

Лекция: Неприводимые и приводимые многочлены. Теорема о построении полей из p^n элементов, где p – простое число, $n \geq 2$.
Вычисления в конечных полях, алгоритм Евклида. Расширения полей. Мультипликативная группа конечного поля.

Лектор - доцент Селезнева Светлана Николаевна

Лекции по “Избранным вопросам дискретной математики”.
3-й курс, группа 318,
факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте <http://mk.cs.msu.su>

Обратимые и необратимые элементы кольца

Пусть $R = (S; +, \cdot)$ – коммутативное, ассоциативное кольцо с единицей 1.

Элемент $a \in S$ называется **обратимым** (в кольце R), если в кольце R найдется обратный к нему элемент, т.е. такой элемент $b = a^{-1} \in S$, что

$$a \cdot b = 1.$$

Иначе, элемент $a \in S$ называется **необратимым** элементом (кольца R).

Пример. В кольце $R = (\mathbb{Z}, +, \cdot)$ сложения и умножения целых чисел есть только два **обратимых** элемента: 1 и -1 , остальные элементы – **необратимы**.

Простые и разложимые элементы кольца

Пусть $R = (S; +, \cdot)$ – коммутативное, ассоциативное кольцо с единицей 1.

Элемент $a \in S$ называется **простым**, или **неразложимым** (в кольце R), если он необратим в этом кольце, и в любом разложении вида

$$a = b \cdot c, \text{ где } b, c \in R,$$

или элемент b – обратим, или элемент c – обратим.

Необратимый элемент $a \in S$ называется *разложимым* (в кольце R), если найдутся такие **необратимые** элементы $b, c \in R$, что

$$a = b \cdot c.$$

Пример простых и разложимых элементов кольца

Пример. В кольце $R = (\mathbb{Z}, +, \cdot)$ сложения и умножения целых чисел элемент 3 является **простым**, т.к. он необратим, и возможны только его разложения

$$3 = 3 \cdot 1 = (-3) \cdot (-1),$$

в которых элементы 1 и -1 обратимы; а элемент 10 является **разложимым**, т.к. он необратим, и

$$10 = 2 \cdot 5,$$

и элементы 2 и 5 необратимы.

Обратимые, простые и разложимые элементы кольца многочленов над полем

Пусть \mathbb{F}_p – поле из p элементов, где p – простое число, и $\mathbb{F}_p[x]$ – кольцо многочленов над полем \mathbb{F}_p .

Обратимыми элементами кольца $\mathbb{F}_p[x]$ являются **ненулевые постоянные многочлены** (многочлены степени 0), т.е. многочлены $1, 2, \dots, p-1 \in \mathbb{F}_p[x]$.

Если многочлен $f(x)$ – **простой** элемент кольца $\mathbb{F}_p[x]$, то в любом разложении $f(x) = g(x) \cdot h(x)$ или $\deg g = 0$, или $\deg h = 0$. При этом говорят, что многочлен $g(x)$ **неприводим** в кольце $\mathbb{F}_p[x]$ (или над полем \mathbb{F}_p).

Если многочлен $f(x)$ – **разложимый** элемент кольца $\mathbb{F}_p[x]$, то найдутся такие многочлены $g(x), h(x) \in \mathbb{F}_p[x]$, что $\deg g \geq 1$, $\deg h \geq 1$, и $f(x) = g(x) \cdot h(x)$. При этом говорят, что многочлен $g(x)$ **приводим** в кольце $\mathbb{F}_p[x]$ (или над полем \mathbb{F}_p).

Неприводимые и приводимые многочлены в кольце

Пример. В кольце $\mathbb{F}_2[x]$ многочлен $f(x) = x^2 + 1$ – **приводим**, т.к.

$$x^2 + 1 = (x + 1)(x + 1), \quad \deg(x + 1) = 1,$$

а многочлен $g(x) = x^2 + x + 1$ – **неприводим**, т.к. его разложение с неопределенными коэффициентами $a, b \in \mathbb{F}_2$

$$x^2 + x + 1 = (x + a)(x + b)$$

приводит к несовместной в поле \mathbb{F}_2 системе уравнений:

$$\begin{cases} a + b = 1, \\ a \cdot b = 1. \end{cases}$$

Неприводимость и приводимость в зависимости от кольца

Неприводимость и приводимость многочлена **зависит** от того, в каком кольце (или над каким полем) мы его рассматриваем.

