Лекция 15 октября (первая половина)

Упражнение оставшееся с прошлого раза:

- Мы построили конечное поле $\mathbb{F}_q$ из $q=p^n$ элементов как множество всех корней многочлена x^q-x в некотором поле $\mathbb{K}$:

  (1) $\mathbb{K}\supset\mathbb{F}_p$

  (2) $x^q-x=\prod_{i=1}^{q}(x-\alpha_i)$ в $\mathbb{K}[x]$

- Произвольное поле $\mathbb{L}$ из q элементов имеет вид $\{0,\underbrace{1,\zeta,\dots,\zeta^{q-2}}_{\mathbb{L}\setminus 0}\}$

Берём многочлен $g\in\mathbb{F}_p[x]$ наименьшей степени, приведённый и такой что $g(\zeta)=0$ [минимальный многочлен эл-та ζ] $g(x)$ неприводим в $\mathbb{F}_p[x]$ и делит нацело любой многочлен $f\in\mathbb{F}_p[x]$: $f(\zeta)=0$.

$$\begin{array}{ccc} \dfrac{\mathbb{F}_p[x]}{(g)} & \xhookrightarrow{\sim} & \mathbb{L} \\ [f] & \longmapsto & f(\zeta) \end{array}$$

$$\begin{tikzcd}
\mathbb{F}_p[x]/(g) \arrow[r, "\sim"] & \mathbb{F}_q \\
{[f]} \arrow[r, mapsto] & f(\xi)
\end{tikzcd}$$

корректно, надо чтобы $g(\xi)=0$ в $\mathbb{F}_q$

Упр: Почему такой ξ существует? Почему g (минимальный многочлен эл-та $\zeta \in \mathbb{L}$) имеет корень в $\mathbb{F}_q$?

Оставим ещё раз на дом

Кольца частных (дробей, локализация).

$K \supset S \leftarrow$ мультипликативно замкнутая система эл-тов, содержащая 1

$S^{-1}K$ ($\doteq K[S^{-1}]$)

$\ni$ дроби $\frac{a}{s}$ $a \in K$, $s \in S$

$$\frac{a_1}{s_1} = \frac{a_2}{s_2} \iff \exists t \in S: \; a_1 s_2 t = a_2 s_1 t,$$

это минимальная эквивалентность, содержащая отождествление

$a = at \quad \forall t \in S$

$s \quad st$

Как нам выходит, что в $\mathbb{Q}$ $\frac{a_1}{s_1} = \frac{a_2}{s_2} \Leftrightarrow$

$$a_1 s_2 \overset{?}{=} s_1 a_2$$

$$\begin{tikzcd}
\frac{a_1}{s_1} \arrow[rr, bend left, leftrightarrow, "?"] \arrow[r, phantom, "\sim"] \arrow[d, phantom, "\Updownarrow"] & \frac{a_2}{s_2} \arrow[r, phantom, "\sim"] & \frac{a_3}{s_3}
\end{tikzcd}$$

$a_1 s_2 = a_2 s_1 \qquad a_2 s_3 = a_3 s_2$

$$\boxed{a_1 s_2 s_3 = a_2 s_1 s_3 = a_3 s_2 s_1}$$

Это не $a_1 s_3 = a_3 s_1$!

$$a_1 s_3 \cdot s_2 = a_3 s_1 \cdot s_2$$

если в K нет делителей нуля "относительно S"
(т.е. выполнено $xs = 0$ с $s \in S \Rightarrow x = 0$)

$$s_2(\underbrace{a_1 s_3 - a_3 s_1}_{0}) = 0$$

Упр.: $\mathbb{Z}/(6) \supset S = \{[1], [2], [4]\}$ мультипликативная система

$S^{-1}\mathbb{Z}/(6)$

$$\mathbb{Z}/[6] \hookrightarrow S^{-1}\mathbb{Z}/(6)$$

$$a \longmapsto a/1$$

[3] – это делитель нуля отн. S

$[3]\cdot[2]=0$ $\quad \dfrac{[3]}{[1]}=0$

$= \dfrac{[3][2]}{[1][2]}$

! Выписать явно все различные эл-ты у $S^{-1}\mathbb{Z}/(6)$ и убедиться, что это кольцо изоморфно полю $\mathbb{F}_3 = \mathbb{Z}/(3)$

Пример K, S – множество всех эл-тов, которые не делят нуль

$$S=\{a\in K \mid ax=0 \text{ только при } x=0\}$$

$a_1a_2x=0$ и $a_2x\neq 0 \Rightarrow a_1\notin S$

$S^{-1}K := \mathbb{Q}_K$ кольцо частных кольца K.

