

**Опр. 1. Кольцом** называется непустое множество  $K$  с операциями сложения и умножения, обладающими следующими свойствами:

- относительно сложения  $K$  есть абелева группа (называемая **аддитивной группой** кольца  $K$ );
- $a(b + c) = ab + ac$  и  $(a + b)c = ac + bc$  для любых  $a, b, c \in K$  (*дистрибутивность умножения относительно сложения*).

Кольцо  $K$  называется **ассоциативным**, если умножение в нем ассоциативно, т. е.  $(ab)c = a(bc)$  для любых  $a, b, c \in K$ .

Кольцо  $K$  называется **кольцом с единицей**, если в  $K$  существует нейтральный элемент относительно умножения, обозначаемый обычно через 1, т.е.  $1a = a1 = a$  для любого  $a \in K$ .

Кольцо  $K$  называется **коммутативным**, если  $K$  — ассоциативное кольцо с единицей, в котором умножение коммутативно, т. е.  $ab = ba$  для любых  $a, b \in K$ .

**Поле** называется коммутативное кольцо, содержащее не менее двух элементов, в котором всякий ненулевой элемент обратим.

**Опр. 2.** Элемент  $a^{-1}$  кольца с единицей называется **обратным** к элементу  $a$ , если  $aa^{-1} = a^{-1}a = 1$ . Элемент, имеющий обратный, называется **обратимым** или **единицей кольца**. Множество  $K^*$  обратимых элементов кольца  $K$  является группой по умножению. Она называется **мультипликативной группой** или **группой обратимых элементов** кольца  $K$ .

**Опр. 3.** Элемент  $a \neq 0 \in K$  называется **делителем нуля**, если найдется такой элемент  $b \neq 0$ , что  $ab = 0$ .

**Опр. 4. Гомоморфизмом** коммутативных колец называется отображение  $\varphi : K \rightarrow L$  множеств, при котором сохраняются операции, то есть  $\forall a, b \in K$  выполнены равенства  $\varphi(a + b) = \varphi(a) + \varphi(b)$ ,  $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ . Аналогично определяется **изоморфизм** колец (это гомоморфизм + биекция).

**Замечание от Ильинского:** Давайте для определённости считать, что  $\varphi(1) = 1$ . Но за это снижать не должны.

Т. к. кольца — абелевы группы по сложению, при гомоморфизме выполняется  $\varphi(0) = 0$ ,  $\varphi(-a) = -\varphi(a)$ .

**Опр. 5.** Коммутативное кольцо без делителей нуля называется **областью целостности** или **кольцом целостности**.

**Опр. 6.** Пусть  $K$  — область целостности. Будем говорить, что элемент  $a \in K$  **делит** элемент  $b \in K$  (обозначим  $a|b$ , или  $b : a$ ), если найдётся такое  $r \in K$ , что  $ar = b$ .

Группа обратимых элементов  $K^*$  действует на всё кольцо  $K$  умножениями слева. Элементы, находящиеся в одной орбите этого действия, будем называть **ассоциированными**, а сами орбиты — **классами ассоциированности**.

То есть элементы  $x$  и  $y$  кольца  $K$  являются **ассоциированными**, если найдётся такое  $r \in K^*$ , что  $x = ry$ . Обозначение:  $x \sim y$ .

**Опр. 7.** Пусть  $K$  — область целостности. Необратимый ненулевой элемент  $x \in K$  называется **неразложимым**, если  $x = ab \Rightarrow \begin{cases} a \in K^* \\ b \in K^* \end{cases}$ .

**Опр. 8.** Пусть  $K$  — область целостности. Назовём ненулевой необратимый элемент  $x \in K$  **простым**, если  $x | ab \Rightarrow \begin{cases} x | a \\ x | b \end{cases}$ .

**Опр. 9.** Область целостности  $K$  называется **евклидовым кольцом**, если существует такое отображение (**норма**)  $N : K \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ , что для любых  $a, b \in K \setminus \{0\}$  выполнены два условия:

1.  $N(ab) \geq N(a)$ ;
2. найдутся такие элементы  $q, r \in K$ , что  $a = qb + r$  и либо  $r = 0$ , либо  $N(r) < N(b)$ .

