Z – област (ком. пр. с 1 без дел. на 0 ~ $\mathbb{Z}$)

$Z_0 = \{(a,b) \mid a, b \in \mathbb{Z}, b \neq 0\}$

$\sim : (a,b) \sim (c,d) \overset{def}{\iff} ad = bc$

<u>Тв.</u> $\sim$ е РЕ

<u>Д-во</u> 1) рефл. ✓

2) симетр.

3) Транзит. $\underline{(a,b)} \sim (c,d)$, $(c,d) \sim \underline{(e,f)}$

$\Rightarrow ad = bc$ и $cf = de$

$a\underline{dc}f = b\underline{cd}e \overset{d\neq 0}{\underset{c\neq 0}{\Rightarrow}} af = de \Rightarrow (a,b) \sim (e,f)$

$c = 0 \Rightarrow ad = 0 \Rightarrow \underline{a = 0} \Rightarrow de = 0 \Rightarrow \underline{e = 0}$

$$\mathbb{Q} = \mathbb{Z}_0/\sim \; = \{[(a,b)] \mid (a,b) \in \mathbb{Z}_0\}$$

$$[(a,b)] = \{(c,d) \mid (a,b) \sim (c,d)\}$$

Дефинираме опер. в $\mathbb{Q}$

$$[(a,b)] + [(c,d)] := [(ad+bc, bd)]$$

$$[(a,b)] \cdot [(c,d)] := [(ac, bd)]$$

<u>Тв.</u> $(\mathbb{Q}, +, \cdot)$ е поле

<u>Д-во</u> 1) коректност на опер.

$(+)$ $(a,b) \sim (a',b')$, $(c,d) \sim (c',d')$

$$\overset{?}{\Longrightarrow} (ad+bc, bd) \sim (a'd'+b'c', b'd')$$

$$ab' = ba', \quad cd' = dc'$$

$$(ad+bc)\,b'd' = (a'd'+b'c')\,bd \;?$$

$$\underline{a}d\underline{b'}d' + b\underline{c}b'\underline{d'} \;\; a'd'bd + b'c'bd$$

$$ba'dd' + dc'bb'$$

⊙ Аналог.

Св-ва на плюс

$$-\big([[a,b]] + [[c,d]]\big) + [[e,f]] = [[(ad+bc,\ bd)]] + [[e,f]] =$$

$$= [[(ad+bc)f + bde,\ bdf]] \quad \checkmark$$

$$[[a,b]] + \big([[c,d]] + [[e,f]]\big) = [[a(df) + b(cf+de),\ b(df)]]$$

Дст. аналог.

$\mathbf{0} = [(0,1)] = \{(0,b) \mid b \in \mathbb{Z}, b \neq 0\}$

$\left(-[(a,b)]\right) = [(-a,b)]$; $[(a,b)] - [(c,d)] = [(ad-bc, bd)]$

$\mathbf{1} = [(1,1)] = \{(a,a) \mid a \in \mathbb{Z}, a \neq 0\}$

$[(a,b)] \neq \mathbf{0} \iff a \neq 0$

$[(a,b)]^{-1} \underset{a\neq 0}{=} [(b,\underline{a})]$

$Q_0 = \{[(a,1)] \mid a \in \mathbb{Z}\} \subseteq Q$

- Q_0 – подпръстен на Q
- $\mathbb{Z} \cong Q_0$

$$\varphi : \mathbb{Z} \to Q_0$$
$$a \mapsto [(a,1)]$$

$\varphi(a) + \varphi(b) = [(a+b, 1)] = \varphi(a+b)$

$\varphi(a)\varphi(b) = [(ab, 1)] = \varphi(ab)$

φ - инект. и сюрект.

$\Phi : \mathbb{Z} \to Q$; $\forall z \in \mathbb{Z}$ $\Phi(z) = \varphi(z)$

Φ - ХММ ; $\operatorname{Ker} \Phi = \{0\}$; $\operatorname{Im} \Phi = Q_0$

$\mathbb{Z}$ се влага в Q .... б.о.о. смятаме, че

$\mathbb{Z}$ е подпръстен на Q

$$[(a,b)] = [(a,1)][(b,1)]^{-1} = ab^{-1}$$

$$[(a,1)] = a, \quad [(b,1)] = b$$

$$Q = \{ab^{-1} \mid a, b \in \mathbb{Z}\}$$

Характеристика на поле. Прости полета

F - поле

<u>Опр.</u> $\operatorname{char} F = |1|_{(F,+)} = \begin{cases} n & |1| = n \\ 0 & |1| = \infty \end{cases}$

характеристика

$|1| = k \quad \to \quad k \cdot 1 = \underbrace{1 + \dots + 1}_{k} = 0$

<u>min</u> с това св-во

Пр. 1) $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$

2) $\operatorname{char} \mathbb{Z}_p = p$ (p - просто)

$a \in F$, $n \in \mathbb{Z}$ $\quad n \cdot a = (n \cdot 1)\, a$

означение $\qquad$ умнож. в F

Зад. $(m\, n) \cdot 1 = (m \cdot 1)(n \cdot 1)$

Тв. $\operatorname{char} F \neq 0 \Rightarrow \operatorname{char} F$ - просто число

Тв. 1) $n \cdot a = 0 \iff a = 0$ или $n = 0$ $\qquad$ за $\operatorname{char} F = 0$

