

# Тема I: Многочлены

## § 7. Поле разложения многочлена

М.В.Волков

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

2021/2022 учебный год

Мы уже неоднократно сталкивались с ситуациями, когда у многочлена нет корней в поле  $F$ , но есть корни в некотором большем поле  $F' \supset F$ .

*Примеры.* 1) У многочлена  $x^2 - 2$  нет корней в  $\mathbb{Q}$ , но есть корни в  $\mathbb{R}$ :

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

2) У многочлена  $x^2 + 1$  нет корней в  $\mathbb{R}$ , но есть корни в  $\mathbb{C}$ :

$$x^2 + 1 = (x - i)(x + i).$$

*Вопрос:* Для каждого ли многочлена  $f \in F[x]$  имеется такое поле  $F' \supset F$ , которое содержит все корни  $f$ ?

Если такое поле  $F'$  существует, то над ним многочлен  $f$  разлагается в произведение линейных множителей:

$$f = a(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \cdots (x - \alpha_s)^{k_s}.$$

Здесь  $a \in F$  – старший коэффициент многочлена,  $\alpha_1, \alpha_2, \dots, \alpha_s \in F'$  – все его различные корни,  $k_i$  – кратность корня  $\alpha_i$ , и  $k_1 + k_2 + \cdots + k_s = \deg f$ . Поэтому такое поле  $F'$  называют *полем разложения* многочлена  $f$ .

## Теорема (существование поля разложения)

Для любого поля  $F$  и любого многочлена  $f$  над  $F$  существует поле разложения  $F' \supseteq F$ .

*Доказательство.* Проведем индукцию по  $\deg f$ . Если  $\deg f = 1$ , доказывать нечего, так как корень линейного двучлена лежит в самом поле  $F$ .

Пусть  $\deg f > 1$  и многочлен  $f$  приводим над  $F$ . Тогда  $f = gh$  для некоторых многочленов  $g$  и  $h$  над  $F$  таких, что  $\deg g, \deg h < \deg f$ .

По предположению индукции, примененному к полю  $F$  и многочлену  $g$ , имеется поле  $F_1 \supseteq F$ , содержащее все корни  $g$ , а по предположению индукции, примененному к полю  $F_1$  и многочлену  $h$ , имеется поле  $F_2 \supseteq F_1$ , содержащее все корни  $h$ . Ясно, что любой корень  $f$  – это корень одного из многочленов  $g$  и  $h$ , и потому  $F_2$  будет полем разложения для  $f$ .

Осталось рассмотреть случай, когда  $\deg f > 1$  и многочлен  $f$  неприводим над  $F$ . Достаточно построить поле  $F_1$ , в котором у  $f$  есть хотя бы один корень  $\alpha$ . Тогда  $f = (x - \alpha)f_1$ , где  $\deg f_1 = \deg f - 1$ , и по предположению индукции, примененному к полю  $F_1$  и многочлену  $f_1$ , имеется поле  $F_2 \supseteq F_1$ , содержащее все корни  $f_1$ . Оно будет полем разложения для  $f$ .

Итак,  $f$  – неприводимый над  $F$  многочлен степени  $> 1$  и нужно построить поле  $F_1$ , в котором у этого многочлена есть корень. Конструкция очень похожа на конструкцию поля вычетов по модулю простого числа.

Пусть  $n := \deg f$ . Ясно, что множество  $F^{<n}[x] := \{g \in F[x] \mid \deg g < n\}$  образует группу относительно обычного сложения многочленов.

Определим умножение в  $F^{<n}[x]$  так: «новое» произведение  $g \odot h$  многочленов  $g, h \in F^{<n}[x]$  – это остаток от деления на  $f$  их обычного произведения  $gh$ . Заметим, что  $g \odot h = gh$ , если  $\deg gh < n$ .

Понятно, что  $F^{<n}[x]$  с операциями  $+$  и  $\odot$  – коммутативно-ассоциативное кольцо с 1. Покажем, что оно является полем.

Если  $g \in F^{<n}[x]$  и  $g \neq 0$ , из неприводимости  $f$  следует, что  $\text{НОД}(f, g) = 1$ . Тогда существуют такие многочлены  $u, v \in F[x]$ , что  $ug + vf = 1$ . Поделим  $u$  на  $f$  с остатком:  $u = qf + r$ , где  $\deg r < n$ . Тогда  $r \in F^{<n}[x]$  и

$$1 = (qf + r)g + vf = rg + (qg + v)f,$$

откуда остаток от деления  $rg$  на  $f$  равен 1. Таким образом,  $r \odot g = 1$ . Мы проверили, что у каждого ненулевого элемента из  $F^{<n}[x]$  есть обратный, т.е.  $F^{<n}[x]$  с операциями  $+$  и  $\odot$  – поле.

Осталось показать, что в  $F^{<n}[x]$  у многочлена  $f$  есть корень.

Корнем будет ... корнем будет ... одночлен  $x$ .