Пример. Многочлен $f(x) = x^2 + 1$ в кольце $\mathbb{F}_2[x]$ **приводим**, т.к.

$$x^2 + 1 = (x + 1)(x + 1), \quad \deg(x + 1) = 1,$$

а в кольце $\mathbb{F}_3[x]$ этот же многочлен **неприводим**, т.к. его разложение с неопределенными коэффициентами $a, b \in E_3$

$$x^2 + 1 = (x + a)(x + b)$$

приводит к несовместной в поле \mathbb{F}_3 системе уравнений:

$$\begin{cases} a + b = 0, \\ a \cdot b = 1. \end{cases}$$

Теорема о фактор-кольце кольца многочленов над полем

Теорема 1. Пусть $\mathbb{F}_p[x]$ – кольцо многочленов над полем \mathbb{F}_p , где p – простое число, и многочлен $g(x) \in \mathbb{F}_p[x]$. Фактор-кольцо $\mathbb{F}_p[x]/(g)$ кольца $\mathbb{F}_p[x]$ по модулю главного идеала (g) является полем тогда и только тогда, когда $g(x)$ – неприводимый многочлен в кольце $\mathbb{F}_p[x]$.

Доказательство. Пусть $\mathbb{F}_p[x]$ кольцо многочленов над полем \mathbb{F}_p , и

$$J = (g) = \{g(x)h(x) \mid h(x) \in \mathbb{F}_p[x]\}$$

его главный идеал по элементу $g(x) \in \mathbb{F}_p[x]$.

1. Если $g(x)$ – **обратимый** элемент кольца $\mathbb{F}_p[x]$, то для единицы 1 верно $1 \in J = (g)$ (**почему?**).

Откуда $J = R$ (**почему?**).

Поэтому фактор-кольцо R/J состоит из одного элемента $J = R = [0]$, и, значит, не поле.

Теорема о фактор-кольце кольца многочленов над полем

Доказательство (продолжение). 2. Пусть $g(x)$ – **приводимый** элемент кольца $\mathbb{F}_p[x]$, т.е. $g(x) = g_1(x) \cdot g_2(x)$, где $\deg g_1 < \deg g$, $\deg g_2 < \deg g$, $g_1(x), g_2(x)$ – **непостоянные** многочлены.

Докажем от противного, что для класса вычетов $[g_1]_J$ нет обратного элемента в фактор-кольце $\mathbb{F}_p[x]/J$.

Пусть для некоторого многочлена $h_1 \in \mathbb{F}_p[x]$ верно $[g_1]_J \cdot [h_1]_J = [1]_J$.

Тогда $(g_1(x) + J)(h_1(x) + J) = g_1(x)h_1(x) + J = 1 + J$. Т.е. найдется такой многочлен $h(x) \in \mathbb{F}_p[x]$, что

$$g_1(x)h_1(x) = 1 + g(x)h(x); \quad \text{или} \quad g_1(x)h_1(x) - g_1(x)g_2(x)h(x) = 1.$$

Но левая часть равенства делится на многочлен $g_1(x)$, а правая часть на него не делится. Противоречие.

Теорема о фактор-кольце кольца многочленов над полем

Доказательство (продолжение). 3. Пусть $g(x)$ – **неприводимый** элемент кольца $\mathbb{F}_p[x]$.

Докажем, что для каждого элемента $[f]_J$ фактор-кольца $\mathbb{F}_p[x]/J$, $[f]_J \neq [0]_J$, есть **обратный** элемент.

Рассмотрим множество

$$T = \{f(x)h(x) + g(x)t(x) \mid h(x), t(x) \in \mathbb{F}_p[x]\}.$$

Докажем, что оно является **идеалом** кольца $\mathbb{F}_p[x]$.

