Лекция 11. Число неприводимых многочленов над простым полем. Расширения полей. Существование и единственность конечного поля с p^n элементами, где p — простое число, $n \geqslant 1$.

Лектор — Селезнева Светлана Николаевна
selezn@cs.msu.ru

Факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Свойство коммутативного и ассоциативного кольца

Утверждение 1 [формула бинома]. *Если K — коммутативное и ассоциативное кольцо, то для всех $a, b \in K$ и целых $n \geqslant 1$ верно*

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k},$$

где $C_n^k = \frac{n!}{k!(n-k)!}$ — биномиальный коэффициент.

Доказательство. Запишем равенство

$$(a+b)^n = \underbrace{(a+b)(a+b)\ldots(a+b)}_{n}.$$

Пользуясь коммутативностью и ассоциативностью кольца K, получаем, что при перемножении скобок слагаемое $a^k \cdot b^{n-k}$ появится C_n^k раз, $0 \leqslant k \leqslant n$. □

Свойство кольца характеристики p

Утверждение 2. *Если K — коммутативное и ассоциативное кольцо простой характеристики p, то*

$$(a+b)^{p^m} = a^{p^m} + b^{p^m},\ (a-b)^{p^m} = a^{p^m} - b^{p^m}$$

для всех $a, b \in K$ и целых $m \geqslant 1$.

Доказательство. Запишем равенство

$$(a+b)^p = \sum_{k=0}^{p} C_p^k a^k b^{p-k},$$

где C_p^k — биномиальный коэффициент. Но

$$C_p^k = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-k+1)}{1 \cdot 2 \cdot \ldots \cdot k}.$$

Число p — простое, значит, $C_p^k = 0 (\mathrm{mod}\ p)$ при $1 \leqslant k \leqslant p-1$. Поэтому $(a+b)^p = a^p + b^p$. Равенство $(a-b)^p = a^p - b^p$ доказывается, если подставить вместо b элемент $(-b)$.

Свойство кольца характеристики p

Для произвольного $m \geqslant 1$ равенства доказываются по индукции.

$\square$

Свойство кольца характеристики p

Утверждение 3. *Если $f(x) \in \mathbb{Z}_p[x]$, где p — простое число, то при целых $m \geqslant 1$ верно равенство*

$$(f(x))^{p^m} = f(x^{p^m}).$$

Доказательство. В самом деле, пусть $f(x) = \sum\limits_{i=0}^{n} a_i x^i$, где $a_0, a_1, \ldots, a_n \in \mathbb{Z}_p$. Тогда, с учетом утверждения 2, получаем

$$(f(x))^{p^m} = \left(\sum_{i=0}^{n} a_i x^i\right)^{p^m} = \sum_{i=0}^{n} a_i^{p^m} x^{ip^m}.$$

Но $a^{p^m} = a$ при $a \in \mathbb{Z}_p$. Поэтому

$$(f(x))^{p^m} = \sum_{i=0}^{n} a_i \left(x^{p^m}\right)^i = f(x^{p^m}).$$

Произведение неприводимых многочленов

Пусть $N_p(n)$ — множество неприводимых нормированных многочленов степени n над полем $\mathbb{Z}_p$.

Теорема 1. *Если p — простое число, $n \geqslant 1$, то произведение всех неприводимых нормированных многочленов над полем $\mathbb{Z}_p$, степени которых являются делителями числа n, равно $x^{p^n} - x$, т. е.*

$$x^{p^n} - x = \prod_{m|n} \prod_{g \in N_p(m)} g(x).$$

Произведение неприводимых многочленов

Доказательство. Пусть $g(x) \in N_p(m)$.
1. Покажем, что многочлен $x^{p^n} - x$ делится на многочлен $g(x)$, если n делится на m, и не делится на него, если n не делится на m.

Т. к. $g(x)$ — неприводимый многочлен степени m, кольцо $\mathbb{Z}_p[x]/(g)$ является полем из p^m элементов. В этом поле для любого элемента $h(x)$, $h(x) \neq 0$, верно

$$h^{p^m-1} = 1 (\mathrm{mod}\ g).$$

Значит, для $h(x) = x$ получаем:

$$x^{p^m} = x (\mathrm{mod}\ g).$$

Произведение неприводимых многочленов

Пусть $n = mk + r$ для некоторых целых k, r, где $0 \leqslant r \leqslant m - 1$.