**Опр. 10.** Область целостности  $K$  называется **факториальным кольцом**, если выполнены следующие два условия:

1. (**существование разложения**) любой элемент  $x \in K$ ,  $x \neq 0$  представляется в виде произведения неразложимых элементов с точностью до ассоциированности, то есть  $x = up_1 \dots p_k$ , где  $u \in K^*$ ,  $p_i$  — неразложимые элементы;
2. (**единственность разложения**) данное разложение единственно в следующем смысле. Пусть  $x = up_1 \dots p_k = wq_1 \dots q_l$  — два разложения, где  $u, w$  обратимы, а  $p_i, q_j$  — неразложимые элементы. Тогда  $k = l$  и элементы  $q_j$  можно перенумеровать так, чтобы для всех  $i$  элементы  $p_i$  и  $q_i$  были ассоциированы.

**Опр. 11.** Корнем из единицы степени  $n$  называется  $z \in \mathbb{C} : z^n = 1$ .

Корень из 1 степени 3, находящийся в верхней полуплоскости, обозначается  $\omega$ .

$\forall u \in \mathbb{C}$  определим  $\mathbb{Z}[u] = \bigcup_{n=0}^{\infty} \{a_0 + a_1 u + \dots + a_n u^n \mid a_0, \dots, a_n \in \mathbb{Z}\}$  — множество, порождённое элементом  $u$  над  $\mathbb{Z}$ .

Тогда  $\mathbb{Z}[\omega]$  — числа Эйзенштейна.

**Опр. 12. Наибольший общий делитель (НОД)**  $(a, b)$  двух элементов  $a, b \in K$  — области целостности, есть их общий делитель, который делится на все их другие общие делители.

**Опр. 13. Подкольцо**  $S \subset K$  есть подгруппа по сложению, замкнутая относительно умножения (т. е.  $\forall a, b \in S \quad ab \in S$ ).

**Опр. 14. Идеал**  $I$  коммутативного кольца  $K$  — это такое множество элементов, что

1.  $(I, +) \subset (K, +)$  — подгруппа по сложению.
2. Для любых элементов  $a \in K$  и  $x \in I$  верно, что  $ax \in I$ .

Таким образом, подкольцо  $I \subset K$  называется идеалом, если  $\forall a \in K, x \in I \Rightarrow ax \in I$ .

**Опр. 15.**  $0 \subset K, K \subset K$  — идеалы. Они называются **тривиальными**.

**Опр. 16.**  $(a_1, \dots, a_n) = \{a_1 x_1 + \dots + a_n x_n \mid x_1, \dots, x_n \in K\}$  — **идеал, порождённый элементами**  $a_1, \dots, a_n$ .

**Опр. 17. Конечное порождённый идеал** — идеал, порождённый конечным количеством элементов.

**Опр. 18.**  $(a) = \{ax \mid x \in K\}$  — **главный идеал** или **идеал, порождённый одним элементом**.

**Опр. 19.** Область целостности, в которой все идеалы главные, называется **кольцом главных идеалов** (сокращённо КГИ).

**Опр. 20.** Назовём нетривиальный идеал  $I$  **простым**, если  $ab \in I \Rightarrow \begin{cases} a \in I \\ b \in I \end{cases}$ .

**Опр. 21.** Назовём нетривиальный идеал  $I$  **максимальным**, если он максимальный по включению, то есть не существует идеала  $J$  такого, что  $I \subsetneq J \subsetneq K$ .

**Опр. 22.** Элементы  $x, y \in K$  называются **взаимно простыми**, если у них нет нетривиальных общих делителей.

Будем называть многочлен  $f \in K[x]$  **примитивным**, если его коэффициенты взаимно просты.

**Опр. 23. Расширением полей** называется вложение полей  $K \supset F$ .

**Вложение** — инъективное отображение  $F \rightarrow K$ .

**Опр. 24.** Определение  $F(\alpha_1, \dots, \alpha_n)$  см. в №30.

Элемент  $\alpha \in K$  **алгебраичен** над  $F$ , если выполнено одно из двух эквивалентных условий:

1. расширение  $F(\alpha) \supset F$  конечно;
2.  $\alpha$  — корень многочлена  $f(x) \in F[x]$ .

