Алгебра, 1 курс

Фейгин Евгений Борисович

2 сентября 2020 г. — 10 октября 2020 г.

Формула оценки: $\dfrac{D+C+K+2E}{5}$*, где* D, C, K, E *— оценки за д/з, КР, коллоквиум и экзамен соответственно.*

Определение 1. Абелева группа — множество A с определённой на нём операцией $+$ со следующими свойствами:

- $\forall a, b : a + b = b + c$;
- $\forall a, b, c : (a + b) + c = a + (b + c)$;
- $\exists 0 \forall a : a + 0 = a$;
- $\forall a \exists (-a) : a + (-a) = 0$.

Определение 2. Кольцо — множество A с операциями $+$ и $\times$ со следующими свойствами:

- $(A, +)$ — группа;
- $a \times (b + c) = a \times b + b \times c$;
- $(b + c) \times a = b \times a + c \times a$.

Кроме того, у $\times$ могут быть такие дополнительные свойства:

- $\exists 1 : \forall a : a \times 1 = 1 \times a = a$ (если есть единица);
- $\forall a, b : a \times b = b \times a$ (если коммутативное кольцо);
- $\forall a, b, c : a \times (b \times c) = (a \times b) \times c$ (если ассоциативное кольцо);
- $\forall a, b : a \times b = 0 \implies a = 0 \vee b = 0$ (если нет делителей нуля).

Определение 3. Целостное кольцо — ассоциативное коммутативное кольцо с единицей без делителей нуля.

Определение 4. Поле — коммутативное ассоциативное кольцо с 1, такое, что $0 \neq 1$ и $\forall a \neq 0 \exists a^{-1} : aa^{-1} = 1$.

Замечание. Отсутствие делителей нуля в кольце не гарантирует, что это поле.

Определение 5. Подгруппа абелевой группы A — множество $B \subset A$, со следующими свойствами:

- $0 \in B$;
- $a \in B \implies (-a) \in B$;
- $a, b \in B \implies a + b \in B$.

Определение 6. Подкольцо — подгруппа $B \subset A$ такая, что $a, b \in B \implies a \times b \in B$.

Определение 7. Подполе — подкольцо $B \subset A$ такое, что $1 \in B$ и $a \in B \implies a^{-1} \in B$.

Определение 8. Комплексные числа — множество $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ (здесь i — формальный символ) с операциями сложения и умножения, определёнными следующим образом:

- $(a + bi) + (c + di) = (a + c) + (b + d)i$;
- $(a + bi) \times (c + di) = (ac - bd) + (bc + ad)i$.

Теорема 1. $\mathbb{C}$ — поле.

Доказательство. Вначале докажем, что $\mathbb{C}$ — кольцо (это очевидно). Кроме того,

$$a^2 + b^2 \neq 0 \implies (a + bi)\left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i\right) = 1,$$

значит, это поле. ■

Определение 9. Вещественная часть — число $\mathrm{Re}(a+bi)=a$.

Определение 10. Мнимая часть — число $\mathrm{Im}(a+bi)=b$.

Определение 11. Модуль комплексного числа — число $N(a+bi)=\sqrt{a^2+b^2}$.

Определение 12. Аргумент комплексного числа — множество $\mathrm{Arg}(a+bi)$ чисел φ таких, что $a+bi=N(a+bi)(\cos\varphi+i\sin\varphi)$.

Тригонометрическая запись числа. Будем записывать

$$z=a+bi=N(z)(\cos\mathrm{Arg}(z)+i\sin\mathrm{Arg}(z)).$$

Тогда получится, что

$$z_1z_2=(N(z_1)N(z_2))\left(\cos(\mathrm{Arg}(z_1)+\mathrm{Arg}(z_2))+i\sin(\mathrm{Arg}(z_1)+\mathrm{Arg}(z_2))\right).$$

Определение 13. Автоморфизм поля — отображение $f:K\to K$ такое, что $f(a)+f(b)=f(a+b)$ и $f(a)f(b)=f(ab)$. Автоморфизмы кольца и абелевой группы определяются аналогично.