1) Множество T с операциями сложения $+$ и умножения \cdot является подкольцом кольца $\mathbb{F}_p[x]$, т.к.

$$(fh_1 + gt_1) - (fh_2 + gt_2) = f(h_1 - h_2) + g(t_1 - t_2) = fh + gt, \text{ где } h, t \in \mathbb{F}_p[x].$$

2) Если $q(x) \in \mathbb{F}_p[x]$, то

$$(fh_1 + gt_1) \cdot q = fh_1q + gt_1q = fh + gt, \text{ где } h, t \in \mathbb{F}_p[x].$$

Значит, T идеал кольца R .

Теорема о фактор-кольце кольца многочленов над полем

Доказательство (продолжение). Но $\mathbb{F}_p[x]$ – **кольцо главных идеалов**, поэтому найдется такой многочлен $g_1(x) \in \mathbb{F}_p[x]$, что $T = (g_1)$.

Заметим, что

$$g(x) = f(x) \cdot 0 + g(x) \cdot 1 \in T.$$

Поэтому, $g(x) = g_1(x) \cdot h_1(x)$ для некоторого многочлена $h_1(x) \in \mathbb{F}_p[x]$.

Но в кольце $\mathbb{F}_p[x]$ многочлен $g(x)$ **неприводимый**, поэтому или $g_1(x)$ – постоянный многочлен, или $h_1(x)$ – постоянный многочлен.

Теорема о фактор-кольце кольца многочленов над полем

Доказательство (продолжение). Рассмотрим два случая.

1. Если $h_1(x)$ – постоянный многочлен, то

$g_1(x) = g(x) \cdot h_1^{-1}(x)$. Заметим, что

$$f(x) = g(x) \cdot 0 + f(x) \cdot 1 \in T.$$

Поэтому $f(x) = g_1(x)h_2(x)$ для некоторого $h_2(x) \in \mathbb{F}_p[x]$.

Откуда

$$f(x) = g_1(x)h_2(x) = (g(x)h_1^{-1}(x)) \cdot h_2(x) = g(x)h(x),$$

где $h(x) \in \mathbb{F}_p[x]$.

Т.е. $f(x) \in (g) = J$, и $[f]_J = J = [0]_J$ – противоречие. Значит, случай 1 невозможен.

Теорема о фактор-кольце кольца многочленов над полем

Доказательство (продолжение).

2. Если $g_1(x)$ – постоянный многочлен, то для единицы 1 верно $1 \in T$ (почему?).

Т.е. найдутся такие многочлены $h(x), t(x) \in \mathbb{F}_p[x]$, что

$$g(x)h(x) + f(x)t(x) = 1.$$

Т.е. $([f]_J)^{-1} = [t]_J$, т.к.

$$[f]_J \cdot [t]_J = [f \cdot t]_J = [1 - g \cdot h]_J = [1]_J \text{ (почему?).}$$

□

Конечные поля из p^n элементов

Пусть $g(x)$ – неприводимый в кольце $\mathbb{F}_p[x]$ многочлен, где \mathbb{F}_p – поле из p элементов.

Тогда по теореме 1 фактор-кольцо $\mathbb{F}_p[x]/(g)$ является **полем**.

Элементы этого поля – классы вычетов $[f]_{(g)}$, $f(x) \in \mathbb{F}_p[x]$, по модулю идеала (g) , т.е.

$$[f]_{(g)} = \{f(x) + g(x) \cdot h(x) \mid h(x) \in \mathbb{F}_p[x]\}.$$

В каком случае два многочлена $f_1(x), f_2(x) \in \mathbb{F}_p[x]$ **принадлежат одному классу вычетов** $[f]_{(g)}$? В том и только в том случае, когда у них **одинаковые** остатки при делении на многочлен $g(x)$.

Следовательно, элементов в поле $\mathbb{F}_p[x]/(g)$ столько, сколько **различных остатков** при делении на многочлен $g(x)$.

