ЛЕКЦИЯ 19

РАЗЛОЖЕНИЕ РАЦИОНАЛЬНЫХ ДРОБЕЙ В СУММУ ПРОСТЕЙШИХ

КОРНИ МНОГОЧЛЕНОВ, ТЕОРЕМА БЕЗУ

ДИФФЕРЕНЦИРОВАНИЯ МНОГОЧЛЕНОВ

РАЦИОНАЛЬНЫЕ ДРОБИ

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

Заметим, что поле рациональных дробей $\mathbb{F}(x)$ всегда содержит бесконечное число элементов, а его характеристика совпадает с характеристикой поля $\mathbb{F}$.

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 $\mathbb{F}[x]$, $g \neq 0$.

По определению $f/g = f_1/g_1$ тогда и только тогда, когда $fg_1 = f_1g$. 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 $\mathbb{F}$, 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 1. *Каждая рациональная дробь из $\mathbb{F}(x)$ 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

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

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 $r/g = \overline{r}/\overline{g}$. □

Замечание 1. Множество $\mathbb{F}_0(x)$ всех правильных дробей, рассматриваемое вместе с операциями сложения и умножения в $\mathbb{F}(x)$, является кольцом без единицы 1.

Доказательство. Действительно, пусть

$$f_1/g_1, f_2/g_2 \in \mathbb{F}_0(x).$$

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

$$\left(\frac{f_1}{g_1}\right)\left(\frac{f_2}{g_2}\right) = \frac{f_1 f_2}{g_1 g_2} \in \mathbb{F}_0(x).$$

Далее,

$$\frac{f_1}{g_1} \pm \frac{f_2}{g_2} = \frac{f_1 g_2 \pm f_2 g_1}{g_1 g_2} \in \mathbb{F}_0(x),$$

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 $0 \in \mathbb{F}_0(x)$, при этом $1 \notin \mathbb{F}_0(x)$. $\square$

ПРОСТЕЙШИЕ ДРОБИ

Правильная рациональная дробь $f/g \in \mathbb{F}(x)$ 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 2. *Каждая правильная рациональная дробь может быть разложена, и притом единственным образом, в сумму простейших.*

Доказательство. Пусть $f/g \in \mathbb{F}(x)$ — 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 $u_1, u_2 \in \mathbb{F}(x)$.

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 $f_1/g_1 \in \mathbb{F}_0(x)$, 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 $f_2, \dots, f_m$. □

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

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

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 дроби q_i/p^i являются простейшими. По построению они однозначно определены. $\square$

Этап 4.

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

КОРНИ МНОГОЧЛЕНОВ

Займемся тем, ради чего в прошлом изучали алгебру, — корнями многочленов. Дело в том, что многие задачи математики в конечном счете сводятся к вычислению отдельных корней конкретных многочленов или к качественному описанию их совокупности.

Пусть коммутативное кольцо R с единицей содержится в целостном кольце S.

Определение 1. Элемент $c \in S$ называется *корнем* (или *нулем*) *многочлена* $f \in R[x]$, если $f(c) = 0$.

Говорят также, что c — корень уравнения $f(x) = 0$.

Необходимость рассмотрения колец, содержащих кольцо R собственным образом, станет понятной, если вспомнить, что многочлен $f(x) = x^2 + 1$ не имеет корней над полем $\mathbb{R}$, но при этом для $i \in \mathbb{C}$ имеет место $f(i) = 0$.

При этом сначала мы рассмотрим случай $S = R$.

Теорема 3 (теорема Безу)**.** *Элемент $c \in R$ является корнем многочлена $f \in R[x]$ тогда и только тогда, когда многочлен $x - c$ делит f в кольце $R[x]$.*

Доказательство. Эта теорема — часть более общего утверждения, которое мы могли бы доказать давно. А именно, алгоритм деления с остатком гласит, что

$$f(x) = (x - c)q(x) + r(x), \text{ где } \deg r(x) < \deg(x - c) = 1.$$

Значит, $r(x)$ — константа.

Подставим вместо x константу c:

$$f(c) = r(c),$$

то есть $r(x)$ — это константа c.