Определение 14. Изоморфизм групп — отображение $f:A\to B$ такое, что $f(0_A)=f(0_B)$ и $f(a_1+_Aa_2)=f(a_1)+_Bf(a_2)$. Если такое отображение существует, то A и B называются изоморфными.

Заметим, что $a+bi\mapsto\overline{a+bi}:=a-bi$ — автоморфизм. Множество его фиксированных точек — это $\mathbb{R}$, и легко доказать, что $z\overline{z},z+\overline{z}\in\mathbb{R}$.

Рассмотрим уравнение $z^n=1$. Если $z=\cos\varphi+i\sin\varphi$, то $z^n=\cos n\varphi+i\sin n\varphi=1$, т.е. $\varphi=\frac{2\pi k}{n}$. Это будет n корней (для $k=0,\dots,n-1$; будем обозначать $\xi_r=\cos\frac{2\pi r}{n}+i\sin\frac{2\pi r}{n}$), и они делят окружность $N(z)=1$ на n равных частей. Понятно, что если z_1,z_2 — корни, то и z_1z_2 тоже, кроме того, 1 — корень. Тогда это абелева группа по умножению, которая изоморфна $\mathbb{Z}/n\mathbb{Z}$ (по сложению).

Определение 15. Первообразный корень из 1 — такой корень ξ_k, что $\forall n\exists m:(\xi_k)^m=\xi_n$.

Лемма 2. ξ_k (r-и степени) первообразный тогда и только тогда, когда $(k,r)=1$.

Определение 16. Фактор-множество — M/R множество классов эквивалентности на множестве M по отношению эквивалентности R.

Определение 17. Отображение проекции — функция $\pi:M\to M/R$, переводящая любой элемент a в множество $R(a)$ элементов, эквивалентных a.

Лемма 3. π — сюръекция и $\pi^{-1}(x)=\{a\in M,a\sim x\}$.

Пусть на M есть операция $*$. Будем говорить, что $*$ согласована с отношением R, если из того, что $a\sim a',b\sim b'$ следует, что $a*b\sim a'*b$. Тогда на M/R возникает индуцированная операция $*$.

Если $*$ согласована с R, то индуцированная операция наследует многие свойства $*$, в частности: ассоциативность, коммутативность, наличие нейтрального элемента.

Теорема 4. $\mathbb{Z}/n\mathbb{Z}$ поле тогда и только тогда, когда n простое.

Доказательство. Пусть $n=n_1*n_2$. Тогда $[n_1]_n[n_2]_n=[n]_n=[0]_n$.

С другой стороны, пусть n простое. Тогда для любого $m=1,2,\dots,n-1$ выполняется $(m,n)=1$, тогда $\exists u,v:um+vn=1\iff[m]_n[u]_n=[1]_n$. Тогда u обратно к m. ■

Определение 18. Характеристика поля — минимальное такое $k\in\mathbb{N}$, что $\underbrace{1+\ldots+1}_{k}=0$ (имеются в виду 0 и 1 из этого поля). Если такого k нет, то характеристика равна 0.

Лемма 5. Если $\mathbb{K}$ — поле, то $\mathrm{char}\,\mathbb{K}$ — 0 или простое число.

Доказательство. Пусть $\mathrm{char}\,\mathbb{K}=n=n_1n_2$. Тогда $0=\underbrace{1+\ldots+1}_{n}=(\underbrace{1+\ldots+1}_{n_1})(\underbrace{1+\ldots+1}_{n_2})$, значит, у нас есть делители нуля. ■

Определение 19. Евклидово кольцо — целостное кольцо K с функцией нормы $N : K \setminus 0 \to Z_{\geqslant 0}$ со следующими свойствами:

- $N(ab) \geqslant N(a)$, причём равенство только если b обратим.
- $\forall a, b \in K, b \neq 0 \exists q, r \in K : a = bq + r, N(r) < N(b)$.