а) Если n делится на m, то $r = 0$. Поэтому

$$x^{p^n} = x^{p^{mk}} = x (\mathrm{mod}\ g).$$

Другими словами, многочлен $x^{p^n} - x$ делится на многочлен $g(x)$.

Произведение неприводимых многочленов

б) Если n не делится на m, т. е. $1 \leqslant r \leqslant m-1$, то

$$x^{p^n} = x^{p^{mk+r}} = x^{p^r} (\mathrm{mod}\ g).$$

Если предположить, что многочлен $x^{p^n} - x$ делится на многочлен $g(x)$, то верно

$$x^{p^r} = x (\mathrm{mod}\ g).$$

Для любого многочлена $h(x) \in \mathbb{Z}_p[x]/(g)$ по утверждению 3 получаем:

$$(h(x))^{p^r} = h(x^{p^r}) = h(x) (\mathrm{mod}\ g).$$

Т. е. порядок по умножению любого ненулевого элемента $h(x)$ поля $\mathbb{Z}_p[x]/(g)$ не превосходит $p^r - 1$, чего не может быть, т. к. $r < m$, а в поле $\mathbb{Z}_p[x]/(g)$ найдется примитивный элемент, порядок которого равен $p^m - 1$.

Произведение неприводимых многочленов

2. Покажем, что многочлен $x^{p^n} - x$ не делится на многочлен $(g(x))^2$. Предположим обратное: пусть

$$x^{p^n} - x = g^2(x) \cdot h(x)$$

для некоторого многочлена $h(x) \in \mathbb{Z}_p[x]$.
Тогда рассмотрим формальную производную многочленов левой и правой частей:

$$(x^{p^n} - x)' = -1,$$

Т. к. характеристика поля $\mathbb{Z}_p$ равна p. Но

$$(g^2(x) \cdot h(x))' = g(x)(2g'(x)h(x) + g(x)h'(x)).$$

Второе выражение делится на многочлен $g(x)$ или равно 0 (если $2g'(x)h(x) + g(x)h'(x) = 0$). В любом случае, оно не может быть равным (-1), чему равно первое выражение.

Неприводимые многочлены степени, кратной 3

Пример. Рассмотрим неприводимые над полем $\mathbb{Z}_2$ многочлены из кольца $\mathbb{Z}_2[x]$ степени m, кратной $n = 3$:

$$\begin{array}{lll} m = 1: & f_1(x) = x, & f_2(x) = x + 1, \\ m = 3: & f_3(x) = x^3 + x + 1, & f_4(x) = x^3 + x^2 + 1. \end{array}$$

Получаем произведение:

$$\begin{aligned} f_1(x) \cdot f_2(x) \cdot f_3(x) \cdot f_4(x) &= x(x+1)(x^3+x+1)(x^3+x^2+1) = \\ &= (x^4+x^3+x)(x^4+x^3+x^2+1) = \\ &= x^8 + x = x^{2^3} + x. \end{aligned}$$

Произведение неприводимых многочленов

Следствие 1.1. *Если p — простое число, $n \geqslant 1$, $M_p(n)$ — число неприводимых нормированных многочленов степени n над полем $\mathbb{Z}_p$, то*

$$p^n = \sum_{m|n} mM_p(m).$$

Действительно, приравняем степени многочленов в левой и правой частях формулы из теоремы 1.