Конечные поля из p^n элементов

Пусть $\deg g = n$, т.е.

$$g(x) = \sum_{i=0}^n a_i x^i, \quad a_n \neq 0.$$

Тогда каждый остаток $r(x)$ при делении на $g(x)$ будет иметь вид:

$$r(x) = \sum_{j=0}^{n-1} b_j x^j,$$

где b_0, b_1, \dots, b_{n-1} – какие-то элементы поля \mathbb{F}_p .

Когда коэффициенты $b_0, b_1, \dots, b_{n-1} \in \mathbb{F}_p$ пробегают **все** свои возможные значения, мы получаем **все** возможные остатки при делении на многочлен $g(x)$.

Возможных остатков всего p^n . А значит, **p^n элементов в поле $\mathbb{F}_p[x]/(g)$.**

Конечные поля из p^n элементов

Поле $\mathbb{F}_p[x]/(g)$ состоит из p^n элементов вида

$$[r] = [r]_{(g)} = \{r(x) + g(x) \cdot h(x) \mid h(x) \in \mathbb{F}_p[x]\},$$

где $r(x)$ – многочлен степени, не превосходящей $n - 1$, из кольца $\mathbb{F}_p[x]$.

Операции сложения и умножения в поле $\mathbb{F}_p[x]/(g)$:

$$[r_1] + [r_2] = [r_1 + r_2],$$

$$[r_1] \cdot [r_2] = [r_1 \cdot r_2],$$

с возможным приведением по модулю многочлена $g(x)$.

Для каждого простого числа p существует конечное поле из p элементов. Поэтому если найдется неприводимый над этим полем многочлен степени n , **можно построить** конечное поле из p^n элементов.

Построение поля из 4-х элементов

Пример. Построим поле из $4 = 2^2$ элементов.

В кольце $\mathbb{F}_2[x]$ многочлен $g(x) = x^2 + x + 1$ – **неприводим**.

Элементами поля $\mathbb{F}_2[x]/(g)$ будут классы вычетов:

$$[0] = 0, [1] = 1, [x] = a, [x + 1] = b,$$

где $[0] = 0$ – нулевой и $[1] = 1$ – единичный элементы.

Таблицы для операций сложения и умножения в поле $\mathbb{F}_2[x]/(g)$:

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Например:

$$a + b = [x] + [x + 1] = [x + x + 1] = [1] = 1,$$

$$a \cdot b = [x] \cdot [x + 1] = [x(x + 1)] = [x^2 + x] = [g(x) + 1] = [1] = 1.$$

Вычисления в конечных полях

Рассмотрим поле $F = \mathbb{F}_p[x]/(g)$ из p^n элементов, где $g(x) \in \mathbb{F}_p[x]$ – неприводимый многочлен над полем \mathbb{F}_p .

Операции сложения $+$ и умножения \cdot в поле F конструктивно определены.

Т.к. F – поле, для каждого ненулевого элемента $a \in F$ найдется **обратный к нему** элемент $a^{-1} \in F$.

Но как его находить?

Один из вариантов: умножать элемент a на все элементы поля F , пока в произведении не получим 1.

Но есть более эффективный метод.

Наибольший общий делитель многочленов

Пусть $F[x]$ – кольцо многочленов над полем F , и $f_1(x), f_2(x) \in F[x]$.

Многочлен $f(x) \in F[x]$ называется **нормированным**, если его старший коэффициент равен 1.

Нормированный многочлен $g(x) \in F[x]$ называется **наибольшим общим делителем** многочленов $f_1(x)$ и $f_2(x)$, если

- 1) многочлены $f_1(x)$ и $f_2(x)$ **делятся** на многочлен $g(x)$;
- 2) многочлен $g(x)$ **делится** на каждый многочлен, на который делятся **одновременно** многочлены $f_1(x)$ и $f_2(x)$.

Наибольший общий делитель многочленов $f_1(x)$ и $f_2(x)$ будем обозначать $\text{НОД}(f_1, f_2)$.