Если в K вообще нет делителей нуля, то $\mathbb{Q}_K$ – это поле, называется поле частных целостного кольца

Подпример 1: $K=\mathbb{Z}$ $\quad \mathbb{Q}_\mathbb{Z}=\mathbb{Q}=\left\{\frac{a}{b} \,\middle|\, \begin{matrix} a\in\mathbb{Z} \\ b\in\mathbb{N}\end{matrix}\right\}$

$\swarrow$

канонический представитель

("несократимая дробь")

$\frac{a}{b}$ $a\in\mathbb{Z}$, $b\in\mathbb{N}$, НОД$(a,b)=1$

такие $\frac{a_1}{b_1}=\frac{a_2}{b_2} \Leftrightarrow a_1=a_2 \; \& \; b_1=b_2$

Подпример 2: $\Bbbk$ - поле, $K=\Bbbk[x]$

$\mathbb{Q}_K := \Bbbk(x)$ поле рациональных функций над $\Bbbk$.

$$\mathbb{Q}_K=\left\{\frac{f}{g} \;\middle|\; f\in\Bbbk[x],\ g\neq 0\right\}$$

несократимое представление:

$\frac{f}{g}$: g приведён, НОД$(f,g)=1$

$$\frac{f_1}{g_1}=\frac{f_2}{g_2} \Leftrightarrow \underline{f_1g_2}=\underline{g_1f_2}$$

$f_2=f_1\cdot s$

$g_2=g_1\cdot t$

$1=s=t \Leftarrow$

НОД$(f_2,g_2)=1$

$f_1g_1t=g_1f_1s$

Подпример 3 $K=\Bbbk[[x]]$

$\mathbb{Q}_K:=\Bbbk((x))$

поле рядов Лорана.

$$\frac{f}{g} = t^{-k}\frac{f}{g_1}$$

$k \in \mathbb{Z}$,

где g_1 - это обратимый ряд (т.е. ряд с ненулевым свободным членом)

$$g = a_k t^k + \ldots = t^k(a_k + a_{k+1}t + \ldots)$$

$$\frac{1}{g_1} = b_0 + b_1 t + \ldots$$

$$\frac{f}{g} = t^{-k}\cdot h \qquad h \in \mathbb{k}[[x]]$$

$$\frac{f}{g} = \sum_{k \geq N} a_k t^k \quad \text{где } N \in \mathbb{Z}$$

← ряд Лорана

степенной ряд, в котором допускается конечное число целых отрицательных степеней.

$$\begin{tikzcd}
\mathbb{k}[x] \arrow[r, hook] \arrow[d, phantom, sloped, "\subset"] \arrow[rr, dashed, bend right] & \mathbb{k}[[x]] \arrow[r, phantom, "\subset"] & \mathbb{k}((x)) \\
\mathbb{k}(x) \arrow[rru, hook]
\end{tikzcd}$$

Рациональные функции содержатся в $\mathbb{k}((x))$ в качестве подполя, т.е. каждая рациональная функция раскладывается в степенной ряд Лорана

Разложение рациональной? функции на простейшие дроби:

$$\frac{f}{g} = q + \frac{r}{g}$$

$\deg r < \deg g$

q - неполное частное от деления f на g.

если $g = g_1 g_2$ и $\text{НОД}(g_1, g_2) = 1$

$$\frac{r}{g} = \frac{r_1}{g_1} + \frac{r_2}{g_2} \quad \deg r_i < \deg g_i \quad i = 1, 2.$$

$$\boxed{r = r_1 g_2 + r_2 g_1} \; *$$

$\downarrow \bmod g_1$

$\leftarrow$ обратим $\bmod g_1$

$$[r]_{g_1} = [r_1]_{g_1} \underline{\underline{[g_2]}}_{g_1}$$

r_1 - это представитель эл-та $\dfrac{[r]}{[g_2]}$ в $\mathbb{k}[x]/(g_1)$

$\deg r_1 < \deg g_1$

из (*) $\deg r_2 < \deg g_2$

Если $g = g_1 g_2 \dots g_m$ и НОД$(g_i; g_j) = 1$

$$\frac{f}{g} = q + \frac{r_1}{g_1} + \dots + \frac{r_m}{g_m} \quad \deg r_i < \deg g_i$$

