# АЛГЕБРА 1999/2000
# I СЕМЕСТР

## Листок 2

**Ф. Зак, А. Иншаков, А. Обломков, С. Дориченко**

**Определение 2.1.** Идеал $\mathfrak{a}$ кольца $A$ называется *простым*, если фактор-кольцо $A/\mathfrak{a}$ — область целостности. Идеал $\mathfrak{m} \subset A$ называется *максимальным*, если не существует идеала $\mathfrak{a} \subset A$ такого, что $\mathfrak{a} \supset \mathfrak{m}$ и $\mathfrak{a} \neq A$.

$\checkmark$**Задача 2.1.** Идеал $\mathfrak{m} \subset A$ максимален тогда и только тогда, когда фактор-кольцо $A/\mathfrak{m}$ является полем. В частности, максимальные идеалы просты.

$\checkmark$**Задача 2.2.** Приведите пример простого идеала, не являющегося максимальным.

$\checkmark$**Упражнение 2.3.** Пусть $\varphi\colon A \to B$ — гомоморфизм колец. Докажите, что если $\mathfrak{b} \subset B$ — простой идеал, то его прообраз $\varphi^{-1}(\mathfrak{b}) \subset A$ также прост. Верно ли аналогичное утверждение для максимальных идеалов?

**Определение 2.2.** Говорят, что $p \in A$ — *неприводимый* (или *простой*) элемент области целостности $A$, если из того, что $p = a \cdot b$, $a, b \in A$ следует, что хотя бы один из элементов $a, b$ обратим (элемент $c \in A$ называется *обратимым*, если $c^{-1} \in A$).

**Упражнение 2.4.** Пусть $A$ — область целостности. Докажите, что если $p \in A$ — элемент, для которого соответствующий главный идеал $(p)$ прост, то $p$ неприводим. Верно ли обратное утверждение?

**Определение 2.3.** Пусть $A$ — область целостности, и пусть $a, b \in A$, $a, b \neq 0$. Говорят, что *$a$ делит $b$* и пишут $a \,|\, b$, если существует элемент $c \in A$ такой, что $ac = b$. Говорят, что элемент $d \in A$ является *наибольшим общим делителем* (НОД) элементов $a$ и $b$, если $d \,|\, a$, $d \,|\, b$ и для всякого $e \in A$ такого, что $e \,|\, a$, $e \,|\, b$ имеем $e \,|\, d$.

**Упражнение 2.5.** Докажите, что НОД элементов $a, b$ области целостности $A$ определён однозначно с точностью до обратимых элементов кольца $A$.

$\checkmark$**Упражнение 2.6.** Пусть $a, b \in A$, где $A$ — область целостности, являющаяся кольцом главных идеалов, и пусть $(a, b) = (d)$. Тогда $d$ НОД $a$ и $b$.

В частности, если $d$ — НОД элементов $a, b \in A$, то существуют элементы $a', b' \in A$ такие, что $a' \cdot a + b' \cdot b = d$.

$\checkmark$**Задача 2.7.** Пусть $A$ — область целостности, являющаяся кольцом главных идеалов, и пусть $p \in A$ — неприводимый элемент. Предположим, что $p \,|\, a \cdot b$, $a, b \in A$. Докажите, что либо $p \,|\, a$, либо $p \,|\, b$.

**Определение 2.4.** Пусть $A$ — область целостности. Говорят, что элемент $a \in A$, $a \neq 0$ обладает однозначным разложением на множители, если существуют обратимый элемент $u \in A$ и (не обязательно различные) неприводимые элементы $p_1, \ldots, p_r \in A$ такие, что $a = u \cdot p_1 \cdots p_r$, причём для любых двух таких разложений $a = u \cdot p_1 \cdots p_r = u' \cdot p'_1 \cdots p'_{r'}$ имеем $r' = r$ и, после подходящей перестановки индексов, $p_i = u_i \cdot p'_i$, где $u_i \in A$, $i = 1, \ldots, r$ — обратимые элементы.