Алгоритм Евклида

Теорема 2 (алгоритм Евклида). Пусть $F[x]$ – кольцо многочленов над полем F , $f_1(x), f_2(x) \in F[x]$ – ненулевые многочлены, и

$$f_1(x) = f_2(x)q_1(x) + r_1(x), \quad \deg r_1 < \deg f_2;$$

$$f_2(x) = r_1(x)q_2(x) + r_2(x), \quad \deg r_2 < \deg r_1;$$

$$r_1(x) = r_2(x)q_3(x) + r_3(x), \quad \deg r_3 < \deg r_2;$$

...

$$r_{s-2}(x) = r_{s-1}(x)q_s(x) + r_s(x), \quad \deg r_s < \deg r_{s-1};$$

$$r_{s-1}(x) = r_s(x)q_{s+1}(x).$$

Тогда если $a \in F$ – старший коэффициент многочлена $r_s(x)$, то $\text{НОД}(f_1, f_2) = a^{-1}r_s(x)$.

Алгоритм Евклида

Доказательство. Пусть

$$f_1(x) = f_2(x)q_1(x) + r_1(x), \quad \deg r_1 < \deg f_2;$$

$$f_2(x) = r_1(x)q_2(x) + r_2(x), \quad \deg r_2 < \deg r_1;$$

$$r_1(x) = r_2(x)q_3(x) + r_3(x), \quad \deg r_3 < \deg r_2;$$

...;

$$r_{s-2}(x) = r_{s-1}(x)q_s(x) + r_s(x), \quad \deg r_s < \deg r_{s-1};$$

$$r_{s-1}(x) = r_s(x)q_{s+1}(x).$$

1) Просматривая равенства „снизу вверх“ получаем, что на многочлен $r_s(x)$ делятся многочлены $f_1(x)$ и $f_2(x)$.

2) Если на многочлен $h(x)$ одновременно делятся многочлены $f_1(x)$ и $f_2(x)$, то, просматривая равенства „сверху вниз“, получаем, что на многочлен $h(x)$ делится и многочлен $r_s(x)$.

Значит, $\text{НОД}(f_1, f_2) = a^{-1}r_s(x)$.

Пример применения алгоритма Евклида

Пример. По алгоритму Евклида найдем наибольший общий делитель многочленов $f_1(x) = x^4 + x$ и $f_2(x) = x^2 + 1$ из кольца $\mathbb{F}_2[x]$.

Тогда

$$\begin{aligned}x^4 + x &= (x^2 + 1)(x^2 + 1) + (x + 1); \\x^2 + 1 &= (x + 1)(x + 1) + 0.\end{aligned}$$

Откуда, $\text{НОД}(x^4 + x, x^2 + 1) = x + 1$.

Применение алгоритма Евклида

Пусть $g(x)$ – неприводимый многочлен над полем F .

Тогда для каждого ненулевого многочлена $r(x) \in F[x]$,
 $\deg r < \deg g$, верно $\text{НОД}(g, r) = 1$.

По алгоритму Евклида можно находить **обратный** к элементу $[r]$ элемент $([r])^{-1}$ в поле $F[x]/(g)$.

Нахождение обратного элемента

Пусть

$$\begin{aligned}g(x) &= r(x)q_1(x) + r_1(x), \deg r_1 < \deg r; \\r(x) &= r_1(x)q_2(x) + r_2(x), \deg r_2 < \deg r_1; \\&\dots; \\r_{s-2}(x) &= r_{s-1}(x)q_s(x) + a, a \in F, a \neq 0.\end{aligned}$$

Тогда

$$\begin{aligned}r_1(x) &= g(x) - r(x)q_1(x) = r(x)h'_1(x) + g(x)h''_1(x); \\r_2(x) &= r(x) - r_1(x)q_2(x) = r(x)h'_2(x) + g(x)h''_2(x); \\&\dots; \\a &= r_{s-2}(x) - r_{s-1}(x)q_s(x) = r(x)h'_s(x) + g(x)h''_s(x),\end{aligned}$$

где многочлены $h'_i(x), h''_i(x) \in F[x]$, $i = 1, \dots, s$.

