle$ для всякого $m = r^{\frac{q-1}{p}}$, где r — первообразный корень по модулю q.*

Доказательство. По теореме Коши в группе G порядка pq существует элемент a порядка q и элемент b порядка p. Так как p — наименьшее простое число, делящее порядок G, то подгруппа $\langle a\rangle$ нормальна в G. Факторгруппа $G/\langle a\rangle$ изоморфна $\mathbb{Z}/p\mathbb{Z}$. Отображение образующей группы $\mathbb{Z}/p\mathbb{Z}$ в элемент b индуцирует сечение $s\colon \mathbb{Z}/p\mathbb{Z} \to G$ точной последовательности

$$\begin{tikzcd} 1 \arrow[r] & \mathbb{Z}/q\mathbb{Z} \arrow[r] & G \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[l, dashed, bend right, "s"'] & 1 \end{tikzcd}$$

поэтому G является полупрямым произведением $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

Группе G соответствует некоторый гомоморфизм $\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}\,(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$ и наоборот, такому гомоморфизму соответствует группа некоторая G.

В общем случае, это не биективное соответствие, но тривиальному гомоморфизму соответствует группа $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$ и наоборот этой группе соответствует только тривиальный гомоморфизм.

Если φ — нетривиальный гомоморфизм, то p обязано делить $\mathbb{Z}/q\mathbb{Z}$. Фиксируем первообразный корень r по модулю q и положим $m = r^{\frac{q-1}{p}}$ и $K = \langle x, y \mid x^q, y^p, yxy^{-1}x^{-m}\rangle$. В силу соотношений, определяющих группу K, каждый её элемент может быть представлен в виде $x^s y^t$, где $0 \leqslant s < q$ и $0 \leqslant t < p$, поэтому группа K состоит не более чем из pq элементов. Построим сюръективный гомоморфизм $f\colon K \to G$. Из сказанного выше, в группе G выполнено равенство $bab^{-1} = a_1^m$ для некоторого $1 < m_1 < q$, причём $a = b^p a b^{-p} = a^{(m_1^p)}$. Поэтому $m_1^p \equiv 1 \mod q$. Так как $m_1 \neq 1$, то оно является $\frac{q-1}{p}$-й степенью некоторого первообразного корня r_1 по модулю q. Существует число n взаимно простое с $q-1$ такое, что $r_1^n = r$, поэтому $m_1^n = m$ и $b^n a b^{-n} = a^{m_1^n} = a^m$, элемент b^n имеет порядок p. Определим гомоморфизм f на образующих по правилу $f\colon x \mapsto a, y \mapsto b^n$. Так как G порождается элементами a и b^n, то f сюръективно и, следовательно, изоморфизм.

□

1.4. **Теорема Жордана-Гёльдера.**

Теорема 1.4.1 (Жордан, Гельдер)**.** *Пусть G — конечная группа. Тогда существует композиционный ряд*

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{e\},$$

причём число n и набор простых групп $\{G_i/G_{i+1}\}_{i=0}^{n-1}$ определены однозначно.

Доказательство.

[существование]

Индукция по мощности группы G.

База: $|G| = 1$. Тогда $G = G_0 = \{e\}$.

Шаг. Если G проста, то возьмём ряд $G = G_0 \rhd G_1 = \{e\}$. Иначе найдём в группе G максимальную нормальную подгруппу G_1, не совпадающую с G. Группа G_0/G_1 проста, иначе её собственную нормальную подгруппу можно было бы поднять до нормальной подгруппы в группе G и G_1 не была бы максимальной. Поскольку порядок группы G_1 меньше порядка G_0, поэтому для неё композиционный ряд для G_1 существует по индукционному предположению.

[единственность]

Индукция по порядку группы G.

База индукции: $|G| = 1$ или G проста. Тогда $G = G_0 = \{e\}$ в первом случае и $G = G_0 \rhd G_1 = \{e\}$ во втором случае.

