Тема I: Многочлены

§ 6. Отделение кратных множителей

М.В.Волков

Уральский федеральный университет
Институт естественных наук и математики
кафедра алгебры и фундаментальной информатики

2021/2022 учебный год

Кратность неприводимого множителя

По теореме о разложении многочлена на неприводимые множители произвольный многочлен f положительной степени над полем F однозначно представи́м в виде

$$f = \alpha p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}.$$

Здесь $p_1, p_2, \ldots, p_m$ – попарно различные неприводимые над F унитарные многочлены, $k_1, k_2, \ldots, k_m \in \mathbb{N}$, а $\alpha \in F$.

Многочлены $p_1, p_2, \ldots, p_m$ называются *неприводимыми множителями* многочлена f, а число k_i (где $1 \leq i \leq m$) – *кратностью* неприводимого множителя p_i. Множители p_i, для которых $k_i > 1$, называют *кратными*.

Разложить многочлен в произведение неприводимых – трудная задача. Однако оказывается, что довольно просто *отделить кратные множители*, т.е. найти многочлен

$$g = p_1^{k_1-1} p_2^{k_2-1} \cdots p_m^{k_m-1}.$$

Здесь мы считаем, что $p_i^0 = 1$, т.е. в разложении g участвуют в точности кратные множители многочлена f.

Характеристика поля

Пусть F – произвольное поле, $x \in F$, а n – натуральное число. Положим $nx := \underbrace{x + x + \cdots + x}_{n \text{ раз}}$. Если существует натуральное число n такое, что $nx = 0$ для всякого $x \in F$, то минимальное n с таким свойством называется *характеристикой* поля F; если такого n не существует, то характеристика поля F полагается равной 0. Характеристика поля F обозначается через $\operatorname{char} F$.
Примеры: $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$, а $\operatorname{char} \mathbb{F}_p = p$.

Нетрудно доказать, что характеристика всякого поля равна либо нулю, либо простому числу (*упражнение*).

Решение: Пусть $\operatorname{char} F = n$. Имеем $n > 1$, поскольку в поле $1 \neq 0$. Возьмем простой делитель p числа n. Тогда $n = pk$ для некоторого $k < n$ и

$$0 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ раз}} = \underbrace{1 + 1 + \cdots + 1}_{p \text{ раз}} \cdot \underbrace{1 + 1 + \cdots + 1}_{k \text{ раз}}.$$

В поле нет делителей нуля, поэтому один из сомножителей равен 0. Второй сомножитель не равен 0, так как $k < n$, а n – минимальное число с тем свойством, что $\underbrace{1 + 1 + \cdots + 1}_{n \text{ раз}} = 0$. Значит, первый сомножитель равен 0, и из минимальности n следует, что $n = p$. □

Определение

Пусть $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_0$ – многочлен над кольцом R. Если $n > 0$, то *производной* многочлена $f(x)$ называется многочлен $n\alpha_n x^{n-1} + (n-1)\alpha_{n-1} x^{n-2} + \cdots + \alpha_1$, обозначаемый через $f'(x)$. Если $n = 0$, то по определению $f'(x) = 0$.

Для многочленов над полем $\mathbb{R}$ производная многочлена в нашем смысле совпадает с производной многочлена как функции от одной переменной в смысле математического анализа.

Степень производной многочлена степени n не обязательно равна $n-1$. Например, для многочлена $f(x) = x^p$ над полем $\mathbb{F}_p$ имеем $f'(x) = px^{p-1} = 0$, поскольку $\operatorname{char} \mathbb{F}_p = p$.

Замечания:

а) для любого многочлена f над любым кольцом R выполнено неравенство $\deg f' \leq \deg f - 1$,

б) если f – многочлен степени > 0 над полем характеристики 0, то $\deg f' = \deg f - 1$.

Лемма о свойствах производной

Если $f(x)$ и $g(x)$ — многочлены над кольцом R, $\alpha \in R$, а $m \in \mathbb{N}$, то:

1) $(\alpha f)' = \alpha f'$,
2) $(f+g)' = f' + g'$,
3) $(fg)' = f'g + fg'$,
4) $(f^m)' = mf^{m-1}f'$.

Доказательство. 1) и 2) непосредственно вытекают из определений.

3) В силу свойств 1) и 2) свойство 3) достаточно доказать в случае, когда $f(x) = x^n$, а $g(x) = x^m$ для некоторых n и m. В самом деле, в этом случае

$$(fg)' = (x^{n+m})' = (n+m)x^{n+m-1},$$
$$f'g = nx^{n-1} \cdot x^m = nx^{n+m-1}, \quad \text{и}$$
$$fg' = x^n \cdot mx^{m-1} = mx^{n+m-1}.$$

Следовательно, $f'g + g'f = (n+m)x^{n+m-1} = (fg)'$.

4) выводится из 3) индукцией по m. □

Лемма о производной неприводимого многочлена

Если p – неприводимый многочлен и $p' \neq 0$, то НОД$(p, p') = 1$.