Формула обращения Мёбиуса

Теорема 2 (формула обращения Мёбиуса). *Если $F(n)$, $G(n)$ — функции, определенные на множестве натуральных чисел, и при каждом натуральном n верно*

$$F(n) = \sum_{m|n} G(m),$$

то при каждом натуральном n также верно

$$G(n) = \sum_{k|n} \mu(k) F(n/k),$$

где $\mu(n)$ — функция Мебиуса,

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

Вспомогательная лемма

Лемма 1 (свойство функции Мёбиуса). *Если $n \geqslant 1$, то*

$$\sum_{m|n} \mu(m) = \begin{cases} 1, & n = 1; \\ 0, & n \geqslant 2. \end{cases}$$

Доказательство леммы. Если $n = 1$, то равенство верно.
Пусть теперь $n \geqslant 2$ и $p_1, \ldots, p_s$ — все простые делители числа n, $s \geqslant 1$.
Тогда $\mu(m) \neq 0$, если только $m = p_{i_1} \cdot \ldots \cdot p_{i_t}$, $0 \leqslant t \leqslant s$.
Способов выбрать t делителей из s найдется ровно C_s^t. Значит,

$$\sum_{m|n} \mu(m) = \sum_{t=0}^{s} (-1)^t C_s^t = 0.$$

□

Формула обращения Мёбиуса

Доказательство теоремы (продолжение). С учетом леммы 1 получаем:

$$\begin{aligned}
\sum_{k|n} \mu(k) F(n/k) &= \sum_{k|n} \mu(k) \sum_{m|(n/k)} G(m) = \\
&= \sum_{m|n} G(m) \sum_{k:k|n, m|(n/k)} \mu(k) = \\
&= \sum_{m|n} G(m) \sum_{k:k|n, k|(n/m)} \mu(k) = \\
&= G(n) + \sum_{m \neq n, m|n} G(m) \sum_{k:k|(n/m)} \mu(k) = \\
&= G(n).
\end{aligned}$$

□

Число неприводимых многочленов над полем

Теорема 3. *Если p — простое число, $n \geqslant 1$, $M_p(n)$ — число неприводимых нормированных многочленов степени n над полем $\mathbb{Z}_p$, то*

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

Доказательство. В следствии 1.1 получено равенство

$$p^n = \sum_{m|n} m M_p(m).$$

Применим формулу обращения Мебиуса для функций $F(n) = p^n$ и $G(n) = nM_p(n)$. Получим утверждение теоремы.

□

Неприводимые многочлены степени 2 над полем $\mathbb{Z}_2$

Пример. Рассмотрим поле $\mathbb{Z}_2$ и пусть $n = 2$.
Тогда

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

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

Неприводимые многочлены степени 3 над полем $\mathbb{Z}_2$

Пример. Рассмотрим поле $\mathbb{Z}_2$ и пусть $n = 3$.
Тогда

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

Т. е. найдутся два неприводимых многочлена степени 3 над полем $\mathbb{Z}_2$: $f_1(x) = x^3 + x^2 + 1$ и $f_2(x) = x^3 + x + 1$.

Существование неприводимого многочлена над полем

Следствие 3.1. *Для каждого простого числа p для каждого целого числа $n \geqslant 2$ в кольце многочленов $\mathbb{Z}_p[x]$ найдется хотя бы один неприводимый нормированный многочлен*.

Действительно, по теореме 3

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

Заметим, что $\mu(1) = 1$ и $\mu(m) \geqslant -1$ при $m \geqslant 2$.

Тогда при $p \geqslant 2$ верно:

$$M_p(n) \geqslant \frac{1}{n}(p^n - p^{n-1} - \ldots - p) = \frac{1}{n}\left(p^n - \frac{p^n - p}{p-1}\right) =$$

$$= \frac{1}{n} \cdot \frac{p}{p-1} \cdot \left(p^n - 2p^{n-1} + 1\right) > 0.$$

Т. к. $M_p(n)$ — целое число, получаем $M_p(n) \geqslant 1$.

Существование поля из p^n элементов

Теорема 4. *Для каждого простого числа p для каждого целого числа $n \geqslant 2$ существует конечное поле из p^n элементов*.

Доказательство.
По следствию 3.1 найдется хотя бы один неприводимый многочлен $f(x) \in \mathbb{Z}_p[x]$ степени n.
Кольцо $\mathbb{Z}_p[x]/(f)$ является полем из p^n элементов.

□

Расширение поля

Если поле F содержит *подполе* K, то говорят, что поле F является **расширением** поля K.

Линейное пространство

Если поле F является расширением поля K, то поле F можно рассматривать как **линейное пространство** над полем K.