Примеры.

- $\mathbb{Z}; N(x) = |x|$.
- Пусть F — поле, тогда $F[x]$ с функцией $N(P) = \deg P$ подходит.

Лемма 6. $F[x]$ — евклидово кольцо.

Доказательство. Очевидно, что это целостное кольцо. Очевидно также, что $\deg fg \geqslant \deg f \deg g$ и равенство, только если какой-то из многочленов 0 степени, т.е. обратим. Докажем деление с остатком. Пусть $f = \sum f_i x^i, g = \sum g_i x^i, n = \deg f \geqslant \deg g = m$. Тогда рассмотрим $k = f - g\frac{f_n}{g_m}x^{n-m}$. Его степень меньше n, кроме того, $k \equiv f \mod g$, значит, можно проделать алгоритм Евклида. ■

Замечание. В этой лемме необходимо, чтобы F было полем. Например, в $\mathbb{Z}[x]$ не получится разделить $3x$ на $2x$ с остатком.

Теорема 7 (Безу). остаток от деления $f(x)$ на $x - c$ равен $f(c)$.

Доказательство. Следует из **Т. 6**. ■

Теорема 8. Многочлен $f(x) \in F[x]$ не может иметь в F более $\deg f$ корней.

Доказательство. Пусть c_1, c_2 — корни этого многочлена. Тогда $f = (x - c_1)f_1$ и $f(c_2) = (c_2 - c_1)f_1(c_2)$. Так как $c_1 - c_2 \neq 0$, то $f_1(c_2)$ имеет корень c_2. Индукция по $\deg f$. ■

Лемма 9. Пусть F — бесконечное поле. Тогда разные многочлены в $F[x]$ определяют разные функции на F.

Доказательство. Пусть $f_1, f_2 \in F[x]$ определяют одну и ту же функцию. Тогда $f_1 - f_2 = 0 \forall x$. Но $f_1 - f_2$ имеет конечную степень, а F бесконечное. Противоречие. ■

Определение 20. Кольцо формальных степенных рядов — множество сумм вида

$$K[[x]] = \{a_0 + a_1 x + a_2 x^2 + \ldots \mid x_i \in K\}.$$

Определение 21. Кольцо рядов Лорана — множество сумм вида

$$K((x)) = \{x^{-r}(a_0 + a_1 x + a_2 x^2 + \ldots) \mid x_i \in K, r \in \mathbb{N}\}.$$

Вернёмся к $K[x]$, причём будем считать, что K — это поле.

Определение 22. Неприводимый многочлен — простой элемент в кольце $K[x]$, т.е. такой многочлен P, что $P = fg \implies \deg f \cdot \deg g = 0$.

Определение 23. Факториальное кольцо — кольцо, в котором выполняется основная теорема арифметики, т.е. в котором каждый элемент раскладывается в конечное произведение простых единственным способом с точностью до перестановки и умножения на обратимые.

Лемма 10. Любое евклидово кольцо факториальное.

Доказательство. Разложение есть: пусть $x \in K$ не простое, тогда $\exists p, q : x = pq$ и p, q необратимые. Тогда $N(x) > N(p)$ и $N(x) > N(q)$, индукция по норме x.

Разложение единственно: линейное представление для НОД позволяет доказать, что если $q \mid ab$ и $(a, q) = 1$, то $q \mid b$, откуда и следует утверждение. ■

Определение 24. Гомоморфизм колец — функция $\varphi : K \to L$ такая, что $\varphi(k_1) + \varphi(k_2) = \varphi(k_1 + k_2)$ и $\varphi(k_1)\varphi(k_2) = \varphi(k_1 k_2)$.

Определение 25. Изоморфизм колец — биективный гомоморфизм.

Пример $\mathbb{R}[x]/(x^2 + 1)$ изоморфно $\mathbb{C}$ с $\varphi([ax + b]) = ai + b$.

Теорема 11. $K[x]/f$ является полем тогда и только тогда, когда f неприводим.