Шаг. Пусть имеются два композиционных ряда

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{e\},$$
$$G = G_0 \rhd H_1 \rhd \ldots \rhd H_m = \{e\}.$$

Если $G_1 = H_1$, то теорема следует из индукционного предположения для G_1 и H_1. Иначе положим $K_2 = G_1 \cap H_1$. Для группы K имеется композиционный ряд

$$K_2 \rhd K_3 \rhd \ldots \rhd K_r = \{e\}.$$

Так как G_1 и H_1 нормальны в G, то G_1H_1 — нормальная подгруппа в G. Так как G_1 и H_1 были максимальными нормальными подгруппами в G, не совпадающими с G и не были тривиальными, то $G_1H_1 = G$.

По теореме об изоморфизме имеем

$$G/H_1 \cong G_1H_1/H_1 \cong G_1/(G_1 \cap H_1) \cong G_1/K_2,$$
$$G/G_1 \cong G_1H_1/G_1 \cong H_1/(G_1 \cap H_1) \cong H_1/K_2.$$

Тогда группы G_1/K_2 и H_1/K_2 просты. Поэтому имеются композиционные ряды

$$G_1 \rhd K_2 \rhd K_3 \rhd \ldots \rhd K_r = \{e\},$$
$$H_1 \rhd K_2 \rhd K_3 \rhd \ldots \rhd K_r = \{e\}.$$

По индукционному предположению наборы простых групп

$$\{G_1/K_2, K_2/K_3, \ldots, K_{r-1}/K_r\} = \{G_1/G_2, G_2/G_3, \ldots, G_{n-1}/G_n\}$$

совпадают. Следовательно, $r = n$. Аналогично, наборы простых групп

$$\{H_1/K_2, K_2/K_3, \ldots, K_{r-1}/K_r\} = \{H_1/H_2, H_2/H_3, \ldots, H_{m-1}/H_m\}$$

совпадают и $n = r = m$. Тогда совпадают наборы

$$\{G/G_1, G_1/G_2, G_2/G_3, \ldots, G_{n-1}/G_n\} = \{G/G_1, G_1/K_2, K_2/K_3, \ldots, K_{r-1}/K_r\} =$$
$$= \{G/H_1, H_1/K_2, K_2/K_3, \ldots, K_{r-1}/K_r\} = \{G/H_1, H_1/H_2, H_2/H_3, \ldots, H_{m-1}/H_m\}.$$

Первое и третье равенство получаются из доказанных ранее добавлением G/G_1 и G/H_1 соответственно. Второе равенство верно, так как $G/G_1 \cong H_1/K_2$ и $G/H_1 \cong G_1/K_2$.

$$\begin{array}{ccccccccccc}
 & & G_1 & \rhd & G_2 & \rhd & G_3 & \rhd & \ldots & \rhd & G_n = \{e\} \\
 & \triangledown & & \vartriangle & & & & & & & \\
G_0 = G_1H_1 & & & & G_1 \cap H_1 = K_2 & \rhd & K_3 & \rhd & \ldots & \rhd & K_r = \{e\} \\
 & \vartriangle & & \triangledown & & & & & & & \\
 & & H_1 & \rhd & H_2 & \rhd & H_3 & \rhd & \ldots & \rhd & H_m = \{e\}
\end{array}$$

$\square$

2. Теория колец

2.1. **Радикал Джекобсона.**

Теорема 2.1.1. *Пусть A — ассоциативное кольцо с двусторонней единицей. Тогда следующие определения подмножества* $\mathrm{Rad}\,(A)$ *эквивалентны:*

(1) $\mathrm{Rad}\,(A)$ *есть множество элементов $a \in A$ таких, что для всякого простого левого A-модуля M*
и $m \in M$ выполнено $am = 0$;
(2) $\mathrm{Rad}\,(A)$ *есть пересечение всех максимальных левых идеалов;*
(3) $\mathrm{Rad}\,(A) = \{a \in A \mid \forall x, y \in A\ 1 - xay$ *— двусторонний обратимый*$\}$*;*
(4) $\mathrm{Rad}\,(A)$ *есть множество элементов $a \in A$ таких, что для всякого простого правого A-модуля M и $m \in M$ выполнено $ma = 0$;*
(5) $\mathrm{Rad}\,(A)$ *есть пересечение всех максимальных правых идеалов.*

Множество $\mathrm{Rad}\,(A)$ *является двусторонним идеалом в A.*

Доказательство.