Заметим прежде всего, что, поскольку  $n = \deg f > 1$ , многочлены 1-й степени, и в том числе  $x$ , лежат в  $F^{<n}[x]$ .

Без ограничения общности можно считать, что  $f$  унитарен. Тогда  $f = x^n + h$ , для некоторого  $h \in F^{<n}[x]$ , и потому остаток от деления  $x^n$  на  $f$  равен  $-h$ . Следовательно,  $\underbrace{x \odot x \odot \dots \odot x}_{n \text{ раз}} = -h$ , и, вычисляя

значение многочлена  $x^n + h$  от элемента  $x \in F^{<n}[x]$ , мы получим

$$\underbrace{x \odot x \odot \dots \odot x}_{n \text{ раз}} + h = -h + h = 0.$$

(Здесь учтено то, что значение  $h$  от  $x$  в  $F^{<n}[x]$  равно  $h$ , так как  $\underbrace{x \odot \dots \odot x}_{k \text{ раз}} = x^k$  при всех  $k < n$ , а сложение в  $F^{<n}[x]$  то же, что и в  $F[x]$ .)

Итак, мы проверили то утверждение, к которому свели доказательство теоремы о существовании поля разложения. □

Для иллюстрации применим описанное построение к многочлену  $x^2 + 1$ , неприводимому над полем  $\mathbb{R}$ .

Элементы поля  $\mathbb{R}^{<2}[x]$  суть линейные двучлены  $a + bx$ , где  $a, b \in \mathbb{R}$ .

Они складываются обычным способом:

$$(a_1 + b_1x) + (a_2 + b_2x) = (a_1 + a_2) + (b_1 + b_2)x,$$

а для умножения нужно сначала перемножить их в  $\mathbb{R}[x]$ :

$$(a_1 + b_1x)(a_2 + b_2x) = a_1a_2 + (a_1b_2 + b_1a_2)x + (b_1b_2)x^2,$$

и взять остаток от деления произведения на  $x^2 + 1$ , т.е. заменить  $x^2$  на  $-1$ . Это дает

$$(a_1 + b_1x) \odot (a_2 + b_2x) = (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)x.$$

Узнаем правила действий с комплексными числами в поле  $\mathbb{C}$ .

Более формально, отображение  $a + bx \mapsto a + bi$  является *изоморфизмом* между полями  $\mathbb{R}^{<2}[x]$  и  $\mathbb{C}$ . Итак, поле комплексных чисел  $\mathbb{C}$  можно было построить как поле разложения многочлена  $x^2 + 1$  (Коши, 1847).

Мы доказали, что для любого простого числа  $p$  над полем вычетов  $\mathbb{F}_p$  существуют неприводимые многочлены любой степени  $n$ .

Если применить конструкцию из доказательства теоремы о существовании поля разложения к полю  $\mathbb{F}_p$  и неприводимому над этим полем многочлену степени  $n$ , получим поле  $\mathbb{F}_p^{<n}[x]$ . Понятно, что в нем  $p^n$  элементов.

Итак, для любого простого числа  $p$  и любого натурального  $n$  существует поле из  $p^n$  элементов.

С другой стороны, легко понять, что если  $F$  – конечное поле, то число его элементов – степень простого числа. Действительно, характеристика  $F$  не может быть нулевой – иначе уже элементов вида  $\underbrace{1 + 1 + \dots + 1}_{k \text{ раз}}$  было

бы бесконечно много. Значит,  $\text{char } F = p$  для некоторого простого  $p$ .

Элементы  $0, 1, 1 + 1, \dots, \underbrace{1 + 1 + \dots + 1}_{p-1 \text{ раз}}$  различны между собой и образуют

подполе в  $F$ . Сопоставляя им соответственно вычеты  $0, 1, 2, \dots, p-1 \in \mathbb{F}_p$ , получим изоморфизм между этим подполем и полем вычетов  $\mathbb{F}_p$ .

Вспомним: любое поле является линейным пространством над любым своим подполем. Итак,  $F$  – конечномерное линейное пространство над  $\mathbb{F}_p$ . Если  $\dim F = n$ , то  $|F| = p^n$ .

Мы доказали такой результат:

### Теорема (о конечных полях)

*Поле из  $q$  элементов существует тогда и только тогда, когда  $q$  – степень простого числа.*

Можно доказать, что все поля из  $q$  элементов изоморфны между собой (Элиаким Гастингс Мур, 1893). Это оправдывает обозначение  $\mathbb{F}_q$ .

Альтернативное обозначение  $GF(q)$  – Galois field, поле Галуа.

Эварист Галуа (1811–1832) строил  $GF(p^n)$  по существу тем же способом, что был описан выше (с помощью многочлена  $n$ -й степени, неприводимого над полем вычетов по модулю  $p$ ) в работе, вышедшей в 1830 г.

Та же идея имеется в работе Гаусса 1797 г., опубликованной лишь в 1863 г.



