Семинар 23, 07.03.24

① Пусть R - кольцо и $\mathfrak{a} \trianglelefteq R$ (т.е. $\mathfrak{a} \subseteq R$ - идеал)

Док-ть, что $\mathfrak{a} = R \Leftrightarrow \exists x = \mathfrak{a} : x \in R^\times$ (идеалы, совпадающие со всем, обознач. (1)).

□ „$\Rightarrow$" очев.

„$\Leftarrow$" $x \in \mathfrak{a} \cap R^\times \Rightarrow x^{-1} \cdot x \in \mathfrak{a} \Rightarrow 1 \in \mathfrak{a}$; $\forall r \in R \quad r = r \cdot 1 \in \mathfrak{a}$ ■

② Является ли мн-во матриц вида $\begin{pmatrix} a & b \\ nb & a \end{pmatrix}$, $a, b \in F$ полем, где F-поле n - фикс. целое число ($F = \mathbb{Q}, \mathbb{R}, \mathbb{Z}_p$ для $p = 2, 3, 5$)?

Фикс. $\begin{pmatrix} a & b \\ nb & a \end{pmatrix} \neq 0$

$$\begin{pmatrix} x & y \\ ny & x \end{pmatrix} \cdot \begin{pmatrix} a & b \\ nb & a \end{pmatrix} = \begin{pmatrix} ax + nby & bx + ay \\ n(bx + ay) & ax + nby \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\Rightarrow \begin{cases} bx + ay = 0 \\ ax + nby = 1 \end{cases} \text{ - слу на } x, y.$$

$$\left(\begin{array}{cc|c} b & a & 0 \\ a & nb & 1 \end{array}\right)$$

1) $b = 0 \Rightarrow a \neq 0$ и $y = 0$, $x = \frac{1}{a}$

2) $b \neq 0$: $\left(\begin{array}{cc|c} 1 & \frac{a}{b} & 0 \\ 0 & nb - \frac{a^2}{b} & 1 \end{array}\right)$ - имеет решение $\Leftrightarrow$

$\Leftrightarrow nb - \frac{a^2}{b} \neq 0$, т.е. $nb^2 \neq a^2$ $\forall a \in F$. В частн., $n \neq 0$

1) $F = \mathbb{Q}$

$n \neq \frac{a^2}{b^2}$, т.е. n не явл. квадратом

2) $F = \mathbb{R}$: $n < 0$

3) $\mathbb{Z}_2$: в $\mathbb{Z}_2$ $\lambda^2 = \lambda$ $\forall \lambda$ $nb \neq a$ $\forall a$ $\forall b \neq 0$

$n \neq a$ $\forall a$

Никогда не поле

4) $\mathbb{Z}_3$: $n = 1$ $b^2 = a^2$ разрешимо

$n = -1$ $-b^2 = a^2$

в $\mathbb{Z}_3$ $b^2 = 1 \Rightarrow a^2 = -1$ – не разрешимо

5) $\mathbb{Z}_5$: Квадраты в $\mathbb{Z}_5$: $1, -1, 0$

$nb^2 \neq \pm 1$, т.е. $n \neq \pm 1 \pmod 5$

③ Конечное поле F имеет положительную характеристику.

□ Рассмотрим группу $(F, +)$ – конечна $\Rightarrow$ порядок 1 конечен ■

∀ конечное поле F имеет порядок p^k, где $\mathrm{char} F = p$ – простое, $k \in \mathbb{N}$

Причём два конечных поля изоморфны $\Leftrightarrow$

$\Leftrightarrow$ у них одинаковые порядки.

Поле порядка q обознач. F_q.

Малая теорема Ферма: в F_p $x^p = x$ $\forall x \in F_p$

В частности, $x^{p-1} = 1$ $\forall x \in F_p^x$ $\Rightarrow x^{-1} = x^{p-2}$

Пусть F – поле и $f \in F[x]$. Если $f = g \cdot h$, то можно найти $g_0, h_0 \in F[x]$, что $f = g_0 \cdot h_0$, старший коэф. $g_0 = 1$ и h_0 и h пропорциональны. И для $g, h \in F[x]$

$\deg(gh) = \deg g + \deg h$ $(\deg 0 = -\infty)$

⑤ Разложить на неприводимые

$f(x) = x^5 + x^3 + x^2 + 1$ в $F_2[x]$

$x \nmid f$, $(x-1) \mid f \Rightarrow f(x) = (x+1)\underbrace{(x^4 + x^3 + x + 1)}_{f_1}$

$x \nmid f_1$, $(x+1) \mid f_1 \Rightarrow f_1(x) = (x+1)\underbrace{(x^3+1)}_{f_2}$

$x \nmid f_2$, $(x+1) \mid f_2 \Rightarrow f_2(x) = (x+1)\underbrace{(x^2+x+1)}_{f_3}$

$x \nmid f_3$, $(x+1) \nmid f_3$

$\Downarrow$

f_3 неприводим $\quad f(x) = (x+1)^3(x^2+x+1)$

⑥ При делении с остатком в $F[x]$ или $\mathbb{Z}$ остаток и неполное частное определены однозначно

□ $f = q_1 \cdot g + r_1 = g \cdot q_2 + r_2$, $\deg r_i < \deg g \Rightarrow$

$\Rightarrow r_1 - r_2 = g(q_1 - q_2)$

$\deg(r_1 - r_2) \leqslant \deg r_i < \deg g$

Если $q_2 = q_1$, то $\deg(g(q_1 - q_2)) \geqslant \deg g$.