Таким образом, всегда

$$f(x) = (x - c)q(x) + f(c).$$

В частности,

$$f(c) = 0 \Longleftrightarrow f(x) = (x - c)q(x).$$

□

Деление многочлена $f(x)$ с коэффициентами в целостном кольце R на линейный многочлен $x - c$ удобно осуществлять по так называемой *схеме Горнера*, более простой, чем общий алгоритм деления с остатком.

Именно, пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \quad a_i \in R.$$

По формуле, полученной в доказательстве теоремы Безу,

$$q(x) = b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-1}, \quad b_j \in R.$$

Подставим теперь эти выражения в формулу

$$f(x) = (x - c)q(x) + f(c)$$

и сравним коэффициенты при одинаковых степенях x (начиная со старших).

После небольшого преобразования получим

$$\begin{aligned}
&b_0 = a_0,\\
&\cdots\cdots\cdots\\
&b_k = b_{k-1}c + a_k,\\
&\cdots\cdots\cdots\\
&b_{n-1} = b_{n-2}c + a_{n-1},\\
&f(c) = b_{n-1}c + a_n,
\end{aligned}$$

так что заодно вычисляется значение f при $x = c$.

Рекуррентные формулы, в которых и заключается схема Горнера, удобны при счете.

Введем теперь более общее

ОПРЕДЕЛЕНИЕ 2. Элемент $c \in R$ называется k-кратным корней многочлена $f \in R[x]$, если f делится на $(x-c)^k$, но не делится на $(x-c)^{k+1}$.

Корень кратности 1 называют *простым корнем.*

Итак, $c \in R$ — корень кратности k многочлена $f \in R[x]$ тогда и только тогда, когда

$$f(X) = (X-c)^k g(X),$$

где

$$\text{НОД}(x-c, g(x)) = 1.$$

Последнее условие также выражается неравенством $g(c) \neq 0$.

Понятно, что $k \leqslant \deg f$.

Имеет место важная

Теорема 4. *Пусть R — целостное кольцо, $f \neq 0$ — многочлен из $R[x]$, $c_1, \ldots, c_r$ — его корни в R кратностей $k_1, \ldots, k_r$, соответственно.*

Тогда

$$f(x) = (x-c)^{k_1} \ldots (x-c)^{k_r} g(x),$$
$$g(x) \in R[x], \quad g(c_i) \neq 0, \quad i = 1, \ldots, r.$$

В частности, число корней многочлена $f \in R[x]$, рассматриваемых вместе с их кратностями, не превосходит степени многочлена

$$k_1 + k_2 + \cdots + k_r \leqslant \deg f.$$

Доказательство. Достаточно перейти к полю отношений $Q(R)$ (если кольцо R не было полем с самого начала) и воспользоваться однозначностью разложения на простые множители (в данном случае на $x - c_1, \ldots, x - c_r$) в кольце $Q(R)[x]$. Однако в реальности нет необходимости применять такое мощное математическое оружие, будем рассуждать просто и прямо.

Так как

$$\deg f = (k_1 + \cdots + k_r) + \deg g,$$

то искомое неравенство — следствие делимости f на $(x-c_1)^{k_1} \ldots (x-c_r)^{k_r}$, которую мы установим индукцией по r.

При $r = 1$ доказывать нечего.

Пусть мы уже знаем, что

$$f(x) = (x - c_1)^{k_1} \ldots (x - c_{r-1})^{k_{r-1}} h(x).$$

Так как у нас

$$c_r - c_1 \neq 0, \quad \ldots, \quad c_r - c_{r-1} \neq 0$$

и R — целостное кольцо, то элемент c_r не является корнем многочлена

$$(x - c_1)^{k_1} \ldots (x - c_{r-1})^{k_{r-1}}.$$

Но c_r — k_r-кратный корень многочлена f, то есть

$$f(x) = (x - c_r)^{k_r} \cdot u(x).$$

Поэтому $h(c_r) = 0$. Соответственно,

$$h(x) = (x - c_r)^s v(x), \quad s \leqslant k_r.$$

Имеем

$$(x-c_r)^{k_r}u(X) = f(X) = \\ = (x-c_1)^{k_1}\dots(x-c_{r-1})^{k_{r-1}}(x-c_r)^s v(x).$$

Используя закон сокращения в целостном кольце $R[x]$, приходим к заключению, что $s = k_r$. □