**Опр. 25. Трансцендентный элемент** — элемент, не являющийся алгебраическим.

**Опр. 26.** Расширение  $K \supset F$  называется **алгебраическим**, если оно состоит из элементов, алгебраических над  $F$ .

**Опр. 27. Пример алгебраического расширения поля.**

- Расширение  $\mathbb{C} \supset \mathbb{R}$  является алгебраическим.
- Расширение  $F \supset F$  является алгебраическим.
- Любое конечное расширение  $K \supset F$  является алгебраическим.

**Примеры алгебраических элементов (не нужно в вопросе, на всякий случай).**

- В расширении  $\mathbb{Q} \subset \mathbb{C}$  элементы  $\sqrt{2}, \sqrt{3}, \sqrt[3]{7}, i, i + \sqrt{3}$  поля  $\mathbb{C}$  — алгебраические над  $\mathbb{Q}$ .
- В  $\mathbb{R} \subset \mathbb{C}$  все элементы алгебраичны над  $\mathbb{R}$ .
- В любом расширении  $K \supset F$  элементы  $F$  являются алгебраическими над  $F$ .

**Опр. 28. Пример не алгебраического расширения поля.**

Если в расширении есть трансцендентный элемент, оно не алгебраическое.

- В расширении  $\mathbb{Q} \subset \mathbb{C}$  элементы  $\pi, e$  трансцендентны над  $\mathbb{Q}$ .
- В расширении  $F \subset F(x)$  элемент  $x$  — трансцендентный над  $F$ . Тут  $x$  — тот  $x$  из определения кольца многочленов  $F[x]$ , а не элемент  $F$ , как могло бы показаться (контрпример: рассмотрим расширение  $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ , тогда многочлен  $x^2 - 2$  имеет своим корнем  $\sqrt{2} \Rightarrow \sqrt{2}$  алгебраический).  
Вспомним, как определяли многочлен как финитную последовательность элементов кольца, и  $x$  у нас был  $(0, 1, 0, \dots, 0)$ , а элемент  $a \in F$  мы отождествляли с последовательностью  $(a, 0, \dots, 0)$ , т. е. при этом  $F \subset F[x]$ .

Элемент  $x$  — не алгебраический, потому что расширение  $F(x) \supset F$  бесконечно.

**Опр. 29.** Для данного элемента  $\alpha \in K$  назовём **минимальным многочленом** многочлен  $m_\alpha = m_{\alpha, F}$  со старшим коэффициентом 1, удовлетворяющий одному из СЭУ (следующих эквивалентных условий):

1. Для идеала  $I_{\alpha, F} := (m_{\alpha, F})$  выполнено  $I_{\alpha, F} = \{f(x) \in F[x] \mid f(\alpha) = 0\}$ ;
2.  $m_\alpha$  — многочлен из  $I_\alpha$  минимальной степени;
3.  $m_\alpha$  — неприводимый многочлен из  $I_\alpha$ .

**Опр. 30.** Через  $F(\alpha_1, \dots, \alpha_n)$  обозначим минимальное поле в  $K$ , содержащее  $F$  и  $\alpha_1, \dots, \alpha_n$ .

**Опр. 31.** Назовём **полем разложения** многочлена  $f(x)$  над полем  $F$  такое расширение  $L \supset F$ , что  $L$  содержит все корни многочлена  $f(x)$  и не существует нетривиального подполя  $K \subset L$ , удовлетворяющего тому же условию.

**Опр. 32.** Поле  $K$  называется **алгебраически замкнутым**, если выполнено одно из следующих эквивалентных условий:

- (1) Любое алгебраическое расширение над  $K$  тривиально.
- (2) Любой многочлен  $f(x) \in K[x]$  с  $\deg f(x) \geq 1$  имеет корень в  $K$ .
- (3) Любой многочлен  $f(x) \in K[x]$  с  $\deg f(x) \geq 1$  раскладывается на линейные множители в  $K$ .
- (4) Все неприводимые над  $K$  многочлены имеют степень 1.
- (5) Для любого многочлена  $f(x) \in K[x]$  с  $\deg f(x) \geq 1$  его поле разложения совпадает с  $K$ .