Доказательство. Пусть f приводим. Тогда $f = pq, \deg f > \deg p, \deg f > \deg q$. Тогда $[p] \neq [0] \neq [q]$, но $[pq] = 0$, т.е. в этом кольце есть делители 0.

Теперь пусть f неприводим. Докажем, что у любого класса $[g]_f \neq [0]$ есть обратный. Это так, т.к. $\exists u, v : gu + fv = 1$ (т.к. f неприводим $\implies (f, g) = 1$), тогда $[gu]_f = [1]_f$. ■

Теорема 12. Для любых n, p существует неприводимый многочлен степени n над $\mathbb{Z}/p\mathbb{Z}$, т.е. существует поле из p^n элементов. Кроме того, все поля, получающиеся таким образом, изоморфны.

Определение 26. Произведение колец — кольцо $K \times L = \{(a, b) \mid a \in K, b \in L\}$ с операциями $(a, b) + (c, d) = (a + c, b + d)$ и $(b, c) \cdot (c, d) = (ac, bd)$.

Теорема 13 (Китайская теорема об остатках). Пусть даны $n_1, \ldots, n_k, r_1, \ldots, r_k \in \mathbb{N}$, причём $(n_i, n_j) = 1$ и $0 \leqslant r_i < n_i$. Тогда $\exists N : R \equiv r_i \mod n_i$, и если N_1, N_2 удовлетворяют этому свойству, то $N_1 \equiv N_2 \mod n_1 \ldots n_k$.

Алгебраическая переформулировка. Пусть $n_1, \ldots, n_k \in \mathbb{N}$ и $(n_i, n_j) = 1$. Тогда

$$\mathbb{Z}/(n_1 n_2 \ldots n_k \mathbb{Z}) \simeq (\mathbb{Z}/n_1 Z) \times \ldots \times (\mathbb{Z}/n_k \mathbb{Z}).$$

Почему отсюда следует Т. 13. Рассмотрим $[R]_{n_1 \ldots n_k} = \varphi^{-1}([r_1]_{n_1} \times [r_2]_{n_2} \ldots \times [r_k]_{n_k})$.

Доказательство. Рассмотрим $\varphi(t) = (t \mod n_1, t \mod n_2, \ldots, t \mod n_k)$. Заметим, что $\varphi(p + q) = \varphi(p) + \varphi(q)$ и $\varphi(pq) = \varphi(p)\varphi(q)$. Докажем, что φ инъективно и сюръективно.

Инъективность. Пусть $\varphi(a) = \varphi(b)$. Тогда $a \equiv b \mod n_i$. Т.к. $(n_i, n_j) = 1$, то $a \equiv b \mod n_1 \ldots n_k$.

Сюръективность. Следует из количества элементов и инъективности. ■

Теорема 14 (КТО для многочленов). Пусть K — евклидово кольцо (в частности, работает для многочленов), $f_1, \ldots, f_k \in K$ и $(f_i, f_j) = 1$. Тогда $K/(f_1 f_2 \ldots f_k) \simeq \prod_j K/(f_j)$.

Доказательство. Рассмотрим ту же самую функцию φ, как и в **Т. 13**. Она является инъективным гомоморфизмом по той же самой причине. Докажем сюръективность. Пусть есть многочлены r_i. Определим $F_i = \prod_{j \neq i} f_j$. Мы знаем, что $(F_i, f_i) = 1$, значит, $\exists a_i, b_i : a_i F_i + b_i f_i = 1$. Рассмотрим $P = \sum v_i r_i F_i$. Тогда $P = f_i(\ldots) + F_i v_i r_i \equiv r_i \mod f_i$. ■

Определение 27. Циклическая группа — группа S, т.ч. $\exists a \in S \forall b \in S \exists n \in \mathbb{Z} : b = a^n$. Любая циклическая группа изоморфна либо $\mathbb{Z}$, либо $\mathbb{Z}/n\mathbb{Z}$ по сложению.

