# ЛЕКЦИЯ 18

# ЭЛЕМЕНТАРНЫЕ СВОЙСТВА ДЕЛИМОСТИ

# ФАКТОРИАЛЬНОСТЬ ЕВКЛИДОВЫХ КОЛЕЦ

# ЭЛЕМЕНТАРНЫЕ СВОЙСТВА ДЕЛИМОСТИ

В самых первых лекциях мы затрагивали вопросы делимости в кольце $\mathbb{Z}$ целых чисел, но так называемая основная теорема арифметики у нас осталась пока недоказанной. Теперь настала пора не только заполнить этот пробел, но и распространить соответствующие утверждения на более широкий класс колец.

В первую очередь нас интересует кольцо $\mathbb{F}[X]$ многочленов над полем.

Начнем с произвольного целостного кольца $R$. Обратимые элементы в $R$ были названы нами делителями единицы.

Совершенно очевидно, что многочлен $f \in R[X]$ обратим тогда и только тогда, когда $\deg f = 0$ и $f = f_0$ — обратимый элемент кольца $R$.

Говорят, что элемент $b \in R$ *делится* на $a \in R$ (или $b$ *кратен* $a$), если существует такой элемент $c \in R$, что $b = ac$ (это обозначается $a|b$).

Если $a|b$ и $b|a$, то $a$ и $b$ называются *ассоциированными* элементами. Тогда $b = ua$, где $u$ — обратимый элемент.

В силу замечания, которое мы сделали выше, ассоциированность многочленов $f$ и $g$ означает, что они отличаются лишь обратимым множителем из $R$.

Элемент $p \in R$ называется *простым* (или *неразложимым*), если $p$ необратим и его нельзя представить в виде $p = ab$, где $a, b$ — необратимые элементы.

В поле $\mathbb{F}$ каждый ненулевой элемент обратим, поэтому там нет простых элементов.

Простой элемент кольца $R[X]$ называется обычно *неприводимым многочленом.*

Отметим следующие основные свойства отношения делимости в целостном кольце $R$:

(1) *Если* $a|b$, $b|c$, *то* $a|c$.

Действительно, мы имеем $b = ab'$, $c = bc'$, где $b', c' \in R$. Поэтому $c = (ab')c' = a(b'c')$.

(2) *Если* $c|a$, $c|b$, *то* $c|(a \pm b)$.

В самом деле, по условию $a = ca'$, $b = cb'$ для некоторых $a', b' \in R$, и ввиду дистрибутивности $a \pm b = c(a' \pm b')$.

(3) *Если* $a|b$, *то* $a|bc$.

Ясно, что $b = ab' \Longrightarrow bc = (ab')c = a(b'c)$.

Комбинируя (2) и (3), получаем

(4) *Если каждый из элементов* $b_1, b_2, \ldots, b_m \in R$ *делится на* $a \in R$, *то на* $a$ *будет делиться также и элемент*

$$b_1c_1 + b_2c_2 + \cdots + b_mc_m,$$

*где* $c_1, c_2, \ldots, c_m$ — *произвольные элементы кольца.*

Определение 1. Говорят, что целостное кольцо $R$ — *кольцо с однозначным разложением на простые множители* (или *факториальное кольцо*), если любой элемент $a \neq 0$ из $R$ можно представить в виде

$$a = up_1p_2 \dots p_r,$$

где $u$ — обратимый элемент, а $p_1, \dots, p_r$ — простые элементы (не обязательно попарно различные), причем из существования другого такого разложения

$$a = vq_1q_2 \dots q_s$$

следует, что $r = s$ и при надлежащей нумерации элементов $p_i$ и $q_j$ будет

$$q_1 = u_1p_1, \dots, q_r = u_rp_r,$$

где $u_1, \dots, u_r$ — обратимые элементы.

Мы допускаем, что $r = 0$, то есть обратимые элементы тоже раскладываются на простые множители.

Ясно, что если $p$ — простой, $u$ — обратимый, то $up$ — тоже простой элемент.