Откуда $([r])^{-1} = [a^{-1}h'_s]$ (почему?).

Пример нахождения обратного элемента

Пример. Найдем в поле $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ обратный элемент к элементу $[x^2 + 1]$.

Обозначим: $g(x) = x^3 + x^2 + 1$, $r(x) = x^2 + 1$.

Тогда

$$\begin{aligned}x^3 + x^2 + 1 &= (x^2 + 1)(x + 1) + x; \\x &= r(x)(-x - 1) + g(x).\end{aligned}$$

Далее

$$\begin{aligned}x^2 + 1 &= x \cdot x + 1; \\1 &= r(x) - x \cdot x = r(x) - (r(x)(-x - 1) + g(x))x = \\&= r(x)(1 + x^2 + x) - g(x)x.\end{aligned}$$

Откуда

$$([x^2 + 1])^{-1} = [x^2 + x + 1].$$

Несложно проверить, что

$$(x^2 + 1)(x^2 + x + 1) = x^4 + x^3 + x + 1 = (x^3 + x^2 + 1)x + 1.$$

Корень многочлена

Пусть $R[x]$ – кольцо многочленов над кольцом R , многочлен $f(x) \in R[x]$,

$$f(x) = \sum_{i=0}^n a_i x^i,$$

и элемент $c \in R$.

Значением многочлена $f(x)$ в точке c называется элемент

$$f(c) = \sum_{i=0}^n a_i c^i \in R.$$

Если $f(c) = 0$, то элемент c называется *корнем* многочлена $f(x)$.

Корень многочлена

Теорема 3. Пусть $F[x]$ – кольцо многочленов над полем F .
Элемент $c \in R$ является корнем многочлена $f(x) \in F[x]$ тогда и только тогда, когда многочлен $f(x)$ делится на многочлен $x - c$.

Доказательство. Поделим с остатком многочлен $f(x)$ на многочлен $x - c$:

$$f(x) = (x - c)q(x) + r(x), \quad \deg r < 1.$$

Т.к. степень многочлена $r(x) \in F[x]$ меньше 1, он является постоянным многочленом: $r(x) = b \in F$.

\Rightarrow . Если c – корень многочлена $f(x)$, то

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

\Leftarrow . Если многочлен $f(x)$ делится на многочлен $x - c$, то $b = 0$.
Откуда $f(c) = 0$.

Неприводимые многочлены степени 2 и 3

Теорема 4 (критерий неприводимости многочленов степени 2 и 3). Пусть $F[x]$ – кольцо многочленов над полем F . Многочлен $f(x) \in F[x]$ степени 2 или 3 неприводим над полем F тогда и только тогда, когда у него нет корней в поле F .
Доказательство. Рассмотрим разложение

$$f(x) = g(x) \cdot h(x),$$

где $g(x), h(x) \in F[x]$, $\deg g \geq 1$, $\deg h \geq 1$.

Т.к. степень многочлена $f(x)$ равна 2 или 3, или $\deg g = 1$, или $\deg h = 1$.

Откуда многочлен $f(x)$ **неприводим** над полем F тогда и только тогда когда у него нет корней в этом поле.



Пример неприводимого многочлена степени 2

Пример. Многочлен $f(x) = x^2 + 2x + 2 \in \mathbb{F}_3[x]$ неприводим над полем \mathbb{F}_3 , т.к.

c	$f(c)$
0	2
1	2
2	1

Т.е. многочлен $f(x)$ не имеет корней в поле \mathbb{F}_3 , и, значит, он **неприводим** над этим полем.

Число неприводимых многочленов над полем

Теорема 5. Число $M_p(n)$ неприводимых нормированных многочленов степени n над полем \mathbb{F}_p вычисляется по формуле

$$M_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}},$$

где запись „ $d \mid n$ “ означает „число d является делителем числа n “, а $\mu(n)$ – функция Мебиуса,

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1; \\ (-1)^k, & \text{если } n \text{ – произведение } k \text{ различных} \\ & \text{простых чисел;} \\ 0, & \text{если } n \text{ делится на квадрат простого числа.} \end{cases}$$

Число неприводимых многочленов над полем \mathbb{F}_2

Примеры. Рассмотрим \mathbb{F}_2 .