Говорят, что кольцо $A$ *факториально*, если произвольный элемент $a \in A$, $a \neq 0$ имеет однозначное разложение на простые множители.

**Задача 2.8.** Рассмотрим кольцо $A = \mathbb{Z}[\sqrt{6}]$. Имеем $6 = 2 \cdot 3 = \sqrt{6} \cdot \sqrt{6}$, но элементы 2, 3 и $\sqrt{6}$ не являются неприводимыми в $A$. Разложите эти элементы на простые множители.

*Замечание 2.1.* В кольце $A = \mathbb{Z}[\sqrt{6}]$ имеем $2 = (\sqrt{6}+2) \cdot (\sqrt{6}-2) = (5 - 2\sqrt{6}) \cdot (\sqrt{6}+2)^2$. Однако эти разложения эквивалентны, поскольку $5 - 2\sqrt{6}$ — обратимый элемент кольца $A$ и $\sqrt{6} - 2 = (5 - 2\sqrt{6}) \cdot (\sqrt{6}+2)$.

✓**Задача 2.9.** Пусть $A$ — область целостности, являющаяся кольцом главных идеалов. Докажите, что $A$ факториально.

✓**Упражнение 2.10.** Пусть $A$ — область целостности, являющаяся кольцом главных идеалов. Докажите, что всякий простой идеал в $A$ максимален.

Решив задачу 1.14, вы сможете использовать результат задачи 2.9 для доказательства факториальности колец $\mathbb{Z}$ и $K[T]$ (где $K$ — поле). Нетрудно заметить, что то, что $\mathbb{Z}$ и $K[T]$ — кольца главных идеалов доказывается аналогично, а именно с помощью деления с остатком. Поэтому представляется разумным дать следующее общее определение.

**Определение 2.5.** Область целостности $A$ называется *евклидовым кольцом*, если на множестве ненулевых элементов $A$ определена функция $e$ с неотрицательными целыми значениями такая, что

(E1) $e(ab) \geq e(a)$ при всех $a, b \in A$, $a, b \neq 0$;

(E2) Для всех элементов $a, b \in A$, $b \neq 0$ возможно деление с остатком $a$ на $b$, т.е. существуют элементы $q, r \in A$ (называемые соответственно частным и остатком) такие, что

$$a = q \cdot b + r, \text{ и } e(r) < e(b) \text{ при } r \neq 0.$$

Функция $e$ называется *евклидовой нормой*.

✓**Упражнение 2.11.** Проверьте, что $\mathbb{Z}$ и $K[T]$ — евклидовы кольца относительно функций $e(a) = |a|$ и $e(a) = \deg a$ соответственно.

**Определение 2.6.** Пусть $A$ — кольцо, являющееся подкольцом кольца $B$, и пусть $P(T) \in A[T]$ — многочлен. Элемент $b \in B$ называется *корнем* $P$ в $B$, если $P(b) = 0$.

✓**Упражнение 2.12.** Докажите следующую теорему Безу:

*Пусть $K$ — поле, и пусть $P[T] \in K[T]$ — многочлен степени $n$. Тогда $P$ имеет не более $n$ корней в поле $K$, и если $\alpha \in K$ — корень $P$ в $K$, то $P(T)$ делится на $T - \alpha$.*

**Упражнение 2.13.** Пусть $K$ — поле, и пусть $P[T] \in K[T]$, $P(T) = \sum_{i=0}^{n} a_i T^i$, $a_i \in K$, $a_0 = 1$ — многочлен, имеющий $n$ (не обязательно различных) корней $\alpha_1, \ldots, \alpha_n$ в некотором расширении $K'$ поля $K$. Выведите *формулы Виета*, выражающие коэффициенты $a_i$, $i = 1, \ldots, n$ через корни $\alpha_1, \ldots, \alpha_n$.

Многочлены над конечными полями имеют ряд непривычных свойств. В частности, ненулевой многочлен может задавать нулевую функцию на поле.