[$1 \Leftrightarrow 2$**]**

Согласно пункту 1 множество $\mathrm{Rad}\,(A)$ равно пересечению аннуляторов всех простых левых A-модулей.

Пусть M — простой левый A-модуль и $m \in M$. Докажем, что $\mathrm{Ann}\,(m)$ — максимальный левый идеал в A. Действительно, пусть $a \notin \mathrm{Ann}\,(m)$. Тогда имеем $am = n \neq 0$. Поскольку M прост, то $An = M$ и найдётся $b \in A$ такой, что $bn = m$. Отсюда $(1 - ba)m = m - bam = m - bn = m - m = 0$ и $1 - ba \in \mathrm{Ann}\,(m)$.

Так как $\mathrm{Ann}\,(M) = \bigcap\limits_{m \in M} \mathrm{Ann}\,(m)$, то имеем

$$\bigcap_{M\text{— простой}} \mathrm{Ann}\,(M) = \bigcap_{M\text{— простой}} \bigcap_{m \in M} \mathrm{Ann}\,(m) \supset \bigcap_{I\text{— макс. левый идеал}} I.$$

С другой стороны, всякий максимальный левый идеал I является аннулятором элемента $1+I$ в левом простом модуле A/I. Поэтому последнее включение является равенством.

[$1 \Rightarrow \mathrm{Rad}\,(A)$ **— двусторонний идеал]**

Аннулятор простого модуля является двусторонним идеалом, пересечение двусторонних идеалов остаётся двусторонним идеалом.

[$4 \Leftrightarrow 5$**]**

Следует из предыдущего для A^{op}.

[$2 \Leftrightarrow 3$**]**

Пусть $a \in A$ таков, что $1 - xay$ является двусторонним обратимым для всяких x и y. Если a не лежит в некотором максимальном левом идеале I, то найдутся $b \in A$ и $i \in I$ такие, что $ba + i = 1$. Однако, тогда $i = 1 - ba$ обратим, что невозможно. Противоречие показывает, что a лежит в пересечении всех максимальных левых идеалов.

Пусть теперь $r \in R = \bigcap\limits_{I\text{— макс. левый идеал}} I$. Предположим, что у $1 - xry$ нет левого обратного. Тогда он содержится в некотором левом максимальном идеале I.

Однако, $r \in R \subset I$ и R — двусторонний идеал по доказанному выше. Поэтому $ry \in R \subset I$ и $xry \in I$. Отсюда следует, что $1 \in I$ и мы приходим к противоречию.

Пусть теперь $u(1 - xry) = 1$. Тогда $u = 1 - uxry$. По доказанному выше u имеет левый обратный v. Следовательно, $v = vu(1-xry) = 1-xry$. Поэтому $(1-xry)u = 1$.

[$3 \Leftrightarrow 4$]

Следует из предыдущего для A^{op}.

[$\mathrm{Rad}\,(A)$ — двусторонний идеал]

Следует из определения, данного в пункте 1.

$\square$

Идеал $\mathrm{Rad}\,(A)$ кольца A называется радикалом Джекобсона.

2.2. **Дедекинд-конечные кольца.** Ассоциативное кольцо R с двусторонней единицей называется Дедекинд-конечным, если для любых двух его элементов a и b равенство $ab = 1$ влечёт $ba = 1$.

Теорема 2.2.1. *Следующие условия на ассоциативное кольцо R с двусторонней единицей эквивалентны:*

(1) *R — не Дедекинд-конечно;*
(2) *в R существует элемент a являющийся одновременно левым делителем 1 и левым делителем 0;*
(3) *в R существует элемент b являющийся одновременно правым делителем 1 и правым делителем 0.*

Доказательство.

[$1 \Rightarrow 2, 3$]

Пусть $ab = 1$ и $ba \neq 1$. Тогда $ba - 1 \neq 0$ и $a(ba - 1) = aba - a = (ab - 1)a = 0$. Аналогично $(ba - 1)b = bab - b = b(ab - 1) = 0$.

