28.10.25

Конечные поля

Опр. Конечное поле – поле с конечным числом элементов

$P[x]$ – кольцо мн-ов над полем P.

Идеалы $P[x]$ – ?

$S(x)$ – произвольный многочлен

$S(x)\cdot P_1(x), S(x)\cdot P_2(x), \dots, S(x)\cdot P_3(x) \in P[x]$

$P[x]/S(x)\cdot P[x]$ – фактор-кольцо $P[x]$ по идеалу $S(x)P[x]$

$\bar{h} = h(x) + S(x)P[x] = h + (S)$ все мн-ны $\vdots\, S(x)$

$S(x)\cdot P[x]$ – идеал $P[x]$

Теорема $P[x]/S(x)\cdot P[x]$ – поле $\Leftrightarrow$ $S(x)$ – неприводим в $P[x]$

Док-во: ▲ Пусть $S(x)$ – приводимый $\Rightarrow S(x) = u(x)\cdot v(x)$

$\bar{u} = u + S(x) \quad \bar{v} = v + (S)$;

$\bar{u}\cdot\bar{v} = (u+(S))(v+(S)) = \underbrace{uv}_{=S} + u(S) + v(S) + (S)(S) = S + (S) = (S) = 0 + (S)$

$\bar{u}\cdot\bar{v}$ – делители нуля $\Rightarrow$ это не поле

Пусть теперь $S(x)$ – неприводимый в $P[x]$

$\forall\, \bar{h} = h + (S) \neq 0 + (S)$

НОД $(S(\alpha), h(\alpha)) = 1 \Rightarrow$ из алг. Евклида следует, что

$\exists v, u:\ uS + vh = 1$

$\bar{v} = v + (S)$

$\bar{h}\cdot\bar{v} = (h+(S))(v+(S)) = hv + h(S) + v(S) + (S)(S) = 1 - uS + (S) = 1 + (S)$

$\bar{v}$ - обратный к элементу h: $\bar{v} = \bar{h}^{-1}$ ■

P – поле $P[x]$ $\quad P[x]/S(x)\cdot P[x]$

1) $S(x)$ – неприводим.

$\alpha \in P \quad \bar{\alpha} + \alpha + (S)$

2) $\bar{x} = x + (S)$

$S = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$

$S(\bar{x}) = a_0 (x+(s))^n + a_1 (x+(s))^{n-1} + \ldots + a_{n-1}(x-(s)) + a_n =$

$$(x+(s))^n = x^n + n x^{n-1}(s) + \frac{n(n-1)}{2} x^{n-1} + \ldots = x^n + (s)$$

$= a_0(x^n + (s)) + a_1(x^{n-1} + (s)) + \ldots + a_{n-1}(x + (s)) + a_n =$

$= a_0 x^n + a_0(s) + a_1 x^{n-1} + a_1(s) + \ldots + a_{n-1} x + a_{n-1}(s) + a_n =$

$= S + (S) = (S) = 0 + (S)$

$S(x)$ — неприводимый многочлен

$S(a) \neq 0$

$P[x] / S(x) \cdot P[x]$ — поле, $S(\bar{x}) = 0$ $\quad \bar{x} = x + S$ — корень $S(x)$

Пример.

$\mathbb{Z}_2[x] / (x^2+x+1)\mathbb{Z}_2[x]$ — поле $= \{0; 1; \alpha; \alpha+1\}$

$x^2 + x + 1 = 0$

$0; 1$ — не корни

$\exists\, \alpha$ — корень $x^2+x+1 = \alpha^2 + \alpha + 1 = 0$

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

$\alpha^2 = -\alpha - 1 = \alpha + 1$

$\alpha(\alpha+1) = \alpha^2 + \alpha = \alpha + 1 + \alpha =$

$= (\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = \alpha + 1 + 0 + 1 = \alpha$

Все элементы в строке и столбце должны быть различны

$P[x]$; $S(x)$ — неприв. $\qquad f(x)$ над полем P

$P[x] / S(x) \cdot P[x] = P_1 \qquad P_1 = P[x] / f(x) \cdot P[x] \qquad f(x) = (x-\alpha)\ldots f_1(x)$

$P_1 = P \cup \{\alpha\} \qquad P_1 = P \cup \{\alpha\} \qquad P_1[x] / f_1(x) \cdot P_1[x] = P_2$

$P_k = P \cup \{\alpha\} \cup \{\beta\} \cup \ldots \cup \{\ldots\} \qquad P_2 = P \cup \{\alpha\} \cup \{\beta\}$

$f(x) = \Pi(x - \alpha_1) \qquad f(x) = (x-\alpha)\ldots(x-\beta), \ldots f_2(x)$

P_k — поле разложения $f(x)$

Пример.

$\mathbb{Z}_3[x]/(x^3+2x+2)\mathbb{Z}_3[x]$

$(x^5-2x^4-x^2+2)\ f = x^4+x^3+x^2+x+1 \ (mod(x^3+2x+2))$

1) $x^3+2x+2=0 \quad x^3=-2x-2$

$x^5-2x^4-x^2+2 = x^2(x+1)-2x(x+1)-x^2+2 = x^3+x^2-2x^2-2x-x^2+2 =$

$= -2x^2-x = x^2+2x$

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

Итог: $(x^2+2x)f = (2x^2+2)(mod(x^3+2x+2))$