ЛЕКЦИЯ 19

ЛЕММА ГАУССА И КРИТЕРИЙ ЭЙЗЕНШТЕЙНА

РАЗЛОЖЕНИЕ ДРОБЕЙ В СУММУ ПРОСТЕЙШИХ

ЛЕММА ГАУССА И КРИТЕРИЙ ЭЙЗЕНШТЕЙНА

Назовем *содержанием* многочлена

$$f = a_0 + a_1X + \dots a_nX^n \in R[X]$$

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 1 (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

$$F = a_0 + a_1X + \dots + a_nX^n, \quad g = b_0 + b_1X + \dots + b_mX^m$$

— 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

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

$\square$

Следствие 1. *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 $\mathbb{Z}[X]$. $\square$

Теорема 1 (критерий неприводимости Эйзенштейна). *Пусть*

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

— нормализованный многочлен над $\mathbb{Z}$*, все коэффициенты* $a_1, \dots, a_n$ *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:

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

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:

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

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. $\square$

РАЦИОНАЛЬНЫЕ ДРОБИ

Пусть F — поле, $F[X]$ — кольцо многочленов над F. Поле отношений $Q(F[X])$ кольца $F[X]$ обозначается символом $F(X)$ и называется *полем рациональных дробей* от переменной X с коэффициентами из F.

Заметим, что поле рациональных дробей $F(X)$ всегда содержит бесконечное число элементов, а его характеристика совпадает с характеристикой поля F.

Соответственно, поле $\mathbb{Z}_p(X)$ дает нам пример бесконечного поля положительной характеристики.

Каждая рациональная дробь записывается (многими способами) в виде f/g или $\frac{f}{g}$, где f, g — многочлены из кольца $F[X]$, $g \neq 0$.

По определению $f/g = f_1/g_1$ тогда и только тогда, когда $fg_1 = f_1 g$. Дробь не меняется, если ее числитель и знаменатель умножить или сократить на один и тот же многочлен. В частности, целое число (положительное или отрицательное)

$$\deg f - \deg g$$

не зависит от представления ненулевой рациональной дроби в виде отношения (частного) f/g двух многочленов.

Это число называется *степенью дроби*.

Рациональная дробь от переменной X называется *несократимой*, если ее числитель взаимно прост со знаменателем.

С точностью до множителя из F, общего для числителя и знаменателя, любая рациональная дробь f/g однозначно определяется некоторой несократимой дробью.

В самом деле, деление f и g на НОД(f, g) приводит к несократимой дроби, а равенство

$$f/g = f_1/g_1$$

двух несократимых дробей, выраженное в виде $fg_1 = f_1g$, дает $f = cf_1$, $c \in F$, $g = cg_1$.

Если

$$\deg(f/g) = \deg f - \deg g < 0,$$

то (несократимая) дробь f/g называется *правильной* (нулевой многочлен считается правильной дробью, так как мы считаем $\deg 0 = -\infty$).

Теорема 2. *Каждая рациональная дробь из $F(X)$ однозначно представима в виде суммы многочлена и правильной дроби.*

Доказательство. Алгоритм деления с остатком, примененный к числителю и знаменателю дроби f/g, дает равенство

$$f = qg + r, \text{ где } \deg r < \deg g.$$

Теперь

$$f/g = q + r/g$$

есть искомая запись, сравнение которой с любой другой записью того же типа

$$f/g = \overline{q} + \overline{r}/\overline{g} \quad (\overline{q}, \overline{r}, \overline{g} \in F[X], \ \deg \overline{r} < \deg \overline{g})$$

приводит к соотношению

$$\overline{q} - q = \frac{r}{g} - \frac{\overline{r}}{\overline{g}} = \frac{r\overline{g} - \overline{r}g}{g\overline{g}}.$$

Так как

$$\overline{q} - q \in F[X],$$

а

$$\deg\left(\frac{r\overline{g} - \overline{r}g}{g\overline{g}}\right) = \deg(r\overline{g} - \overline{r}g) - \deg g - \deg \overline{g} < 0,$$

то это возможно лишь в случае $\overline{q} - q = 0$ и $r/g = \overline{r}/\overline{g}$. $\square$

Замечание 1. Множество $F_0(X)$ всех правильных дробей, рассматриваемое вместе с операциями сложения и умножения в $F(X)$, является кольцом без единицы 1.

Доказательство. Действительно, пусть

$$f_1/g_1, f_2/g_2 \in F_0(X).$$

Так как

$$\deg f_1 f_2 = \deg f_1 + \deg f_2 < \deg g_1 + \deg g_2 = \deg g_1 g_2,$$

то

$$\left(\frac{f_1}{g_1}\right)\left(\frac{f_2}{g_2}\right) = \frac{f_1 f_2}{g_1 g_2} \in F_0(X).$$

Далее,

$$\frac{f_1}{g_1} \pm \frac{f_2}{g_2} = \frac{f_1 g_2 \pm f_2 g_1}{g_1 g_2} \in F_0(X),$$

так как степени каждого из слагаемых $f_1 g_2$ и $f_2 g_1$ строго меньше степени знаменателя $g_1 g_2$.