В кольце $\mathbb{Z}$ с обратимыми элементами 1 и $-1$ отношение порядка дает возможность выделить положительное простое число $p$ из двух возможных $\pm p$.

В кольце $\mathbb{F}[X]$ принято рассматривать нормализованные многочлены (с коэффициентом при старшей степени, равным единице).

Справедлива следующая общая

**Теорема 1.** *Пусть $R$ — произвольное целостное кольцо с разложением на простые множители.*

*Однозначность разложения в $R$ имеет место тогда и только тогда, когда любой простой элемент $p \in R$, делящий произведение $ab \in R$, делит по крайней мере один из множителей $a, b$.*

*Доказательство.* Пусть $R$ факториально, и пусть $ab = pc$. Если

$$a = \prod a_i, \quad b = \prod b_j, \quad c = \prod c_k$$

— разложения $a, b, c$ на простые множители, то из равенства

$$\prod a_i \times \prod b_j = p \prod c_k$$

следует, что элемент $p$ ассоциирован с одним из $a_i$ или $b_j$, то есть $p$ делит $a$ или $b$.

Обратно, установим однозначность разложения в $R$, где

$$p|ab \Longrightarrow p|a \text{ или } p|b.$$

Рассуждая по индукции, допустим, что разложение всех элементов из $R$ с числом $\leqslant n$ простых множителей единственно (конечно, с точностью до порядка множителей и их ассоциированности).

Докажем теперь это для любого элемента $a \neq 0$, который может быть разложен на $n+1$ простых множителей. Именно, пусть

$$a = \prod_{i=1}^{n+1} p_i = \prod_{j=1}^{m+1} r_j$$

— два разложения элемента $a$ с $m \geqslant n$.

Условие теоремы, примененное к $p = p_{n+1}$, дает нам, что $p_{n+1}$ должен делить один из элементов $r_1, \ldots, r_{m+1}$.

Без ограничения общности (ибо это вопрос нумерации) считаем, что

$$p_{n+1} | r_{m+1}.$$

Но $r_{m+1}$ — простой элемент, поэтому

$$r_{m+1} = u p_{n+1},$$

где $u$ — обратимый элемент.

Опираясь на закон сокращения в $R$, получаем равенство

$$\prod_{i=1}^{n} p_i = u \prod_{j=1}^{m} r_j.$$

В левой части его стоит произведение $n$ простых множителей. По предположению индукции $m = n$ и оба разложения отличаются лишь порядком простых элементов, снабженных, возможно, какими-то обратимыми множителями. $\square$

В произвольном целостном кольце $R$ элемент $a \neq 0$ вообще не обязан допускать разложения на простые множители. Что более интересно, имеются целостные кольца, в которых разложение на простые множители хотя и возможно, но не является однозначным.

Пример 1. Рассмотрим поле $\mathbb{Q}[\sqrt{-5}]$, а в нем целостное кольцо

$$\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}.$$

Норма

$$N(a + b\sqrt{-5}) = a^2 + 5b^2$$

каждого отличного от нуля элемента $\alpha \in R$ — целое положительное число. Если $\alpha$ обратим в $R$, то

$$(N(\alpha))^{-1} = N(\alpha^{-1}) \in \mathbb{Z},$$

откуда $N(\alpha) = 1$. Это возможно лишь при $b = 0$, $a = \pm 1$.

Таким образом, в $R$ обратимыми элементами, как и в $\mathbb{Z}$, являются только $\pm 1$.

Если

$$\alpha = \varepsilon\alpha_1\alpha_2 \dots \alpha_r \neq 0, \quad \varepsilon = \pm 1,$$

то

$$N(\alpha) = N(\alpha_1) \dots N(\alpha_r).$$

Так как $1 < N(\alpha_i) \in \mathbb{N}$, то при заданном $\alpha$ число множителей $r$ не может неограниченно расти.

Значит, разложение на простые множители в $R$ возможно.

Вместе с тем число 9 (да и не только оно) допускает два существенно различных разложения на простые множители:

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Неассоциированность элементов 3 и $2 \pm \sqrt{-5}$ очевидна.