[$2 \Rightarrow 1$]

Пусть $ab = 1$ и $ac = 0$, $c \neq 0$. Если бы было выполнено $ba = 1$, то $c = bac = b0 = 0$, что противоречило бы предположению.

[$3 \Rightarrow 1$]

Следует из предыдущего для R^{op}.

$\square$

Пример. Фиксируем поле $\Bbbk$ и рассмотрим кольцо $\mathrm{End}_{\Bbbk}\,(\Bbbk[k])$ эндоморфизмов векторного пространства $\Bbbk[x]$ многочленов над $\Bbbk$. Пусть $\frac{d}{dx}$ — оператор формального дифференцирования и $\int_0^x$ — оператор формального взятия интеграла с переменным верхним пределом. Тогда $\frac{d}{dx}\int_0^x = \mathrm{Id}_{\Bbbk[x]}$, но $\int_0^x \frac{d}{dx} \neq \mathrm{Id}_{\Bbbk[x]}$. Поэтому кольцо $\mathrm{End}_{\Bbbk}\,(\Bbbk[k])$ эндоморфизмов кольца многочленов как векторного пространства не является Дедекинд-конечным. Также имеем

$$\tfrac{d}{dx}\left(\int_0^x \tfrac{d}{dx} - \mathrm{Id}_{\Bbbk[x]}\right) = \tfrac{d}{dx}\int_0^x \tfrac{d}{dx} - \tfrac{d}{dx} = \left(\tfrac{d}{dx}\int_0^x - \mathrm{Id}_{\Bbbk[x]}\right)\tfrac{d}{dx} = 0$$

и, аналогично,

$$\int_0^x \left(\tfrac{d}{dx}\int_0^x - \mathrm{Id}_{\Bbbk[x]}\right) = \int_0^x \tfrac{d}{dx}\int_0^x - \int_0^x = \left(\int_0^x \tfrac{d}{dx} - \mathrm{Id}_{\Bbbk[x]}\right)\int_0^x = 0.$$

3. Коммутативная алгебра

3.1. Классификация конечно порождённых модулей над областями главных идеалов.

Теорема 3.1.1. *Пусть R — область главных идеалов и M — конечно порождённый R-модуль. Тогда существует однозначно определённое число s и упорядоченный набор идеалов $R \neq (d_1) \supset \ldots \supset (d_s)$ таких, что*

$$M \cong \bigoplus_{i=1}^{s} R/(d_i).$$

Кроме того, существует однозначно определённое число t и набор (неупорядоченный) примарных идеалов $\mathfrak{q}_i$ такие, что

$$M \cong \bigoplus_{i=1}^{t} R/\mathfrak{q}_i.$$

Лемма 3.1.2. *Пусть R — ненулевое коммутативное кольцо. Тогда изоморфизм R-модулей $R^k \cong R^m$ равносилен равенству $k = m$.*

Доказательство. Из равенства показателей немедленно следует изоморфизм модулей. Докажем обратное.

Так как R — ненулевое кольцо, то оно обладает главным идеалом m. Пусть $\varphi\colon R^k \to R^m$ — изоморфизм. Рассмотрим индуцированное отображение

$$1 \otimes \varphi\colon (R/m) \otimes R^k \to (R/m) \otimes R^m.$$

Поскольку φ был изоморфизмом, то $1 \otimes \varphi$ также является изоморфизмом. Более того, $1 \otimes \varphi$ — изоморфизм R/m-модулей, то есть векторных пространств над полем R/m. Поэтому $k = m$. □

Пусть M — конечно порождённый свободный R-модуль. Рангом модуля M будем называть число образующих M. Согласно последней определение ранга корректно.

Лемма 3.1.3. *Пусть R — область главных идеалов и $M = R^k$ — свободный R-модуль. Пусть $N \subset M$ — его подмодуль. Тогда N свободно порождается над R, причём ранг N не превосходит ранга M.*

Доказательство. Докажем индукцией по k.