**Опр. 33.** **Алгебраическим замыканием** поля  $F$  называется алгебраическое расширение  $K = \bar{F}$  поля  $F$ , которое является алгебраически замкнутым полем.

**Опр. 34.** Даны точки 0 и 1 комплексной плоскости. Точку  $x \in \mathbb{C}$  можно *построить*, если найдётся такая последовательность точек  $x_0 = 0, x_1 = 1, \dots, x_n = x$ , где точка  $x_k$  получается из точек  $\{x_0, x_1, \dots, x_{k-1}\}$  при помощи применения трёх следующих действий:

1. Провести прямую через ранее построенные точки.
2. Провести окружность с центром в уже построенной точке, проходящую через другую построенную точку.
3. Построить точку пересечения двух *различных* прямых, прямой и окружности, двух *различных* окружностей, полученных в результате действий 1 и 2.

**Опр. 35.** Обозначим через  $\xi_n$  **примитивный корень**  $n$ -ой степени из 1, то есть корень многочлена  $x^n - 1$ , который не является корнем многочлена  $x^k - 1$  при  $k < n$ .

**Опр. 36.** Алгебраические над  $F$  элементы  $\alpha$  и  $\beta$  называются **сопряженными**, если  $m_{\alpha, F} = m_{\beta, F}$  (или, эквивалентно,  $m_{\alpha, F}(\beta) = 0$ ).

**Опр. 37.** **Признак неприводимости Эйзенштейна**

Пусть  $f(x)$  — многочлен с целыми коэффициентами и существует такое простое число  $p$ , что:

1. старший коэффициент  $f(x)$  не делится на  $p$ ;
2. все остальные коэффициенты  $f(x)$  делятся на  $p$ ;
3. свободный член  $f(x)$  не делится на  $p^2$ .

Тогда многочлен  $f(x)$  неприводим над полем рациональных чисел.

**Более общая формулировка из Lecture\_all.pdf:**

Пусть  $F$  — факториальное кольцо,  $I \subset F$  — простой идеал,  $f(x) = a_n x^n + \dots + a_1 x + a_0 \in F[x]$  — многочлен степени  $n > 1$ . Если  $a_0, a_1, \dots, a_{n-1} \in I, a_0 \notin I^2, a_n \notin I$ , то у  $f(x)$  нет делителей степени  $d$  при  $1 \leq d \leq n-1$ .

**Опр. 38.**  $\varphi : F \rightarrow F$ , где  $\varphi$  — изоморфизм, — **автоморфизм** поля  $F$  (изоморфизм поля на себя).

**Степенью**  $[K : F]$  расширения  $K \supset F$  называется размерность  $K$  над  $F$  как линейного пространства.

Пусть  $F \subset K$  — расширение полей. Множество автоморфизмов  $K$ , оставляющих  $F$  на месте, является группой и называется **группой автоморфизмов** и обозначается  $\text{Aut}_F(K) = \text{Aut}([K : F])$ . Если  $F$  — основное поле ( $\mathbb{Q}$  или  $\mathbb{Z}_p$ ), то символ  $F$  опускают.

**Опр. 39.** Пусть  $H \subset \text{Aut}_F(K)$  — подгруппа. Тогда  $K^H = \{x \in K \mid \forall h \in H \ h(x) = x\}$  является полем, причём  $K \supset K^H \supset F$ .

**Опр. 40.** Пусть  $K \supset F$  — конечное расширение. Будем называть это расширение **нормальным**, или **расширением Галуа** если выполнено одно из следующих эквивалентных условий:

- (1) Вместе с каждым элементом поле  $K$  содержит и все сопряженные;
- (2)  $K$  — поле разложение многочлена  $f(x) \in F[x]$ ;
- (3)  $|\text{Aut}_F K| = [K : F]$ ;
- (4)  $K^{\text{Aut}_F K} = F$ .

**Опр. 41.** Группа автоморфизмов расширения Галуа  $K$ , сохраняющих  $F$ ,  $\text{Aut}_F K$ , называется **группой Галуа**  $\text{Gal}_F K$ .