1. Сложение элементов поля F — коммутативная группа.

2. Умножение элемента поля F (вектора) на элемент поля K (на скаляр): для любых $a \in F$, $\alpha, \beta \in K$ верно

а) $(\alpha\beta) \cdot a = \alpha \cdot (\beta a)$;
б) $1 \cdot a = a$.

3. Дистрибутивность операций: для любых $a, b \in F$, $\alpha, \beta \in K$ верно

а) $\alpha \cdot (a + b) = \alpha \cdot a + \alpha \cdot b$;
б) $(\alpha + \beta) \cdot a = \alpha \cdot a + \beta \cdot a$.

Размерность линейного пространства

Если поле F конечно и является расширением поля K, то поле F как линейное пространство над полем K имеет конечную размерность n.

Значит, каждый элемент $a \in F$ можно задавать вектором $(a_1, \ldots, a_n) \in K^n$.

При этом, если $a, b \in F$, $a = (a_1, \ldots, a_n) \in K^n$, $b = (b_1, \ldots, b_n) \in K^n$, то

$$a + b = (a_1 + b_1, \ldots, a_n + b_n) \in K^n.$$

Поле из 4-х элементов

Пример. Рассмотрим поле из 4-х элементов $F = \mathbb{Z}_2[x]/(x^2 + x + 1)$ как линейное пространство над полем $K = \mathbb{Z}_2$.

Тогда

$$0 = (0,0), \quad 1 = (0,1), \quad x = (1,0), \quad x + 1 = (1,1).$$

Базисом этого линейного пространства являются элементы $1, x \in F$.

Разложение на сомножители

Утверждение 4. *Если F — поле из p^n элементов, где p — простое число, $n \geqslant 1$, то*

$$x^{p^n} - x = \prod_{a \in F} (x - a).$$

Доказательство. Ясно, что $0^{p^n} = 0$. Если $a \in F$, $a \neq 0$, то $a^{p^n - 1} = 1$ по свойству мультипликативной группы поля F, откуда $a^{p^n} = a$.

□

Корни неприводимых многочленов

Теорема 5 (о корнях неприводимых многочленов). *Пусть p — простое число, $n \geqslant 1$ и поле F — расширение поля $\mathbb{Z}_p$, содержащее p^n элементов. Тогда*

1) *каждый неприводимый над полем $\mathbb{Z}_p[x]$ многочлен $f(x) \in \mathbb{Z}_p[x]$ степени m, где m — делитель n, в поле F имеет ровно m различных корней;*

2) *каждый элемент $\theta \in F$ является корнем некоторого неприводимого над полем $\mathbb{Z}_p$ нормированного многочлена $f(x) \in \mathbb{Z}_p[x]$ степени m, где m — делитель n, и не является корнем никакого другого неприводимого нормированного многочлена степени k, где $k \leqslant n$.*

Корни неприводимых многочленов

Доказательство. Напомним, что $N_p(n)$ — множество неприводимых нормированных многочленов из $\mathbb{Z}_p$ степени n. По теореме 1

$$x^{p^n} - x = \prod_{m|n} \prod_{g \in N_p(m)} g(x).$$

По утверждению 4

$$x^{p^n} - x = \prod_{a \in F} (x - a).$$

Корни неприводимых многочленов

Значит, в поле F верно равенство

$$\prod_{m|n} \prod_{g \in N_p(m)} g(x) = \prod_{a \in F} (x - a).$$

Из однозначности разложения многочлена в произведение неприводимых многочленов в поле получаем, что в поле F каждый неприводимый многочлен $f(x) \in N_p(m)$, где m — делитель n, имеет ровно m различных корней.
При этом корни различных таких многочленов не пересекаются.

Корни неприводимых многочленов

Осталось доказать п. 2) для многочленов степени k, не являющейся делителем n.

Покажем это от противного. Пусть $h(x) \in \mathbb{Z}_p[x]$ — неприводимый нормированный многочлен степени k, для которого θ — корень. При этом k не является делителем n.