Такое представление единственно!

q – это неполное частное от деления f на g: $f = qg + r_1 G_1 + r_2 G_2 + \dots + r_m G_m$

$$G_i = \frac{g}{g_i} = \prod_{\nu \neq i} g_\nu \leftarrow \boxed{\text{помножим все кроме } g_i}$$

Так как все G_j с $j \neq i$ делятся на g_i

по mod g_i: $[f - qg]_{g_i} = [r_i G_i]_{g_i}$

остаток от деления f на g

$[r_i]$ – класс частного $\dfrac{[f - qg]_{g_i}}{[G_i]_{g_i}}$

в $\mathbb{k}[x]/(g_i)$ (элемент $[G_i]_{g_i}$ обратим! НОД$(g_i, G_i) = 1$).

Если $g \neq g_1 g_2 \dots g_m$, то

$g = p^m$ где p — неприводим

7-

$a_0 + 7a_1 + 7^2 a_2$

$\boxed{0 \leq a_i \leq 6}$

$g = p^m$

$$\boxed{\frac{r}{g} = \frac{r_1}{p} + \frac{r_2}{p^2} + \dots + \frac{r_m}{p^m}}$$

где $\deg r_i < \deg p$.

$$r = \overbrace{r_1 p^{m-1} + r_2 p^{m-2} + \dots + \underline{r_{m-1}} p} + r_m$$

r_m = остаток от деления r на p

r_{m-1} = остаток " — " $\frac{r - r_m}{p}$ на p

. . . . .

Такая запись единственна.

r_{m-2} = остаток $\dfrac{\frac{r - r_m}{p} - r_{m-1}}{p}$ от делен. на p

Это представление многочлена r в p-ичной позиционной системе счисления совершенно аналогичное представлению целого числа r в m-ичной позиционной системе

Над алгебраически замкнутым полем

∀ любого многочлена $1+a_1x+\ldots+a_mx^m$

$$\frac{1}{1+a_1x+\ldots+a_mx^m}=\sum\frac{\alpha_i}{(1-\beta_i x)^{m_i}}$$

$\alpha_i \in \mathbb{k}$

β_i − это [illegible] $\beta_i \in \mathbb{k}$

$\xrightarrow[t \leftarrow \frac{1}{x}]{}$

потом помножив всё на x^n

$$\frac{1}{1-x}=1+x+x^2+x^3+\ldots$$

$$(1-x)(1+x+x^2+x^3+\ldots)=1$$

$$\frac{1}{1-\alpha x}=1+\alpha x+\alpha^2x^2+\alpha^3x^3+\ldots$$

$$\frac{1}{(1-\alpha x)^2}\qquad \frac{d}{dx}(1-\alpha x)^{-1}=\alpha(1-\alpha x)^{-2}$$

$$=\frac{1}{\alpha}\frac{d}{dx}(1+\alpha x+\alpha^2x^2+\ldots)=$$

$$=\frac{1}{\alpha}(\alpha+2\alpha^2x+3\alpha^3x^2+\ldots)=1+2\alpha x+3\alpha^2x^2+\ldots$$

Упр. Получить формулу для

$$(1+\alpha x)^{-m}=1+\binom{-m}{1}\alpha x+\binom{-m}{2}\alpha^2x^2+\ldots$$

$$\binom{-m}{k}=\frac{\overbrace{-m(-m-1)\ldots(-m-k+1)}^{k}}{k!}$$

Как устроен образ $\mathbb{k}(x)$ в $\mathbb{k}((x))$

$$\frac{b_0+b_1x+b_2x^2+\dots+b_mx^m}{\underline{\underline{1}}+c_1x+c_2x^2+\dots+c_kx^k}=a_0+a_1x+a_2x^2+\dots$$

при x^n получим слева 0 при $n>m$

а справа $\underbrace{a_n+c_1a_{n-1}+c_2a_{n-2}+\dots+c_ka_{n-k}}_{\substack{\| \\ 0}}$

$$\boxed{a_n=c_1a_{n-1}+c_2a_{n-2}+\dots+c_ka_{n-k}}$$

рекуррентное уравнение
k-того порядка

Их можно явно решать, разлагая
разлагая рациональные ф-ции в ряды.