Доказательство. Положим $d =$ НОД(p, p'). Тогда $p = dq$ и $p' = dr$ для некоторых многочленов q и r. Если $\deg q = 0$, то

$$\deg p = \deg dq = \deg d + \deg q = \deg d \leq \deg p' \leq \deg p - 1.$$

Полученное противоречие показывает, что $\deg q \neq 0$, и потому $q \notin F$. Следовательно, $d \in F$. Раз $d \neq 0$, заключаем, что d ассоциирован с 1. □

Замечание. Условие $p' \neq 0$ в формулировке леммы *существенно*. Приведем пример неприводимого многочлена p, для которого оно не выполняется. Рассмотрим поле $\mathbb{F}_2(y)$ рациональных функций от y над двухэлементным полем $\mathbb{F}_2$. Многочлен $p(x) = x^2 + y$ неприводим над $\mathbb{F}_2(y)$ по обобщенному критерию Эйзенштейна. Однако $p'(x) = 2x = 0$, так как $\operatorname{char} \mathbb{F}_2 = 2$.

Предложение о неприводимых множителях многочлена и его производной

Пусть F – поле характеристики 0, а p – неприводимый множитель кратности k многочлена $f \in F[x]$. Если $k = 1$, то p не делит f'. Если $k > 1$, то p является неприводимым множителем многочлена f' кратности $k - 1$.

Доказательство. Обозначим через g произведение всех неприводимых множителей многочлена f, отличных от p, и старшего коэффициента многочлена f. Тогда $f = p^k g$ и $p \nmid g$. Раз $\operatorname{char} F = 0$, то $p' \neq 0$ и по лемме о производной неприводимого многочлена имеем НОД$(p, p') = 1$.
Из свойств взаимно простых многочленов заключаем, что p не делит $p'g$. Если $k = 1$, то $f = pg$, и потому $f' = (pg)' = p'g + pg'$. Если бы p делил f', то p делил бы и $p'g = f' - pg'$. Итак, если $k = 1$, то p не делит f'.
Пусть теперь $k > 1$. Тогда

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

Видно, что p^{k-1} делит f'. Осталось проверить, что p не делит $kp'g + pg'$. Предположим, что p делит $kp'g + pg'$. Тогда, очевидно, p делит и $kp'g$. Поскольку $\operatorname{char} F = 0$, в F есть элемент α, обратный к $\underbrace{1 + 1 + \cdots + 1}_{k \text{ раз}} \neq 0$.
Умножив $kp'g$ на α, получим, что p делит $p'g$, что невозможно. □

Отделение кратных множителей

Пусть $f = \alpha p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ — разложение на неприводимые множители многочлена f над полем F нулевой характеристики и $k = \max_i\{k_i\}$. Обозначим через d_j, $j = 1, 2, \ldots, k$, произведение всех тех неприводимых множителей многочлена f, кратность которых равна j, т.е. $d_j := \prod_{k_i=j} p_i$. (Если множителей какой-то кратности j нет, полагаем $d_j := 1$.) Тогда

$$f = \alpha d_1 d_2^2 d_3^3 \cdots d_k^k,$$

поскольку неприводимые множители из d_1 входят в разложение f по одному разу, множители из d_2 – по два раза и т.д. Из предложения о неприводимых множителях многочлена и его производной вытекает, что

$$f_1 := \text{НОД}(f, f') = d_2 d_3^2 \cdots d_k^{k-1}.$$

Многочлен $g_1 := \frac{f}{\alpha f_1} = d_1 d_2 \cdots d_k = p_1 p_2 \cdots p_m$ есть произведение всех попарно различных неприводимых множителей f. Применяя эту же процедуру к многочлену f_1, можно найти многочлены

$$f_2 := \text{НОД}(f_1, f_1') = d_3 \cdots d_k^{k-2} \quad \text{и} \quad g_2 := \frac{f_1}{f_2} = d_2 \cdots d_k.$$

Разделив g_1 на g_2, найдем d_1. Продолжая этот процесс, можно *отделить кратные множители* многочлена f, т.е. найти все многочлены $d_2, \ldots, d_k$.

По следствию теоремы Безу α является корнем многочлена $f(x)$ тогда и только тогда, когда $(x-\alpha)|f(x)$, т.е. когда двучлен $x-\alpha$ служит одним из неприводимых множителей многочлена $f(x)$.
Если $x-\alpha$ – множитель кратности $k>1$ для $f(x)$, то α называют *кратным корнем*, а число k – *кратностью* этого корня.
Следствием проведенных выше рассмотрений является полезный факт:

Замечание (исключение кратных корней)

Пусть f – многочлен на полем характеристики 0. Многочлен $\dfrac{f}{\text{НОД}(f,f')}$ *имеет те же корни, что и f, но не имеет кратных корней. В частности, если* $\text{НОД}(f,f')=1$, *то сам многочлен f не имеет кратных корней.*