Определение 28. Гомоморфизм групп — отображение $\varphi : A \to B$ такое, что, $\varphi(e) = e$ и $\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$. Множество всех гомоморфизмов обозначается $\mathrm{Hom}(A, B)$ (которое является группой по сложению, т.е. $(\varphi + \psi)(a) = \varphi(a) + \psi(a)$).

Определение 29. Ядро гомоморфизма — множество $\mathrm{Ker}\,\varphi = \{a \in A \mid \varphi(a) = e\}$.

Определение 30. Подгруппа — подмножество группы, которое содержит e и замкнуто относительно сложения и взятия обратного.

Определение 31. Порядок элемента — такое минимальное число k, что $\underbrace{a + \ldots + a}_{k} = e$.

Определение 32. Произведение групп — группа $K_1 \times \ldots \times K_n$, состоящая из элементов $(k_1, \ldots, k_n), k_i \in K_i$, с поэлементным сложением.

Лемма 15. Пусть L целостное и $\varphi : K \to L$ — гомоморфизм. Тогда $\varphi \equiv 0$ или $\varphi(1) = 1$.

Доказательство. $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)^2$. Отсюда (т.к. кольцо целостное) либо $\varphi(1) = 1$, либо $\varphi(1) = 0$. В первом случае утверждение доказано, во втором $f(k) = f(1)f(k) = 0$. ■

Лемма 16. Пусть G циклическая и $H \subset G$ — подгруппа. Тогда H циклическая.

Теорема 17. Пусть $\mathbb{F}$ — поле, и $A \subset \mathbb{F}^*$ — конечная подгруппа. Тогда A циклическая.

Лемма 18. Пусть A — абелева группа, $b_1, b_2 \in A, \operatorname{ord} b_1 = m_1, \operatorname{ord} b_2 = m_2, (m_1, m_2) = 1$. Тогда $\operatorname{ord}(b_1 b_2) = m_1 m_2$.

Доказательство. Пусть $(b_1 b_2)^s = e$. Тогда $b_1^s = b_2^{-s} \implies b_1^{sm_2} = b_2^{-sm_2} = e$, откуда sm_2 делится на m_1. Значит, s делится на m_1. Аналогично s делится на m_2. С другой стороны, $(b_1 b_2)^{m_1 m_2} = 1$. ■

Лемма 19. Пусть $A \subset \mathbb{F}^*$ и $\max_{a \in A} \operatorname{ord} a = m$, кроме того, $\forall b \in A : \operatorname{ord} b \mid m$. Тогда $A \simeq C_m$.

Доказательство. Пусть все элементы A являются корнями $x^m - 1 = 0$. Отсюда следует, что $m \geqslant |A|$. Но мы знаем, что $m \leqslant |A|$, значит, $m = |A|$. Тогда $A = \{1, a, \ldots, a^{m-1}, a^m = 1\}$ (где a — элемент с максимальным порядком), т.е. циклическая. ■

Доказательство теоремы Т. 17. Докажем, что выполняется условие **Т. 19**. Для этого достаточно доказать, что $\forall x, y \in A \exists z \in A : \operatorname{ord} z = [\operatorname{ord} x, \operatorname{ord} y]$. Пусть

$$x = \prod_{i=1}^{s} p_i^{u_i}, y = \prod_{i=1}^{s} p_i^{v_i}; p_i \neq p_j; u_i, v_i \in \mathbb{Z}_{\geqslant 0}; u_i + v_i > 0.$$

Обозначим

$$l_1 = \prod_{i: u_i > v_i} p_i^{u_i}; l_2 = \prod_{i: u_i \leqslant v_i} p_i^{v_i}; m_1 = l_1 k_1; m_2 = l_2 k_2.$$

Тогда $(l_1, l_2) = 1, [m_1, m_2] = l_1 l_2$. Рассмотрим $a_3 = a_1^{k_1} \cdot a_2^{k_2}$. Тогда по **Т. 18** $\operatorname{ord} a_3 = [m_1, m_2]$.■