Без предположения о целостности кольца R доказанная теорема перестает быть верной, как показывает пример многочлена

$$f(x) = x^3$$

над кольцом $\mathbb{Z}_8$:

$$f(0) = f(2) = f(4) = f(6) = 0.$$

Разложение f на простые множители в $\mathbb{Z}_8$ тоже неоднозначно:

$$f = x^3 = x(x-4)^2 = (x-2)(x^2+2x+4) = (x-6)(x^2-2x+4).$$

Из доказанной нами теоремы вытекает

Следствие 1. *Два многочлена $f, g \in R[x]$ степени $\leqslant n$, принимающие одинаковые значения при подстановке $n+1$ различных элементов из целостного кольца R, равны: $f = g$.*

Доказательство. Положим $h := f - g$, так что $\deg h \leqslant n$. По условию

$$h(c_1) = \dots = h(c_{n+1}) = 0$$

для попарно различных элементов $c_1, \dots, c_{n+1} \in R$, то есть многочлен степени n имеет не менее $n+1$ корней. Противоречие. □

ДИФФЕРЕНЦИРОВАНИЯ КОЛЬЦА МНОГОЧЛЕНОВ

Пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

— многочлен степени n над произвольным полем $\mathbb{F}$. Его *производной* называется многочлен

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \cdots + a_{n-1}.$$

Если мы имеем дело с полем $\mathbb{R}$, то это определение повторяет определение обычных производной (которую проходят в математическом анализе).

Однако и над произвольным полем имеют место хорошо известные из анализа соотношения

$$(\alpha f + \beta g)' = \alpha f' + \beta g', \quad \alpha, \beta \in \mathbb{F},$$

и

$$(fg)' = f'g + fg'.$$

Первое соотношение проверяется совершенно очевидным образом. Второе благодаря первому можно свести к тому случаю, когда $f = x^k$, $g = x^l$:

$$(x^{k+l})' = (k+l)x^{k+l-1} = (kx^{k-1})x^l + x^k(lx^{l-1}) = \\ = (x^k)'x^l + x^k(x^l)'.$$

Обобщением такой формулы дифференцирования произведения служит легко доказываемая по индукции формула

$$(f_1 f_2 \dots f_k)' = \sum_{i=1}^{k} f_1 \dots f_{i-1} f_i' f_{I+1} \dots f_k.$$

В частности,

$$(f^k)' = k f^{k-1} f'.$$

Будем обозначать отображение дифференцирования через

$$\frac{d}{dx} : f \to f'.$$

Результат m-кратного применения отображения $\frac{d}{dx}$ к $f(x)$ обычно обозначается символом $f^{(m)}(x)$.

Очевидно, что

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n \Longrightarrow f^{(n)}(x) = n! a_0,\ f^{(n+1)}(x) = 0.$$

Если $\mathbb{F}$ — поле нулевой характеристики, то

$$\deg f' = \deg f - 1.$$

Однако для полей положительной характеристики p это уже не так, поскольку

$$(x^{kp})' = kpx^{kp-1} = 0.$$

Все же некоторую пользу из рассмотрения производной можно извлечь и в общем случае.

Разделив произвольный многочлен $f \in \mathbb{F}[x]$ на $(x-c)^2$, $c \in \widetilde{\mathbb{F}}$, $\widetilde{\mathbb{F}} \supset \mathbb{F}$, а затем записав (линейный) остаток в виде

$$(x-c)s + r, \text{ где } s, r \in \widetilde{\mathbb{F}},$$

мы придем к соотношениям

$$\begin{aligned} f &= (x-c)^2 t(x) + (x-c)s + r, \\ f' &= (x-c)[2t(x) + (x-c)t'(x)] + s. \end{aligned}$$

Подставив в них значение $x = c$, получим

$$r = f(c), \quad s = f'(c),$$

то есть

$$f(x) = (x-c)^2 t(x) + (x-c)f'(c) + f(c).$$

Мы пришли к следующему утверждению:

Теорема 5. *Пусть $\mathbb{F}$ — произвольное поле, а $\widetilde{\mathbb{F}}$ — некоторое его расширение. Многчлен $f \in \mathbb{F}[x]$ имеет кратный корень $c \in \widetilde{\mathbb{F}}$ тогда и только тогда, когда*

$$f(c) = f'(c) = 0.$$

Предположим, что $\mathbb{F}$ — поле нулевой характеристики, и без ограничения общности под $\mathbb{F}$ можно понимать одно из полей $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Нормализованный неприводимый многочлен $p_i(x)$ в разложении

$$f(x) = \lambda p_1(x)^{k_1} \dots p_i(x)^{k_i} \dots p_r(x)^{k_r}, \quad \lambda \in \mathbb{F},$$

многочлена $f(x) \in \mathbb{F}[x]$ называется *k_i-кратным множителем* для f.