Далее,

$$N(3) = N(2 \pm \sqrt{-5}) = 9.$$

Поэтому из разложения $\alpha = \alpha_1\alpha_2$ для $\alpha = 3$ или $2 \pm \sqrt{-5}$ с необратимыми $\alpha_1, \alpha_2$ следовало бы $9 = N(\alpha) = N(\alpha_1)N(\alpha_2)$, откуда $N(\alpha_i) = 3$ при $i = 1, 2$. Но это невозможно, так как уравнение $x^2 + 5y^2 = 3$ в целых числах неразрешимо. Отсюда следует простота элементов 3 и $2 \pm \sqrt{-5}$.

Наибольшим делителем НОД$(a, b)$ двух элементов $a, b \in R$ целостного кольца $R$ называется такой элемент $d$ этого кольца, который удовлетворяет двум свойствам:

(1) $d|a, d|b$;

(2) Если $d'|a, d'|b$, то $d'|d$.

Очевидно что наибольший общий делитель двух элементов (если он существует) определен с точностью до ассоциированности.

Аналогично, наибольшим общим кратным НОК$(a, b)$ двух элементов $a, b \in R$ называется такой элемент $c \in R$, что

(1) $a|c, b|c$;

(2) Если $a|c', b|c'$, то $c|c'$.

Аналогично, наименьше общее кратное также определено с точностью до ассоциированности.

Определение 2. Элементы $a, b$ целостного кольца, в котором существует разложение на множители, называются взаимно простыми, если все их общие делители обратимы.

# ФАКТОРИАЛЬНОСТЬ ЕВКЛИДОВЫХ КОЛЕЦ

Алгоритм деления с остатком в $\mathbb{Z}$ и $\mathbb{F}[X]$ делает естественным рассмотрение целостного кольца $R$, в котором каждому элементу $a \neq 0$ поставлено в соответствие неотрицательное целое число $\delta(a)$, то есть определено отображение

$$\delta : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

так, что при этом выполняются условия:

(1) $\delta(ab) \geqslant \delta(a)$ для всех $a, b \neq 0$ из $R$;

(2) каковы бы ни были $a, b \in R$, $b \neq 0$, найдутся $q, r \in R$ такие, что

$$a = bq + r, \quad \delta(r) < \delta(q) \text{ или } r = 0.$$

Целостное кольцо $R$ с этими свойствами называют *евклидовым кольцом*. Полагая $\delta(a) = |a|$ для $a \in \mathbb{Z}$ и $\delta(a) = \deg a$ для $a = a(X) \in F[X]$, мы приходим к выводу, что $\mathbb{Z}$ и $\mathbb{F}[X]$ — евклидовы кольца.

В евклидовых кольцах существует способ нахождения НОД$(a, b)$, называемый *алгоритмом последовательного деления* или *алгоритмом Евклида* и заключающийся в следующем.

Пусть даны ненулевые элементы $a, b$ евклидова кольца $R$.

Применяя достаточно большое (но конечное) число раз правило (2), мы поулчим систему равенств с последним нулевым остатком:

$$\begin{aligned}
a &= q_1 b + r_1, & \delta(r_1) &< \delta(b),\\
b &= q_2 r_1 + r_2, & \delta(r_2) &< \delta(r_1),\\
r_1 &= q_3 r_2 + r_3, & \delta(r_3) &< \delta(r_2),\\
&\ldots\ldots\ldots\ldots & &\ldots\ldots\ldots\\
r_{k-2} &= q_k r_{k-1} + r_k, & \delta(r_k) &< \delta(r_{k-1}),\\
r_{k-1} &= q_{k+1} r_k, & r_{k+1} &= 0.
\end{aligned}$$

Это действительно так, поскольку строго убывающая цепочка неотрицательных целых чисел

$$\delta(b) > \delta(r_1) > \delta(r_2) > \ldots$$

должна оборваться, а обрыв может произойти только за счет обращения в нуль одного из остатков.

Утверждается, что последний отличный от нуля остаток $r_k$ является как раз наибольшим общим делителем элементов $a$ и $b$.

