13 Неприводимые многочлены. Поля Галуа

13.1 Неприводимые многочлены

13.1.1 Определение

Пусть K — поле. Тогда $P(x) \in K[x]$ неприводим, если не существует нетривиальный делитель $Q(x) \in K[x]$, такой, что его степень больше 0, меньше степени многочлена P и $P(x)$ делится на $Q(x)$:

$$\nexists Q(x) \in K[x] : 0 < \deg Q < \deg P \text{ и } P(x) \vdots Q(x)$$

13.1.2 Определение

$P(x)$ свободный от квадратов, если не существует $Q(x)$, такой, что $\deg Q >$ и $P(x) \vdots Q^2(x)$.

13.1.3 Утверждение

$P(x) = Q^k(x)M(x)$
НОД$(Q(x), M(X)) = 1$ и $Q(x)$ неприводим $\Rightarrow P'(x) = Q^{k-1}(x)N(x)$
НОД$(Q(x), N(x)) = 1$

13.1.4 Доказательство

$P'(x) = kQ^{k-1}(x)Q'(x)M(x) + Q^k(x)M'(x)$
$P'(x) = Q^{k-1}(x)(kQ'(x)M(x) + Q(x)M'(x))$, где $kQ'(x)M(x) + Q(x)M'(x) = N(x)$

$kQ'(x)M(x) = N(x) - Q(x)M'(x) \vdots Q(x)$

$kQ'(x) \vdots Q(x)$ — противоречие
$\deg Q' = \deg Q - 1$

Это работает при $\mathbb{Z}_k$ ($k \not\vdots$ характериситку поля).

13.1.5 Следствие

$P(x) = Q_1^{k_1}(x)...Q_m^{k_m}(x)$, Q_i — неприводимы $\Rightarrow$ $P'(x) = Q_1^{k_1-1}(x)...Q_m^{k_m-1}Q(x)$, Q взаимно прост с Q_i

13.1.6 Критерий Эйзенштейн

$P(x) \in \mathbb{Z}[x]$
$P(x) = a_n x^n + ... + a_0$

$a_{n-1} \vdots p,\ a_{n-2} \vdots p,\ ..., a_0 \vdots p,\ a_n \not\vdots p \Rightarrow$ неприводима над Q

13.1.7 Доказательство

Рассмотрим $P(x) = f(x)g(x)$.

$$f(x) = b_m x^m + ... + b_0$$
$$g(x) = c_{n-m} x^{n-m} + ... + c_0$$
$$p(x) = a_n x^n + ... + a_0 = (b_m x^m + ... + b_0) \cdot (c_{n-m} x^{n-m} + ... + c_0)$$

$$a_0 = b_0 c_0 \vdots p \qquad b_0 \vdots p \qquad c_0 \not\vdots p$$

$$a_1 = b_0 c_2 + b_1 c_1 + b_2 c_0 \vdots p \Rightarrow b_2 \vdots p$$

$\vdots$

$a_m = b_0c_m + ... + b_mc_0 \vdots p \Rightarrow b_{m-1} \vdots p$

$a_n = b_nc_{n-m} \vdots p$ — противоречие

13.2 Поля Галуа

13.2.1 Определение

Конечное поле, или поле Галуа в общей алгебре — поле, состоящее из конечного числа элементов. Обозначается $\mathbb{F}_q$ или $\mathbf{GF}(q)$ или $< \mathbf{GF}(q), +, * >$, где $q = |\mathbf{GF}(q)|$ — порядок поля. Порядком поля называется количество входящих в него элементов. Пример: $\mathbb{Z}_p,\ p \in \mathbb{P}$.

13.2.2 Определение

Характериситка поля F — наименьшее n, такое, что $\forall a \in F$ выполняется следующее равенство:

$$\underbrace{a + a + ... + a}_{n \text{ раз}} = 0$$

Если такого n не существует, то n считается равным 0.

13.2.3 Лемма

Характериситка поля — простое или 0.

13.2.4 Доказательство

Рассмотрим $n = \alpha\beta$.

$$\underbrace{1 + 1 + ... + 1}_{n \text{ раз}} = 0$$

$$\underbrace{\underbrace{1 + 1 + ... + 1}_{\alpha \text{ раз}} + \underbrace{1 + 1 + ... + 1}_{\alpha \text{ раз}} + ... + \underbrace{1 + 1 + ... + 1}_{\alpha \text{ раз}}}_{\beta \text{ раз}} = 0$$

$$\underbrace{\alpha + \alpha + ... + \alpha}_{\beta \text{ раз}} = 0 \qquad \Rightarrow \text{ характеристика — } \mathbb{P}$$

13.2.5 Свойства

$f(x) \in \mathbb{Z}_p[x]$ ($f(x)$ принадлежит множеству многочленов с целыми коэффициентами по модулю p) $\mathbb{Z}_p[x]/f(x)$ (кольцо вычетов многочленов с целыми коэффициентами по модулю $f(x)$)

$$\left.\begin{matrix} g_1(x) \equiv_{f(x)} h_1(x) \\ g_2(x) \equiv_{f(x)} h_2(x) \end{matrix}\right| \Rightarrow \begin{matrix} g_1 + g_2 \equiv_{f(x)} h_1 + h_2 \\ g_1g_2 \equiv_{f(x)} h_1h_2 \end{matrix}$$

13.2.6 Теорема

$\mathbb{Z}_p[x]/f(x) \ \Leftrightarrow\ f(x)$ неприводим над $\mathbb{Z}_p$.
$\deg f = m\ \mathbf{GF}(p^m)$

13.2.7 Доказательство

Прямое. Рассмотрим $f(x) = g(x)h(x)$
$g(x)h(x) \equiv_{f(x)} 0 \qquad | \cdot g^{-1}(x)$
$h(x) \equiv_{f(x)} 0| \Rightarrow f(x) = 0$

От обратного. $\forall g(x) \neq 0 \deg g < \deg p$
НОД$(g(x), f(x)) = 1 \ \Rightarrow$ по расширенному алгоритму Евклида:
$a(x)g(x) + b(x)f(x) = 1$
$a(x)g(x) \equiv_{f(x)} 1 \ \Rightarrow \ a = g^{-1} \ \Rightarrow \ \mathbb{Z}_p$ — поле

13.2.8 Связь с линейным пространством

Поле Галуа образует линейное (векторное) пространство. Его аксиомы:

- $(a + b) + c = a + (b + c)$
- $\exists 0 : a + 0 = a$
- $\forall a \ \exists (-a) : a + (-a) = 0$
- $a + b = b + a$
- $\alpha(a + b) = \alpha a + \alpha b$
- $(\alpha + \beta)a = \alpha a + \beta a$
- $\alpha(\beta a) = (\alpha\beta)a$
- $\exists 1 : 1 \cdot a = a$

$\alpha, \beta \in \mathbb{Z}_p$, F — линейное пространство. $m = \dim F$.

13.2.9 Определение

α — примитивный элемент, если $\forall b \neq 0 \in F \qquad b = \alpha^i$.