Мы уже условились, что $0 \in F_0(X)$, при этом $1 \notin F_0(X)$. $\square$

ПРОСТЕЙШИЕ ДРОБИ

Правильная рациональная дробь $f/g \in F(X)$ называется *простейшей*, если $g = p^n$, $n \geqslant 1$, где $p = p(X)$ — неприводимый многочлен, причем $\deg f < \deg p$.

Основной теоремой о рациональных дробях является

Теорема 3. *Каждая правильная рациональная дробь может быть разложена, и притом единственным образом, в сумму простейших.*

Доказательство. Пусть $f/g \in F(X)$ — данная нам правильная рациональная дробь, в которой без ограничения общности многочлен g можно считать нормализованным.

Дальнейшие рассуждения распадаются на ряд этапов.

Этап 1. Предположим, что $g = g_1 g_2$ — произведение двух взаимно простых нормализованных многочленов. Тогда

$$\frac{f}{g_1 g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2},$$

причем обе дроби в правой части правильные, а сама запись в виде суммы единственна.

Доказательство. Действительно, из взаимной простоты g_1 и g_2 следует, что
$$1 = u_1 g_1 + u_2 g_2$$
для некоторых $u_1, u_2 \in F(X)$.

Если теперь
$$f u_2 = q g_1 + f_1, \quad \deg f_1 < \deg g_1$$
(делениие $f u_2$ на g_1 с остатком), то
$$f = f_1 g_2 + f_2 g_1, \text{ где } f_2 = f u_1 + q g_2.$$
Разделив обе части этого соотношения на $g_1 g_2$, мы придем к искомому разложению, поскольку по построению $f_1/g_1 \in F_0(X)$, а разность двух правильных дробей — правильная дробь.

Так мы доказали существование искомого разложения. Докажем единственность.

Пусть теперь наряду с разложением $f/g = f_1/g_1 + f_2/g_2$ есть еще одно разложение $f/g = f_1'/g_1 + f_2'/g_2$ в сумму правильных дробей. Тогда их равенства
$$f_1/g_1 + f_2/g_2 = f_1'/g_1 + f_2'.g_2$$
будем иметь
$$(f_1 - f_1')g_2 = (f_2 - f_2')g_1.$$
Из делимости $(f_1 - f_1')g_2$ на g_1 и из взаимной простоты g_1 и g_2, следует, что разность $f_1 - f_1'$ должна делиться на g_1. Но $\deg(f_1 - f_1') < \deg g_1$, откуда следует, что $f_1 - f_1'$. Единственность разложения установлена. $\square$

Этап 2.

Пусть в правильной рациональной дроби f/g для нормализованного занменателя g имеется каноническое разложение

$$g = p_1^{n_1} p_2^{n_2} \dots p_m^{n_m}$$

в произведение степеней попарно различных нормализованных неприводимых над F многочленов $p_1(X)$, $p_2(X)$,..., $p_m(X)$.

Тогда существует однозначно определенное разложение

$$\frac{f}{g} = \sum_{i=1}^{m} f_i p_i^{n_i}$$

в сумму правильных дробей $f_i/p_i^{n_i}$.

Доказательство. Наше утверждение легко получается индукцией по m, базу для которого дает этап 1:

$$\frac{f}{g} = \frac{f_1}{p_1^{n_1}} + \frac{f_0}{p_2^{n_2} \dots p_m^{n_m}} = \frac{f_1}{p_1^{n}} + \left(\frac{f_2}{p_2^{n_2}} + \dots + \frac{f_m}{p_m^{n_m}} \right).$$

Так как f_1 и f_0 определены однозначно, то по предположению индукции это верно и относительно $f_2, \dots, f_m$. $\square$

Этап 3.

Всякая правильная примарная дробь a/p^n представляется, и притом единственным образом, в виде суммы правильных простейших дробей.

Доказательство. Действительно, так как по условию

$$\deg a < n \deg p,$$

то евклидов алгоритм деления с остатком приведет нас к системе неравенств

$$\begin{array}{rlr}
a &= q_1 p^{n-1} + r_1, & \deg r_1 < (n-1)\deg p, \\
r_1 &= q_2 p^{n-2} + r_2, & \deg r_2 < (n-2)\deg p, \\
\multicolumn{2}{c}{\dots\dots\dots\dots\dots\dots} & \dots\dots\dots\dots \\
r_{n-2} &= q_{n-1} p + r_{n-1}, & \deg r_{n-1} < \deg p, \\
r_{n-1} &= q_n, &
\end{array}$$

где $\deg q_i < \deg p$ для всех однозначно определенных частных $q_1, \dots, q_n$.

Мы видим, что

$$a = q_1 p^{n-1} + q_2 p^{n-2} + \dots + q_{n-1} p + q_n,$$

откуда

$$\frac{a}{p^n} = \frac{q_1}{p} + \frac{q_2}{p^2} + \dots + \frac{q_{n-1}}{p^{n-1}} + \frac{q_n}{p^n}.$$

Так как $\deg q_i < \deg p$, то броби q_i/p^i являются простейшими. По построению они однозначно определены. $\square$

Этап 4.

Рассуждения этапов 1–3, соединенные вместе, дают все, что нужно. $\square$