$\surd$**Задача 2.14.** Пусть $p \in \mathbb{Z}$ — простое число. Докажите, что многочлен $P(T) = T^p - T$ определяет нулевую функцию на поле $\mathbb{Z}/p\mathbb{Z}$ (см. задачу 1.2), т.е. $P(\alpha) = 0$ для всех $\alpha \in \mathbb{Z}/p\mathbb{Z}$ (это утверждение называется *малой теоремой Ферма*).

$\surd$**Задача 2.15.** Докажите теорему Вильсона.

*Следующие условия эквивалентны*:

(1) $p \in \mathbb{Z}$ — *простое число*;
(2) $(p-1)! + 1 \equiv 0 \bmod p$ (здесь и далее $m! = 1 \cdot 2 \cdots m$ (такое произведение называется факториалом), $a \equiv b \bmod m$ если и только если $m \mid a - b$ (в этом случае говорят, что $a$ и $b$ сравнимы по модулю $m$)).

$\surd$**Упражнение 2.16.** Пусть $A$ — евклидово кольцо, и пусть $u \in A$ его элемент. Следующие условия эквивалентны:

а) $u$ обратим;
б) $e(u) = e(1)$;
в) $e(ua) = e(a)$ для всех $a \in A$, $a \neq 0$.

$\surd$**Задача 2.17.** Докажите, что всякое евклидово кольцо является кольцом главных идеалов (ввиду задачи 2.9, отсюда следует, что всякое евклидово кольцо факториально).

**Определение 2.7.** Пусть $A$ — подкольцо $B$, пусть $b \in B$, и пусть $\varphi_b \colon A[T] \to B$ — гомоморфизм, задаваемый соответствием $P(T) \mapsto P(b)$. Элемент $b$ называется *трансцендентным* над $A$, если $\operatorname{Ker} \varphi_b = 0$, т.е. $b$ не является корнем никакого многочлена с коэффициентами в $A$. В противном случае $b$ называется *алгебраическим* над $A$.

**Задача 2.18.** Докажите, что над полем рациональных чисел $\mathbb{Q}$ существуют как алгебраические, так и трансцендентные вещественные числа.

Пусть $K$ — поле, и пусть $P(T)$ — неприводимый многочлен. Из упражнения 2.10 следует, что $K[T]/(P)$ — поле.

$\surd$**Задача 2.19.** Если $K \subset K'$ — расширение полей и $\alpha \in K'$ — корень многочлена $P$, то поле $K[T]/(P)$ изоморфно полю $K(\alpha)$.

**Задача 2.20.** Докажите, что поле $\mathbb{R}[T]/(T^2+1)$ изоморфно полю $\mathbb{C}$ комплексных чисел, причём изоморфизм даётся сопоставлением $P \mapsto P(i)$, где $i \in \mathbb{C}$ — мнимая единица.

Те, кто не знает комплексных чисел, могут принять задачу 2.20 за их определение.

✓**Задача 2.21.** Пусть $\mathbb{Z}[i] \subset \mathbb{Q}(i)$ — *кольцо целых гауссовых чисел*, т.е. чисел вида $m + ni \in \mathbb{C}$, $m, n \in \mathbb{Z}$. Докажите, что $\mathbb{Z}[i]$ — евклидово кольцо (в частности, оно факториально и все идеалы в нём главные). Найдите все обратимые элементы в кольце $\mathbb{Z}[i]$.

Пусть $p \in \mathbb{N}$ — простое число. Согласно задаче 2.21, в кольце $\mathbb{Z}[i]$ число $p$ разлагается в произведение простых множителей: $p = p_1 \cdots p_r$, $r \geq 1$ (например, $2 = (1+i)(1-i)$).

**Задача 2.22.** В указанных выше обозначениях следующие условия эквивалентны:

(1) $r > 1$ (т.е. $p$ перестаёт быть простым в $\mathbb{Z}[i]$);
(2) $r = 2$;
(3) Число $p$ представимо в виде суммы двух квадратов, т.е. $p = m^2 + n^2$, $m, n \in \mathbb{Z}$;
(4) Либо $p = 2$, либо $p \equiv 1 \bmod 4$, т.е. $p = 4k + 1$ для некоторого $k \in \mathbb{N}$.