1. Если $n = 2$, то

$$M_2(2) = \frac{1}{2} \sum_{d|2} \mu(d) 2^{\frac{2}{d}} = \frac{1}{2} (2^2 - 2) = 1.$$

Т.е. существует только **один** неприводимый многочлен степени 2 над полем \mathbb{F}_2 : $f(x) = x^2 + x + 1$.

2. Если $n = 3$, то

$$M_2(3) = \frac{1}{3} \sum_{d|3} \mu(d) 2^{\frac{3}{d}} = \frac{1}{3} (2^3 - 2) = 2.$$

Т.е. найдется **два** неприводимых многочленов степени 3 над полем \mathbb{F}_2 : $f_1(x) = x^3 + x^2 + 1$ и $f_2(x) = x^3 + x + 1$.

Число неприводимых многочленов над полем

Следствие 5.1. Для каждого простого числа p для каждого натурального числа $n \geq 2$ в кольце многочленов $\mathbb{F}_p[x]$ над полем \mathbb{F}_p найдется хотя бы один неприводимый нормированный многочлен над этим полем.

Доказательство. По теореме 5

$$M_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

Заметим, что $\mu(1) = 1$, и $\mu(d) \geq -1$, если $d \geq 2$.

Тогда

$$\begin{aligned} M_p(n) &\geq \frac{1}{n} (p^n - p^{n-1} - \dots - p) = \frac{1}{n} \left(p^n - \frac{p^n - p}{p - 1} \right) = \\ &= \frac{1}{n} \cdot \frac{p}{p - 1} \cdot (p^n - 2p^{n-1} + 1) > 0, \end{aligned}$$

если $p \geq 2$.

Существование полей из p^n элементов

Следствие 5.2. *Для каждого простого числа p для каждого натурального числа $n \geq 2$ существует конечное поле из p^n элементов.*

Доказательство. По следствию 5.1 найдется неприводимый (нормированный) многочлен $g(x) \in \mathbb{F}_p[x]$ степени n над полем \mathbb{F}_p .

По теореме 1 фактор-кольцо $\mathbb{F}_p[x]/(g)$ кольца $\mathbb{F}_p[x]$ по модулю главного идеала по неприводимому в этом кольце многочлену $g(x)$ является полем из p^n элементов.

□

Расширения полей

Рассмотрим поле $F = \mathbb{F}_p[x]/(g)$ из p^n элементов, где $g(x) \in \mathbb{F}_p[x]$ – неприводимый многочлен над полем \mathbb{F}_p .

Т.к. многочлен $g(x)$ **неприводим** над полем \mathbb{F}_p , у него **нет корней в поле \mathbb{F}_p** .

Пусть

$$g(x) = \sum_{i=0}^n a_i x^i.$$

Тогда для элемента $[x] \in F$ верно

$$g([x]) = \sum_{i=0}^n a_i ([x])^i = \left[\sum_{i=0}^n a_i x^i \right] = [g] = [0]$$

Т.е. элемент $\theta = [x] \in F$ – **корень** многочлена $g(x)$ в поле F .

Расширения полей

Говорят, что поле $F = \mathbb{F}_p[x]/(g)$ является **простым алгебраическим расширением** поля \mathbb{F}_p , что оно получено из поля \mathbb{F}_p **присоединением корня** θ неприводимого над полем \mathbb{F}_p многочлена $g(x)$ и обозначают $F = \mathbb{F}_p(\theta)$.

Тогда все элементы поля $F = \mathbb{F}_p(\theta)$ имеют вид

$$b_{n-1}\theta^{n-1} + \dots + b_1\theta + b_0,$$

где коэффициенты b_{n-1}, \dots, b_1, b_0 **пробегают все возможные значения** из поля \mathbb{F}_p .