Поле  $\mathbb{F}_4$  можно построить, исходя из многочлена  $x^2 + x + 1$ , т.е. единственного неприводимого многочлена 2-й степени над  $\mathbb{F}_2$ . Имеем  $\mathbb{F}_4 = \{0, 1, x, x + 1\}$ , а сложение и умножение в  $\mathbb{F}_4$  задаются так:

+	0	1	$x$	$x + 1$	×	0	1	$x$	$x + 1$
0	0	1	$x$	$x + 1$	0	0	0	0	0
1	1	0	$x + 1$	$x$	1	0	1	$x$	$x + 1$
$x$	$x$	$x + 1$	0	1	$x$	0	$x$	$x + 1$	1
$x + 1$	$x + 1$	$x$	1	0	$x + 1$	0	$x + 1$	1	$x$

Поле  $\mathbb{F}_9$  можно построить, исходя из одного из неприводимых многочленов 2-й степени над  $\mathbb{F}_3$ . Таких унитарных многочленов три:  $x^2 + 1$ ,  $x^2 + x + 2$ ,  $x^2 + 2x + 2$ . Возьмем  $x^2 + 1$ ; если взять другой многочлен, получится изоморфное поле. Имеем  $\mathbb{F}_9 = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}$ . Умножение ненулевых элементов в  $\mathbb{F}_9$  задается так:

$\times$	1	2	$x$	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$
1	1	2	$x$	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$
2	2	1	$2x$	$2x + 2$	$2x + 1$	$x$	$x + 2$	$x + 1$
$x$	$x$	$2x$	2	$x + 2$	$2x + 2$	1	$x + 1$	$2x + 1$
$x + 1$	$x + 1$	$2x + 2$	$x + 2$	$2x$	1	$2x + 1$	2	$x$
$x + 2$	$x + 2$	$2x + 1$	$2x + 2$	1	$x$	$x + 1$	$2x$	2
$2x$	$2x$	$x$	1	$2x + 1$	$x + 1$	2	$2x + 2$	$x + 2$
$2x + 1$	$2x + 1$	$x + 2$	$x + 1$	2	$2x$	$2x + 2$	$x$	1
$2x + 2$	$2x + 2$	$x + 1$	$2x + 1$	$x$	2	$x + 2$	1	$2x$

И шифр «Кузнечик», и шифр AES работают с полем из 256 элементов, но в «Кузнечике» для его построения используется неприводимый над  $\mathbb{F}_2$  многочлен  $x^8 + x^7 + x^6 + x + 1$ , а в AES – другой неприводимый над  $\mathbb{F}_2$  многочлен, а именно  $x^8 + x^4 + x^3 + x + 1$ . Эти построения приводят к изоморфным, т.е. одинаковым с точки зрения *математика* полям. Важно понимать, что с точки зрения *инженера* (реализующего соответствующие процедуры аппаратно) или *программиста* (реализующего их программно) умножения в построенных с помощью разных неприводимых многочленов полях существенно различны.

Пусть  $f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n$  – многочлен над некоторым полем, а  $x_1, x_2, \dots, x_n$  – его корни (в поле разложения), причем каждый корень взят столько раз, какова его кратность.

Тогда выполняется равенство:

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n = a_0(x - x_1)(x - x_2) \cdots (x - x_n).$$

Раскрывая скобки в его правой части и приравнявая коэффициенты при одинаковых степенях  $x$ , получаем *формулы Виета*:

$$\frac{a_1}{a_0} = -(x_1 + x_2 + \dots + x_n),$$

$$\frac{a_2}{a_0} = x_1x_2 + x_1x_3 + \dots + x_1x_n + x_2x_3 + \dots + x_{n-1}x_n,$$

$$\frac{a_3}{a_0} = -(x_1x_2x_3 + x_1x_2x_4 + \dots + x_{n-2}x_{n-1}x_n),$$

.....

$$\frac{a_{n-1}}{a_0} = (-1)^{n-1}(x_1x_2 \cdots x_{n-1} + x_1x_2 \cdots x_{n-2}x_n + \dots + x_2x_3 \cdots x_n),$$

$$\frac{a_n}{a_0} = (-1)^n x_1x_2 \cdots x_n.$$

Компактно:

$$\frac{a_k}{a_0} = (-1)^k \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}, \quad k = 1, 2, \dots, n.$$

Иначе говоря,  $(-1)^k \frac{a_k}{a_0}$  есть сумма всевозможных произведений по  $k$  корней.

Сумма всевозможных произведений по  $k$  переменных из множества  $x_1, x_2, \dots, x_n$  называется  *$k$ -й элементарной симметрической функцией* этих переменных и обозначается  $\sigma_k(x_1, x_2, \dots, x_n)$  или просто  $\sigma_k$ :

$$\sigma_k := \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}, \quad k = 1, 2, \dots, n.$$

Важное для дальнейшего следствие формул Виета звучит так:  
*с точностью до знака коэффициенты унитарного многочлена суть элементарные симметрические функции его корней.*