*Доказательство.* Действительно, по условию $r_k | r_{k-1}$. Двигаясь в данной системе снизу сверх, получим цепочку

$$r_k | r_{k-1}, \quad r_k | r_{k-2}, \ldots, r_k | r_2, \quad r_k | r_1,$$

и, наконец,

$$r_k | b, \quad r_k | a.$$

Значит, $r_k$ — общий делитель элементов $a$ и $b$.

Обратно, пусть $c$ — некоторый общий делитель элементов $a$ и $b$. Будем теперь двигаться по нашем системе в прямом направлении. Если $c$ делит $a$ и $b$, то делит и $r_1$. Если $c$ делит $b$ и $r_1$, то делит и $r_2$. Двигаясь так дальше, получаем, что $c$ делит $r_k$, что и требовалось.

Значит,

$$r_k = \text{НОД}(a, b).$$

□

Заметим теперь, что каждый остаток $r_i$ в системе выражется в виде линейной комбинации с коэффициентами из $R$ от двух предыдущих остатков $r_{i-1}$ и $r_{i-2}$. При этом $r_1$ выражается через $a$ и $b$, а $r_2$ выражается через $b$ и $r_1$, тем самым снова выражаясь через $a$ и $b$. Последовательная подстановка в $r_i$ выражений $r_{i-1}$ и $r_{i-2}$ через $a$ и $b$ даст нам при $i = k$ выражение

$$r_k = au + bv$$

с какими-то элементами $u, v \in R$.

Получаем таким образом следующее утверждение:

**Теорема 2.** *В евклидовом кольце $R$ любые два элемента $a, b$ имеют наибольший общий делитель и наименьшее общее кратное. При помощи алгоритма Евклида можно найти такие $u, v \in R$, то будет выполнено соотношение*

$$НОД(a, b) = au + bv.$$

*В частности, элементы $a, b \in R$ взаимно просты тогда и только тогда, когда существуют элементы $u, v \in R$, для которых*

$$au + bv = 1.$$

**Следствие 1.** *Пусть $a, b, c$ — элементы евклидова кольца $R$.*
*(1) Если $НОД(a, b) = 1$ и $НОД(a, c) = 1$, то $НОД(a, bc) = 1$.*
*(2) Если $a|bc$ и $НОД(a, b) = 1$, то $a|c$.*
*(3) Если $b|a$, $c|a$ и $НОД(b, c) = 1$, то $bc|a$.*

*Доказательство.* (1) По доказанной теореме имеем

$$au_1 + bv_1 = 1, \quad au_2 + cv_2 = 1.$$

Перемножая соответственно левые и правые части этого равенства, получим

$$a(au_1u_2 + bu_2v_1 + cu_1v_2) + bc(v_1v_2) = 1.$$

Это и дает нужное утверждение.

(2) Имеем $au + bv = 1$, откуда

$$ac \cdot u + (bc)v = c.$$

Но $bc = aw$, поэтому

$$c = a(cu + wv),$$

то есть $a|c$.

(3) $ub + vc = 1$, откуда $uab + vac = a$. Элемент $ab$ делится на $bc$, элемент $ac$ делится на $bc$, поэтому $a$ делится на $bc$ что и требовалось.

□

Непосредственным шагом к установлению факториальности евклидова кольца служит

**Лемма 1.** *Всякое евклидово кольцо $R$ является кольцом с разложением (то есть любой элемент $a \neq 0$ из $R$ записывается в виде произведения простых).*

*Доказательство.* Пусть элемент $a \in R$ обладает собственным делителем $b$: $a = bc$, где $b$ и $c$ —необратимые элементы.

Докажем, что

$$\delta(b) < \delta(a).$$

Действительно, по свойству (1) нормы в евклидовом кольце имеем

$$\delta(b) \leqslant \delta(bc) = \delta(a).$$

Предположим, что $\delta(b) = \delta(a)$ и воспользуемся условием (2) в определении евклидова кольца — разделим $b$ на $a$ с остатком:

$$b = qa + r, \quad \delta(r) < \delta(a) \text{ или } r = 0.$$

Случай $r = 0$ отпадает, так как по условию $a$ не делится на $b$ (они не ассоциированны).