Значит, каждый элемент поля F можно задавать **вектором** из n элементов из поля \mathbb{F}_p :

$$(b_{n-1}, \dots, b_1, b_0), \quad b_{n-1}, \dots, b_1, b_0 \in \mathbb{F}_p.$$

При такой записи операция сложения элементов поля F – это операция **покоординатного сложения** задающих их векторов.

Расширения полей

Т.е. поле $F = \mathbb{F}_p(\theta)$ можно рассматривать как **линейное пространство** над полем \mathbb{F}_p .

В разных случаях бывает удобной та или иная форма записи элементов поля из p^n элементов.

Мультипликативная группа конечного поля

Пусть $F = (S; +, \cdot)$ – конечное поле.

По определению поля множество $S \setminus \{0\}$ с операцией умножения \cdot является абелевой группой.

Эта группа называется **мультипликативной группой поля F** и обозначается F^* ,

$$F^* = (S \setminus \{0\}; \cdot).$$

Пример. В поле $\mathbb{F}_3 = (\mathbb{Z}_3; + \pmod{3}, \cdot \pmod{3})$ – мультипликативная группа

$$\mathbb{F}_3^* = (\{1, 2\}, \cdot \pmod{3}),$$

в которой единица 1, и

$$1 \cdot x = x, \quad x = 1, 2;$$

$$2 \cdot 2 = 1.$$

Теорема о мультипликативной группе конечного поля

Теорема 6. *Мультипликативная группа F^* конечного поля F является циклической группой.*

Образующий элемент циклической мультипликативной группы F^* конечного поля F называется **примитивным элементом** поля F и обозначается e .

Примитивный элемент поля \mathbb{F}_5

Примеры.

1. Найдем примитивный элемент поля $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$.

Заметим, что $e = 2$ – примитивный элемент поля \mathbb{F}_5 , и $e = 3$ – примитивный элемент поля \mathbb{F}_5 :

x	x^2	x^3	x^4
0	0	0	0
1	1	1	1
2	4	3	1
3	4	2	1
4	1	4	1

Примитивный элемент поля из 4-х элементов

Примеры.

2. Найдем примитивный элемент поля

$$\mathbb{F}_4 = \mathbb{F}_{2^2} = \mathbb{F}_2[x]/(x^2 + x + 1) = \{0, 1, \theta, \theta + 1\}.$$

Заметим, что $e = \theta$ – примитивный элемент поля \mathbb{F}_4 , и

$e = \theta + 1$ – примитивный элемент поля \mathbb{F}_4 :

x	x^2	x^3
0	0	0
1	1	1
θ	$\theta + 1$	1
$\theta + 1$	θ	1

Задачи для самостоятельного решения

1. Является ли многочлен $f(x)$ неприводимым над полем F , если

1) $f(x) = x^3 + x^2 + 1, F = \mathbb{F}_2$;

2) $f(x) = x^3 + 2x^2 + 2, F = \mathbb{F}_3$;

3) $f(x) = x^4 + x^2 + 1, F = \mathbb{F}_2$;

4) $f(x) = 3x^4 + 2, F = \mathbb{F}_5$.

2. Является ли фактор-кольцо $F[x]/(f)$ полем, если

1) $F = \mathbb{F}_3, f(x) = x^3 + 2x + 2$;

2) $F = \mathbb{F}_5, f(x) = x^4 + 3$?

При положительном ответе дополнительно выяснить, сколько элементов содержит это поле.

Задачи для самостоятельного решения

3. Найти таблицы сложения, умножения и обратные элементы (если они существуют) для элементов $[g_1], [g_2]$ в фактор-кольце $F[x]/(f)$, если

1) $f(x) = x^3 + x + 1, F = \mathbb{F}_2, g_1(x) = x^2 + 1, g_2(x) = x + 1;$

2) $f(x) = x^3 + x^2 - 1, F = \mathbb{F}_3, g_1(x) = x^2 + 2x + 2,$

$g_2(x) = x^2 + 1.$

4. Найти примитивный элемент

1) простого поля $F = \mathbb{F}_7;$

2) простого поля $F = \mathbb{F}_{13}.$

Литература к лекции

1. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988.

Конец лекции