$\Downarrow$

противоречие $\Rightarrow q_2 = q_1 \Rightarrow r_1 = r_2$ ■

F-поле, $S \in F[x]$, $\deg S = n$

Операции в $F[x]/S$: многочлены рассматриваются по mod S, т.е. их остатки при делении на S.

Степень остатка $< n \Rightarrow$ рассматриваются многочлены степени $< n$. Сложение понятно ($(f_1+)^n$).

Умножение: как в $F[x]$, но нужно снова брать остаток mod S

$F[x]/S$ - является полем $\Leftrightarrow$ S неприводим.

$|F[x]/S| = |F|^n$

В частности, для $F = f_p$ мы нашли F_{p^n} как в $F[x]/S$ найти обратный к F! Можем считать $\deg f < n$

I) Обозначим $g = f^{-1}$ и запишем $g = a_0 x^{n-1} + a_1 x^{n-2} + \dots + a_{n-1}$

для нек. $a_i \in F$. Считаем $h_i(x) = f(x) \cdot x^i$ для всех $i = \overline{0, n-1}$

$\Rightarrow$ система на коэфф. a_i

$$1 = f \cdot g = \sum_{i=0}^{n-1} a_i x^{n-1-i} \cdot f = \sum_{i=0}^{n-1} a_i h_i \text{ - слу}$$

⑧ Вычислить $\frac{x+1}{x^4}$ в $\mathbb{Z}_3[x]/(x^3+2x^2+x+1)$

x^3+2x^2+x+1 - неприв., т.к. у него нет корней

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

$\overline{x^4} = \overline{2x+1}$, $f(x) = 2x+1$

$(2x+1)^{-1} = ax^2 + bx + c$

$h_0 = f \cdot 1 = 2x+1$

$h_1 = f \cdot x = 2x^2 + x$

$h_2 = f \cdot x^2 = 2x^3 + x^2 = 2(x^3+2x^2+x+1) + (x^2+x+1) + x^2 \equiv x+1$

$1 = a_0 h_0 + a_1 h_1 + a_2 h_2$

$1 = 1 + 0x + 0 \cdot x^2$

$h_0 = 1 + 2x + 0x^2$

$h_1 = 0 + 1x + 2x^2$

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 2 & 1 & 1 & 0 \\ 0 & 2 & 0 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & -2 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -2 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{array}\right)$$

$\Rightarrow f^{-1} = -1 - x^2$

$\frac{x+1}{x^4} = (x+1)(-x^2-1) = -x^3-x^2-x-1 = (-1)(x^3+x^2+x+1)+(x^2+0x+0) = x^2$.

II) S неприводим $\Rightarrow \forall f \in F[x]$: $\deg f < n$ $\quad НОД(f,S)=1$

$\Rightarrow 1 = a\cdot S + b f$ для нек. $a, b \in F[x]$

$\Rightarrow$ в $F[x]/S$ $\quad 1 = b\cdot f$, т.е. $b = f^{-1}$

(может получиться $НОД(S,f) = \lambda \in F^*$ $\Rightarrow$

$\Rightarrow \lambda = a\cdot S + bf$, $1 = \lambda^{-1} a S + \lambda^{-1} b f \Rightarrow f^{-1} = \lambda^{-1} b$)

⑨ $(x^6+x^4+x+1)^{-1}$ в $\mathbb{Z}_2[x]/(x^8+2x^4+x^3+x+1)$

$f_0 = x^8+2x^4+x^3+x+1 \qquad g_0 = x^6+x^4+x+1$

$f_0 = g_0(x^2+1) + x^2$

$f_1 = g_0 = x^6+x^4+x+1 \qquad g_1 = x^2$

$f_1 = g_1(x^4+x^2) + (x+1)$

$f_2 = x^2 \qquad g_2 = x+1$

$f_2 = g_2(x+1) + 1$

$f_3 = x+1 \qquad g_3 = 1$

$1 = f_2 - g_2(x+1) = f_2 - g_2(f_1 - g_1(x^4+x^2)) =$

$= g_1(1-x^4-x^2) - g_2 f_1 =$

$= (f_0 - g_0(x^2+1))(1-x^4-x^2) - (x+1) g_0 =$

$= g_0 \underbrace{(x+1+(x^2+1)(1+x^2+x^4))}_{g_0^{-1}} + \dots$