База индукции: $k = 1$. Пусть $m \in M$ — базисный элемент. Рассмотрим множество $I = \{r \in R \mid rm \in N\}$. Оно является идеалом в R и поэтому существует такое $a \in R$, что $I = (a)$. Тогда N порождается элементом $n = am$. Если $a = 0$, то $n = 0$ и N свободен. Проверим, что $\{n\}$ является базисом N в остальных случаях. Пусть для некоторого $b \in R$ выполнено равенство $bn = 0$. Тогда $0 = bn = b(am) = (ba)m$ и отсюда $ba = 0$. Так как R — область целостности, то либо $b = 0$, либо $a = 0$. Последний случай был рассмотрен ранее, поэтому $b = 0$ и $\{n\}$ — базис N.

Шаг индукции. Пусть $m_1, \ldots, m_k$ — базис M. Пусть $M' = Rm_k$ — свободный подмодуль, порождённый элементом m_k. Пусть $M'' = M/M'$. Тогда M'' является свободным модулем с $k-1$ образующей: $m_1 + Rm_k, \ldots, m_{k-1} + Rm_k$. Пусть N — подмодуль в M. Пусть $N' = N \cap M'$ и N'' — образ подмодуля N в M'' при отображении факторизации. Имеем $N/N' \cong N''$. Оба модуля N' и N'' являются подмодулями конечно порождённых модулей. Поэтому, по индукционному предположению, N' и N'' являются свободными модулями.

Если $N' = 0$, то $N \cong N''$ и теорема доказана. Пусть теперь n' — базис модуля N' и $n''_1, \ldots, n''_t$ — базис модуля N''. Выберем в N по одному прообразу n_i для каждого базисного элемента модуля N''. Покажем, что $n', n_1, \ldots, n_t$ порождают N, а затем, что они являются базисом N.

Пусть $n \in N$ и n'' — его образ в N''. Тогда для некоторых $a_1, \ldots, a_t \in R$ выполнено равенство $n'' = a_1 n''_1 + \ldots + a_t n''_t$. Тогда разность $n'' - (a_1 n_1 + \ldots + a_t n_t)$ лежит в ядре проекции из N на N'', то есть в N'. Поэтому n'' выражается через $n', n_1, \ldots, n_t$.

Проверим, что эти элементы образую базис N. Пусть для некоторых $a, a_1, \ldots, a_n \in R$ выполнено $an' + a_1 n_1 + \ldots + a_t n_t = 0$. Тогда в N'' выполнено $a_1 n''_1 + \ldots + a_t n''_t = 0$ из чего следует, что $a_1 = \ldots = a_t = 0$, так как $n''_1, \ldots, n''_t$ — базис N''. Тогда $an' = 0$ и уже $a = 0$, так как N' свободно порождён $n' \neq 0$.

Из индукционного предположения следует, что ранг N не превосходит $1 + (k - 1) = k$. □

Лемма 3.1.4 (Нормальная форма Смита)**.** *Пусть R — область главных идеалов и $M = R^k$ — свободный R-модуль. Пусть $N \subset M$ — его подмодуль. Тогда найдутся базис $m_1, \ldots, m_k$ модуля M и элементы $d_1, \ldots, d_k$ кольца R такие, что $(d_1) \supset \ldots \supset (d_k)$ и N свободно порождается ненулевыми элементами из набора $d_1 m_1, \ldots, d_k m_k$. Более того $d_1, \ldots, d_k$ определены однозначно с точностью до умножения на обратимые элементы кольца.*

Доказательство. Пусть $x_1, \ldots, x_k$ — базис M и $y_1, \ldots, y_s$ — базис N. Элементы $y_1, \ldots, y_s$ выражаются как линейные комбинации базисных $x_1, \ldots, x_k$. Запишем в матрицу C размера $k \times s$ коэффициенты, с которыми базисные x_i входят в разложение элементов y_j. Обратимые элементарные преобразования строк и столбцом матрицы C соответствуют замене базиса в M или N.