Выберем среди всех таких многочленов многочлен с наименьшей степенью. При таком выборе $k < m$ (т. к. иначе можно поделить с остатком многочлен $h(x)$ на многочлен $f(x)$ и для полученного ненулевого остатка $r(x)$ элемент θ — также корень).

Тогда элементы $1, \theta, \theta^2, \ldots, \theta^{k-1}$ — линейно независимы над полем $\mathbb{Z}_p$. Действительно, иначе θ являлся бы корнем некоторого ненулевого многочлена степени, меньшей k, чего не может быть по выбору k.

Корни неприводимых многочленов

Рассмотрим поле $F' = \mathbb{Z}_p[\theta]/(h)$ для многочлена $h(\theta)$. Все элементы поля F' имеют вид

$$b_0 + b_1\theta + \ldots + b_{k-1}\theta^{k-1},\ \ b_0, b_1, \ldots, b_{k-1} \in \mathbb{Z}_p.$$

Значит, поле F' можно считать подполем поля F.

Следовательно, поле F можно рассмотреть как линейное пространство над полем F'. Но тогда для размерности s этого линейного пространства должно выполняться $(p^k)^s = p^n$, чего не может быть, т. к. k не является делителем n.

□

Корни в поле из 8 элементов

Пример. Рассмотрим поле $F = \mathbb{Z}_2[x]/(x^3 + x + 1)$ из 8 элементов. Его элементами являются:

$$0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1.$$

Рассмотрим неприводимые над полем $\mathbb{Z}_2$ многочлены из кольца $\mathbb{Z}_2[x]$ степени, кратной 3:

$$\begin{aligned} m = 1: &\quad f_1(x) = x,\ f_2(x) = x+1, \\ m = 3: &\quad f_3(x) = x^3 + x + 1,\ f_4(x) = x^3 + x^2 + 1. \end{aligned}$$

Тогда многочлен $f_i(x)$, $i = 1, \ldots, 4$, имеет следующие корни θ в поле F:

$$\begin{aligned} f_1(x): &\quad \theta = 0; \\ f_2(x): &\quad \theta = 1; \\ f_3(x): &\quad \theta = x,\ x^2,\ x^2+x; \\ f_4(x): &\quad \theta = x+1,\ x^2+1,\ x^2+x+1. \end{aligned}$$

Свойства корней неприводимых многочленов

Теорема 6 (о свойствах корней неприводимых многочленов). *Пусть p — простое число, $n \geqslant 1$ и поле F — расширение поля $\mathbb{Z}_p$, содержащее p^n элементов. Тогда*

1) *если $\theta \in F$ — корень неприводимого над полем $\mathbb{Z}_p$ многочлена $f(x) \in \mathbb{Z}_p[x]$ степени n, то элементы $1, \theta, \theta^2, \ldots, \theta^{n-1}$ — линейно независимы над полем $\mathbb{Z}_p$;*

2) *если $\theta \in F$ — корень неприводимого над полем $\mathbb{Z}_p$ многочлена $f(x) \in \mathbb{Z}_p[x]$ степени n, то элементы $\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$ — все различные корни многочлена $f(x)$ в поле F.*

Свойства корней неприводимых многочленов

Доказательство.
1. Если элементы $1, \theta, \theta^2, \ldots, \theta^{n-1}$ — линейно зависимы над полем $\mathbb{Z}_p$, то θ является корнем некоторого ненулевого многочлена степени, меньшей n, что противоречит п. 2) теоремы 5.

Свойства корней неприводимых многочленов

2. Если $\theta \in F$ — корень многочлена $f(x) \in \mathbb{Z}_p$, то при $m \geqslant 1$ по утверждению 3 верно

$$f(\theta^{p^m}) = (f(\theta))^{p^m} = 0.$$

Значит, $\theta^{p^m} \in F$ — также корень многочлена $f(x)$.

Если $\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$ — не все различны, то

$$\theta^{p^m} = \theta$$

для некоторого m, $1 \leqslant m \leqslant n-1$.
Это означает, что θ является корнем многочлена $x^{p^m} - x \in \mathbb{Z}_p[x]$, а значит, по теореме 1 и корнем некоторого неприводимого над полем $\mathbb{Z}_p[x]$ многочлена степени k, где $k \leqslant m \leqslant n-1$. Но это противоречит п. 2) теоремы 5.