По той же причине $qc \neq 1$, то есть $1 - qc \neq 0$.

Получим

$$\delta(a) = \delta(b) \leqslant \delta(b(1 - qc)) = \delta(b - qa) = \delta(r) < \delta(a).$$

Получаем противоречие, из которого $\delta(b) < \delta(a)$.

Если теперь

$$a = a_1 a_2 \dots a_n,$$

где все $a_i$ необратимы, то

$$a_{m+1} a_{m+2} \dots a_n$$

— собственный делитель $a_m a_{m+1} \dots a_n$, и по доказанному

$$\delta(a) = \delta(a_1 a_2 \dots a_n) > \delta(a_2 \dots a_n) > \dots > \delta(a_n) > \delta(1).$$

Эта строго убывающая цепочка неотрицательных чисел имеет длину $n \leqslant \delta(a)$.

Значит, для элемента $a \in R$ имеется разложение максимальной длины, которое и будет разложением на простые множители. $\square$

**Теорема 3.** *Всякое евклидово кольцо факториально (то есть обладает свойством однозначности разложения на простые множители).*

*Доказательство.* С учетом леммы и критерия факториальности нам остается показать, что если $p$ — простой элемент кольца $R$, делящий произведение $dc$ каких-то элементов $b, c \in R$, то $p$ делит или $b$, или $c$.

Действительно, при $b = 0$ или $c = 0$ доказывать нечего.

Если же $bc \neq 0$ и $d = \text{НОД}(b, p)$, то $d$, будучи делителем простого элемента $p$, либо равен 1 (точнее, является делителем единицы), либо ассоциирован с $p$. В первом случае $b$ и $p$ оказываются взаимно простыми, поэтому $p|c$. Во втором случае $d = up$, $u|1$, поэтому $p|b$. □

**Следствие 2.** *Кольца $\mathbb{Z}$ и $F[X]$ факториальны ($F$ — произвольное поле).*

# НЕПРИВОДИМЫЕ МНОГОЧЛЕНЫ

Неприводимость многочлена степени $> 1$ или разложение его на неприводимые множители — понятия, тесно связанные с основным полем $F$. Например, над $\mathbb{R}$ многочлен $X^2 + 1$ неприводим, а над $\mathbb{C}$ он раскладывается на (линейные) множители $X^2 + 1 = (X + i)(X - i)$.

Как и простых чисел в $\mathbb{Z}$, так и *нормализованных неприводимых многочленов над произвольным полем $F$ бесконечно много.*

*Доказательство.* В случае бесконечного поля $F$ это ясно: достаточно рассмотреть неприводимые многочлены вида $X - c$, $c \in F$.

Если же поле $F$ конечно, то годится рассуждение Евклида. Именно, пусть уже найдены $n$ неприводимых многочленов $p_1, \ldots, p_n$. Многочлен

$$f = p_1 p_2 \ldots p_n + 1$$

имеет хотя бы один нормализованный простой делитель, поскольку $\deg f \geqslant n$. Обозначим его через $p_{n+1}$.

Он отличен от $p_1, \ldots, p_n$, так как из $p_{n+1} = p_s$ для какого-то $s \leqslant n$ следовало бы

$$p_s | (f - p_1 \ldots p_n), \text{ т.е. } p_s | 1.$$

□

Так как многочленов заданной степени над конечным полем конечное число, то можно сделать следующее полезное заключение.

*Над любым конечным полем существуют неприводимые многочлены коль угодно высокой степени.*

Неприводимые многочлены над полем $\mathbb{Q}$ играют особую роль в теории алгебраических чисел. Так как умножением на подходящее натуральное число от многочлена из $\mathbb{Q}[X]$ всегда можно перейти к многочлену из $\mathbb{Z}[X]$, то естественно уточнить сначала связь между свойствами приводимости над $\mathbb{Q}$ и $\mathbb{Z}$.