Пусть $a_{11}, \ldots, a_{1s}$ — первая строка матрицы. Можем считать, что она ненулевая, иначе поменяем её местами с ненулевой строкой. Так же можем считать, что $a_{11} \neq 0$, иначе поменяем столбцы. Пусть $(a) = (a_{11}, a_{12})$ — идеал в R. Тогда существуют $r_1, r_2, q_1, q_2 \in R$ такие, что $a = r_1 a_{11} + r_2 a_{12}$ и $a_{11} = q_1 a, a_{12} = q_2 a$. Отсюда $r_1 q_1 + r_2 q_2 = 1$. Тогда следующая матрица является обратимой:

$$\begin{pmatrix} r_1 & -q_2 & 0 & \ldots & 0 \\ r_2 & q_1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{pmatrix}$$

Умножим матрицу перехода C на эту матрицу. В новой матрице на позиции $(1,1)$ будет стоять элемент a. Повторив операцию для элементов на позициях $(1,1)$ и $(1,3)$ и далее мы добьёмся того, чтобы на позиции $(1,1)$ стоял НОД всей первой строки исходной матрицы. Элементарными преобразованиями строк сделаем нулевыми все остальные элементы строки. Проделаем аналогичную операцию с первым столбцом. Будем повторять процесс до тех пор, пока и первая строка и первый столбец не будут содержать единственный ненулевой элемент на позиции $(1,1)$. Процесс завершится за конечное время, так как возрастающая цепочка идеалов, порождённых элементом на позиции $(1,1)$ стабилизируется.

Повторим операцию, описанную выше, для подматрицы $(k-1)\times(s-1)$, полученной удалением первых строки и столбца. Далее, будем повторять операцию до тех пор, пока не образуется диагональная матрица

$$\begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ 0 & 0 & a_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{pmatrix}$$

Теперь покажем, как из этой матрицы получить матрицу, в которой каждый элемент на диагонали делит следующий. Пусть снова $(a)=(a_1,a_2)$ и $a=r_1a_1+r_2a_2, a_1=q_1a, a_2=q_2a$. Тогда $r_1q_1+r_2q_2=1$. Будем выполнять элементарные преобразования только первых двух строк и столбцов:

$$\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} a_1 & a_2 \\ 0 & a_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} a_1 & a_2 \\ 0 & a_2 \end{pmatrix}\begin{pmatrix} r_1 & -q_2 \\ r_2 & q_1 \end{pmatrix} = \begin{pmatrix} a & -q_2a_1+q_1a_2 \\ r_2a_2 & q_1a_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} a & 0 \\ 0 & * \end{pmatrix}$$

При всех преобразованиях определитель сохранился, а на позиции $(2,2)$ теперь стоит элемент, кратный a. Повторяя эту операцию для всех пар диагональных элементов мы добьёмся требуемого. Коэффициентами d_i будут служить элементы на диагонали, а в качестве базиса m_i следует взять получившийся в ходе замены базис M.

При умножении на матрицы в ходе рассуждения выше наибольший общий делитель миноров каждого фиксированного размера продолжал делиться на НОД миноров того же размера до умножения. Так как матрицы и преобразования были обратимы, то наибольший общий делитель всех миноров фиксированного размера не изменится в ходе преобразований. Поэтому элементы d_i определены однозначно с точностью до умножения на обратимые элементы кольца R. □

Доказательство теоремы о классификации. Пусть M — k-порождённый R-модуль. Пусть $m_1,\dots,m_k$ — образующие M. Накроем M свободным модулем R^k с образующими $x_1,\dots,x_k$, посредством отображения, сопоставляющее элементу x_i элемент m_i. Пусть N — ядро этого гомоморфизма.

По лемме о нормальной форме Смита существует базис $y_1,\dots,y_k$ и определённые с точностью до умножения на константу элементы $d_1\mid\dots\mid d_k$ такие, что $d_1y_1,\dots d_ky_k$ свободно порождают подмодуль N. Удалим все обратимые d_i и перенумеруем их. Тогда $M\cong R^k/N\cong\bigoplus\limits_{i=0}^{s}R/(d_i)$. Идеалы $R\neq(d_1)\supset\dots(d_s)$ определены однозначно.

По китайской теореме об остатках и факториальности кольца R модуль $R/(d_i)$ однозначно раскладывается в прямую сумму модулей вида $R/(p_j^{a_j})$, где p_j — простой элемент. Единственность разложения M следует из возможности восстановить d_i по разложению на факторы по примарным идеалам.

□

Список литературы

[1] М.И. Каргаполов, Ю.И. Мерзляков *Теория групп*, Наука, 1996.
[2]