**Задача 2.23.** Выясните, какие числа $n \in \mathbb{N}$ представимы в виде $n = a^2 + b^2$, $a, b \in \mathbb{N}$.

**Задача 2.24.** Пусть $p \in \mathbb{Z}$ — нечётное простое число. Докажите, что следующие условия эквивалентны:

а) Многочлен $T^2 + 1$ неприводим над полем $\mathbb{Z}/p\mathbb{Z}$;
б) Идеал $(p)$ прост в кольце $\mathbb{Z}[i]$;
в) $p \equiv 3 \bmod 4$.

Проверьте, что если эти условия выполнены, то $\mathbb{Z}/p\mathbb{Z}[T]/(T^2+1) \simeq \mathbb{Z}[i]/(p)$ — поле из $p^2$ элементов.

Перейдём к исследованию колец многочленов $A[T]$, где $A$ — любое факториальное кольцо. Такие кольца, вообще говоря, не являются кольцами главных идеалов и, тем более, евклидовыми (см. задачу 1.14).

**Определение 2.8.** Пусть $A$ — факториальное кольцо, и пусть $P(T) = a_0 + a_1T + \cdots + a_nT^n \in A[T]$ — многочлен. *Содержанием* $\operatorname{cont} P$ многочлена $P$ называется наибольший общий делитель его коэффициентов $a_0, \ldots, a_n$. Заметим, что содержание определено с точностью до обратимых элементов кольца $A$. Многочлен $P$ называется *примитивным*, если $\operatorname{cont} P = 1$.

✓**Задача 2.25.** Докажите следующую лемму Гаусса:

*Пусть $P, Q \in A[T]$, где $A$ — факториальное кольцо. Тогда $\operatorname{cont} PQ = \operatorname{cont} P \cdot \operatorname{cont} Q$. В частности, произведение примитивных многочленов примитивно.*

✓**Задача 2.26.** Пусть $A$ — факториальное кольцо, $K = K(A)$ — поле частных $A$, и пусть $P \in A[T]$ — неприводимый многочлен. Тогда $P$ остаётся неприводимым и в $K[T]$ (разумеется, верно и обратное утверждение).

✓**Задача 2.27.** Докажите следующую теорему Эйзенштейна.

*Пусть $A$ — факториальное кольцо, $K = K(A)$ — поле частных $A$, пусть $P = a_0 + a_1T + \cdots + a_nT^n \in A[T]$ — многочлен, и пусть $p \in A$ — неприводимый элемент. Предположим, что $p \mid a_i$ для всех $i < n$, но $p \nmid a_n$ и $p^2 \nmid a_0$. Тогда $P$ неприводим в $K[T]$.*

✓**Задача 2.28.** При каких натуральных числах $n, m$ многочлен $T^n - m$ неприводим над $\mathbb{Q}$?

**Задача 2.29.** Пусть $p \in \mathbb{Z}$ — простое число. Докажите, что многочлен $1 + T + \cdots + T^{p-1}$ неприводим над $\mathbb{Q}$.

✓**Задача 2.30.** Пусть $A$ — факториальное кольцо. Докажите, что кольцо многочленов $A[T]$ также факториально. Сравните неприводимые элементы в $A[T]$ и $K(A)[T]$.

**Следствие.** *Если $A$ — факториальное кольцо, то для всех $m$ кольцо многочленов $A[T_1, \ldots, T_m]$ также факториально.*

Тем не менее, далеко не все кольца факториальны.

✓**Задача 2.31.** Докажите, что кольцо $\mathbb{Z}[\sqrt{2}]$ факториально, а кольцо $\mathbb{Z}[\sqrt{-5}]$ таковым не является (хотя бы потому, что $21 = 3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$ — два существенно различных разложения на простые множители — докажите!).