На практике получить разложение многочлена $f(x)$ в произведение неприводимых довольно сложно. Опишем вкратце метод, основанный на понятии производной и дающий возможность узнать, содержит ли $f(x)$ над данным полем $\mathbb{F}$ (или его расширением) кратные множители.

Теорема 6. *Пусть $p(x)$ есть k-кратный неприводимый множитель многочлена $f \in \mathbb{F}[x]$ ($k \geqslant 1$, $\deg p(x) \geqslant 1$).*

Тогда $p(x)$ бцдет $(k-1)$-кратным множителем производной $f'(x)$. В частности, при $k = 1$ f' не делится на $p(x)$.

Доказательство. По условию имеем

$$f(x) = p(x)^k g(x),$$

где

$$\text{НОД}(p(x), g(x)) = 1,$$

то есть $g(x)$ не делится на $p(x)$.

Применим правила производной суммы и произведения:

$$f'(x) = p(x)^{k-1}(kp'(x)g(x) + p(x)g'(x)).$$

Достаточно показать, что многочлен в скобках не делится на $p(x)$. Если бы это было не так, то на $p(x)$ делился бы многочлен $kp'(x)g(x)$, что, однако, невозможно, поскольку $g(x)$ не делится на $p(x)$, а

$$\deg kp'(x) < \deg p(x).$$

□

Понятно, что в ходе доказательства существенно были использованы и неприводимость $p(x)$, и условие $\operatorname{char}\mathbb{F} = 0$.

Следствие 2. *Для многочлена $f(x)$ коэффициентами в поле $\mathbb{F}$ характеристики ноль следующие два условия эквивалентны:*

(1) *f имеет в некотором расширении $\widetilde{\mathbb{F}} \supset \mathbb{F}$ поля $\mathbb{F}$ корень c кратности k;*

(2) *$f^{(j)}(c) = 0$, $0 \leqslant j \leqslant k-1$, но $f^{(k)}(c) \neq 0$.*

Доказательство. Применим k раз предыдущую теорему, имея в виду линейный множитель $p(x) = x - c$, с самого начала заменяя, в случае необходимости, поле $\mathbb{F}$ его расширением $\widetilde{\mathbb{F}}$. □

Следствие 3. *Если многочлен $f \in \mathbb{F}[X]$ степени $\geqslant 1$ раскладывается в произведение степеней неприводимых:*

$$f(x) = \lambda p_1(x)^{k_1} \dots p_i(x)^{k_i} \dots p_r(x)^{k_r}, \quad \lambda \in \mathbb{F},$$

то разложением для наибольшего общего делителя f и его производной f' будет

$$НОД(f, f') = p_1(x)^{k_1-1} p_2(x)^{k_2-1} \dots p_r(x)^{k_r-1}.$$

Доказательство. Действительно, по доказанной только что теореме каждый из простых делителей $p_i(x)$ многочлена $f(x)$ входит в разложение многочлена $f'(x)$ с показателем $k_i - 1$, то есть

$$f'(x) = p_1(x)^{k_1-1} p_2(x)^{k_2-1} \dots p_r(x)^{k_r-1} \cdot u(x),$$

где

$$\text{НОД}(u, p_i) = 1, \quad 1 \leqslant i \leqslant r.$$

Поэтому получается условие следствия. □

Используя это утверждение про $\text{НОД}(f, f')$, мы получаем средство освободиться от кратных множителей, вхдящих в разложение $f(x)$. Именно, многочлен

$$g(x) = \frac{f(x)}{\text{НОД}(f, f')} = p_1(x) p_2(x) \dots p_r(x)$$

содержит те же простые делители, что и $f(x)$, но с единичной кратностью.

Важно отметить, что многочлен $g(x)$ можно найти, не зная фактически разложений для f и f', а используя лишь алгоритм Евклида.