ЛЕКЦИЯ 18

ФАКТОРИАЛЬНОСТЬ ЕВКЛИДОВЫХ КОЛЕЦ

НЕПРИВОДИМЫЕ МНОГОЧЛЕНЫ

ЛЕММА ГАУССА И ПРИЗНАК ЭЙЗЕНШТЕЙНА

ФАКТОРИАЛЬНОСТЬ ЕВКЛИДОВЫХ КОЛЕЦ

В конце прошлой лекции мы получили следующее утверждение:

Теорема 1. *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 2. *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 $\mathbb{Z}$.

ЛЕММА ГАУССА И ПРИЗНАК ЭЙЗЕНШТЕЙНА

Назовем *содержанием* многочлена

$$f = a_0 + a_1 x + \dots a_n x^n \in R[x]$$

наибольший общий делитель $d = d(f)$ всех его коэффициентов. До сих пор мы говорили о НОД(a, b) двух элементов, но свойства НОД позволяют без труда распространить это понятие на любое конечное число элементов целостного кольца.

Если $d(f)$ — обратимый элемент в R, то многочлен f называют *примитивным.*

Лемма 2 (лемма Гаусса)**.** *Пусть R — факториальное кольцо и $f, g \in R[x]$. Тогда*

$$d(fg) \approx d(f) \cdot d(g).$$

В частности, произведение двух примитивных многочленов снова будет примитивным многочленом.

Доказательство. Начнем с последнего утверждения.

Пусть

$$F = a_0 + a_1 x + \dots + a_n x^n, \quad g = b_0 + b_1 x + \dots + b_m x^m$$

— примитивные многочлены из $F[x]$, произведение fg которых не является примитивным.

Значит, существует простой элемент $p \in R$, делящий $d(fg)$.

Выберем наименьшие индексы s, t, для которых

$$p \not| a_s, \quad p \not| b_t.$$

Такие индексы найдутся в силу примитивности f и g.

Коэффициентом при x^{s+t} в многочлене fg будет

$$c_{s+t} = a_s b_t + (a_{s+1} b_{t-1} + a_{s+2} b_{t-2} + \dots) + \\ + (a_{s-1} b_{t+1} + a_{s-2} b_{t+2} + \dots).$$

Так как a_{s-i} и b_{t-i} при $i > 0$ делятся на p по условию и $p | c_{s+t}$ по предположению, то мы имеем соотношение

$$pu = a_s b_t + pv,$$

из которого следует, что $p | a_s b_t$. Ввиду факториальности кольца R имеем $p | a_s$ или $p | b_t$ — противоречие.

Переходя к общему случаю, запишем произвольные многочлены $f, g \in R[x]$ в виде

$$f = d(f)f_0, \quad g = d(g)g_0,$$

где f_0, g_0 — примитивные многочлены.

Так как

$$fg = d(f)d(g) \cdot f_0 g_0$$

и по доказанному

$$d(f_0 g_0) \approx 1,$$

то

$$d(fg) \approx d(f)d(g).$$

□

Следствие 3. *Многочлен $f \in \mathbb{Z}[x]$, неприводимый над $\mathbb{Z}$, продолжает оставаться неприводимым над $\mathbb{Q}$ ($\deg f > 0$).*

Доказательство. Мы уже доказывали, что $\mathbb{Z}$ — факториальное кольцо, поэтому к нему можно применить лемму Гаусса.

Предположим, что $f = gh$, где $f \in \mathbb{Z}[x]$, а $g, h \in \mathbb{Q}[x]$.

Умножая обе части этого равенства на наименьшее общее кратное знаменателей всех коэффициентов у g и h, мы перепишем его в виде

$$af = bg_0 f_0,$$

где $a, b \in \mathbb{Z}$, и g_0, f_0 — примитивные многочлены над $\mathbb{Z}$.

По лемме Гаусса

$$a \cdot d(f) = b,$$

так что получается разложение

$$f = d(f) g_0 h_0 \text{ над } \mathbb{Z}.$$

Остается вспомнить о неприводимости f в $\mathbb{Z}[x]$. □

Теорема 3 (критерий неприводимости Эйзенштейна)**.** *Пусть*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_0$$

— нормализованный многочлен над $\mathbb{Z}$*, все коэффициенты* $a_1, \ldots, a_n$ *которого делятся на некоторое простое число* p*, но* a_n *не делится на* p^2*.*

Тогда $f(x)$ *неприводим над* $\mathbb{Q}$*.*

Доказательство. Предположим противное, воспользуемся следствием из леммы Гаусса и запишем f в виде произведения двух целочисленных многочленов:

$$f(x) = (x^s + b_1 x^{s-1} + \cdots + b_s)(x^t + c_1 x^{t-1} + \cdots + c_t), \quad st > 0.$$

Это разложение сохранится и в кольце $\mathbb{Z}_p[x]$, элементы которого получаются из целочисленных многочленов взятием их коэффициентов по модулю p.

Мы знаем, что кольцо $\mathbb{Z}_p[x]$ факториально.

Сравним два разложения:

$$x^s x^t = (x^s + \overline{b}_1 x^{s-1} + \ldots)(x^t + \overline{c}_1 x^{t-1} + \ldots), \quad s + t = n.$$

Видим, что

$$\overline{b}_i = 0 = \overline{c}_j,$$

то есть все коэффициенты b_i, c_j делятся на p.

В таком случае $a_n = b_s c_t$ делится на p^2 — противоречие. $\square$