□

Корни неприводимого многочлена в поле из 8 элементов

Пример. Рассмотрим поле $F = \mathbb{Z}_2[x]/(x^3 + x + 1)$ из 8 элементов.
Рассмотрим неприводимый над полем $\mathbb{Z}_2$ многочлен из кольца $\mathbb{Z}_2[x]$ степени 3

$$f_3(x) = x^3 + x + 1.$$

Элемент $x \in F$ — корень многочлена $f_3(x)$ в поле F. Далее получаем другие корни:

$$\begin{array}{ll} x^2 = x^2: & (x^2)^3 + x^2 + 1 = (x^3 + x + 1)^2; \\ (x^2)^2 = x^4 = x^2 + x: & (x^2 + x)^3 + (x^2 + x) + 1 = \\ & = (x^3 + x + 1)(x^3 + x^2 + 1). \end{array}$$

Изоморфизм полей

Два поля $F_1 = (S_1; +, \cdot)$ и $F_2 = (S_2; \oplus, \otimes)$ называются **изоморфными**, если найдется взаимно однозначное отображение

$$\varphi : S_1 \to S_2,$$

сохраняющее операции, т. е. для любых $a, b \in S_1$ верно:

$$\begin{aligned} &1) \quad \varphi(a + b) = \varphi(a) \oplus \varphi(b), \\ &2) \quad \varphi(a \cdot b) = \varphi(a) \otimes \varphi(b). \end{aligned}$$

Единственность простого поля из p элементов

Утверждение 5. *Каждое поле с p элементами, где p — простое число, изморфно полю $\mathbb{Z}_p$.*

Доказательство. Пусть F — поле с p элементами, где p — простое число, с нулем e_0 и единицей e_1. Тогда

$$e_1, 2e_1, \ldots, (p-1)e_1, pe_1 = e_0 -$$

все элементы этого поля.

Отображение $\varphi : \mathbb{Z}_p \to F$,

$$\varphi(b) = be_1 \in F,$$

где $b \in \mathbb{Z}_p$, является изоморфизмом полей $\mathbb{Z}_p$ и F.

□

Единственность поля из p^n элементов

Теорема 7. *Для каждого простого числа p и каждого целого числа $n \geqslant 1$ существует единственное (с точностью до изоморфизма) поле с p^n элементами*.

Доказательство.
Существование. Поле $\mathbb{Z}_p[x]/(f)$, где p — неприводимый над полем $\mathbb{Z}_p$ многочлен степени n, является полем с p^n элементами.

Единственность поля из p^n элементов

Единственность. Пусть F — какое-то поле с p^n элементами. Можно считать, что простое поле $\mathbb{Z}_p$ является его подполем (т. к. простое поле с p элементами единственно с точностью до изоморфизма). Пусть $f(x) \in \mathbb{Z}_p[x]$ — неприводимый над полем $\mathbb{Z}_p$ многочлен степени n. По теореме 5 в поле F найдется корень $\theta \in F$ этого многочлена $f(x)$. При этом по теореме 6 элементы $1, \theta, \theta^2, \ldots, \theta^{n-1} \in F$ являются линейно независимыми над полем $\mathbb{Z}_p$. Рассмотрим поле F как линейное пространство над полем $\mathbb{Z}_p$ с базисом $1, \theta, \theta^2, \ldots, \theta^{n-1}$. Тогда отображение $\varphi : \mathbb{Z}_p[x]/(f) \to F$,

$$\varphi(b_0 + b_1 x + \ldots + b_{n-1} x^{n-1}) = b_0 + b_1\theta + \ldots + b_{n-1}\theta^{n-1},$$

где $b_0, b_1, \ldots, b_{n-1} \in \mathbb{Z}_p$, является изоморфизмом полей $\mathbb{Z}_p[x]/(f)$ и F.

□

Литература к лекции

1. Чашкин А.В. Лекции по дискретной математике. М.: Изд-во механико-математического факультета МГУ, 2007. С. 254–258.

Конец лекции