Алгебра, 1 курс

Фейгин Евгений Борисович

2 сентября 2020 г. — 20 сентября 2020 г.

Формула оценки: $\frac{D+C+K+2E}{5}$, *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 $Arg(a+bi)$ чисел φ таких, что $a+bi=N(a+bi)(\cos\varphi+i\sin\varphi)$.

Тригонометрическая запись числа. Будем записывать

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

Тогда получится, что

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

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 $f(a_1+_A a_2)=f(a_1)+_B f(a_2)$. 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 $char\mathbb{K}$ — 0 или простое число.

Доказательство. Пусть $char\mathbb{K}=n=n_1n_2$. 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 $N : K \setminus 0 \to Z_{\geq 0}$ со следующими свойствами:

- $N(ab) \geq N(a)$, 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 $\deg fg \geq \deg f \deg g$ и равенство, только если какой-то из многочленов 0 степени, т.е. обратим. Докажем деление с остатком. Пусть $f = \sum f_i x^i, g = \sum g_i x^i, n = \deg f \geq \deg g = m$. 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 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. ■