2) $n \cdot a = 0 \iff a = 0$ или $p \mid n$ $\qquad$ за $\operatorname{char} F = p$

Опр. F - просто поле, ако няма собствени подполета, т.е. $\nexists F$

Тв. Всяко поле има просто подполе

Д-во F - поле; $K = \bigcap\limits_{\substack{P<F \\ \text{подполе}}} P$ - подполе на F ... просто

Тв. $\mathbb{Q}$ и $\mathbb{Z}_p$ са прости полета

Д-во 1/ $F < \mathbb{Q}$; $1 \in F \Rightarrow \mathbb{N} \subseteq F \Rightarrow \mathbb{Z} \subseteq F \Rightarrow \mathbb{Q} \subseteq F \Rightarrow F = \mathbb{Q}$

2/ $F < \mathbb{Z}_p$; $(\mathbb{Z}_p, +) \cong C_p$; $(\mathbb{Z}_p, +) = \langle \bar{1} \rangle$

$\bar{1} \in F \Rightarrow \forall\, \bar{a} \in F \Rightarrow F = \mathbb{Z}_p$

Тв. F - поле; P - простото му подполе

1/ $\operatorname{char} F = 0 \Rightarrow P \cong \mathbb{Q}$

2/ $\operatorname{char} F = p \Rightarrow P \cong \mathbb{Z}_p$

Зад. K е подполе на L, то L е лин. простр. над K

Зад. $\operatorname{char} F = 0 \Rightarrow |F| = \infty$

Зад. $|F| < \infty \Rightarrow \exists\, p$-пр. : $\mathbb{Z}_p < F$; $\dim_{\mathbb{Z}_p} F = n$

$\Rightarrow |F| = p^n$; $\exists\, \alpha_1 \ldots \alpha_n : F = \{ \sum_{i=1}^{n} \lambda_i \alpha_i \mid \lambda_i \in \mathbb{Z}_p \}$

Б.о.о. $\alpha_1 = 1$

$|F| = p^2$ ... още $\exists$ ... $\exists \alpha$: $F = \{ \overset{1 \cdot a}{\overset{\shortparallel}{a}} + \alpha b \mid a, b \in \mathbb{Z}_p \}$

(1 и α – базис)

$\exists\, p, q : \alpha^2 = p + \alpha q \rightarrow f(\alpha) = 0$ за $f = x^2 - qx - p$

с коеф. в $\mathbb{Z}_p$

Напр. за $\mathbb{Z}_2$ $f = x^2 + x + \bar{1}$; $\alpha^2 = \alpha + 1$

$F = \{(a,b) \mid a,b \in \mathbb{Z}_2\}$ $\quad ((a,b) \sim a + \alpha b)$

$(a,b) + (c,d) := (a+c,\ b+d)$

$(a,b)(c,d) := (ac+bd,\ bc+ad+bd)$

може да се провери, че $(F, +, \cdot)$ е поле

$\alpha := (0,1)$ $\qquad (a,b) = (a,0) + \underbrace{(b,0)(0,1)}_{(0,b)} = \underset{(a,0)}{a} + \underset{(b,0)}{b}\alpha$

$F = \{0, 1, \alpha, \alpha+1\}$ $\quad +$ лесно

$\cdot$	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

Д-во на Тв. // char $F = 0$

$$\varphi : \mathbb{Q} \longrightarrow F$$

$$\frac{a}{b} \longmapsto (a.1)(b.1)^{-1}$$

— коректност

$$\frac{a}{b} = \frac{c}{d} \Rightarrow ad = bc \Rightarrow (ad).1 = (bc).1 \Rightarrow$$

$b \neq 0 \neq d$

$$\Rightarrow (a.1)\underset{\neq 0}{(d.1)} = \underset{\neq 0}{(b.1)}(c.1) \xrightarrow{\cdot (d.1)^{-1}(b.1)^{-1}}$$

$$\Rightarrow (a.1)(b.1)^{-1} = (c.1)(d.1)^{-1}$$

— φ — ХММ

$$\varphi\left(\frac{a}{b}+\frac{c}{d}\right)=\varphi\left(\frac{ad+bc}{bd}\right)=\left[(ad+bc).1\right]\left[(bd).1\right]^{-1}=$$

$$=\left[(a.1)(d.1)+(b.1)(c.1)\right](b.1)^{-1}(d.1)^{-1}=$$

$$=(a.1)(b.1)^{-1}+(c.1)(d.1)^{-1}=\varphi\left(\frac{a}{b}\right)+\varphi\left(\frac{c}{d}\right)$$

$$\varphi\left(\frac{a}{b}\cdot\frac{c}{d}\right)=\varphi\left(\frac{a}{b}\right)\varphi\left(\frac{c}{d}\right)$$ Аналог.

— $\operatorname{Ker}\varphi \lhd \mathbb{Q} \xRightarrow{\text{поле}} \operatorname{Ker}\varphi=\{0\},\ \mathbb{Q} \Rightarrow \operatorname{Ker}\varphi=\{0\}$

$\varphi\left(\frac{a}{b}\right)=0\ \forall$

$\Rightarrow$ φ е влагане.

$\operatorname{Im}\varphi \cong \mathbb{Q}/\{0\} \cong \mathbb{Q} \Rightarrow \operatorname{Im}\varphi$ — просто

подполе на F

$\mathbb{Q} \cong \operatorname{Im}\varphi$ — простото подполе на F

2) char $F = p$

$$\varphi : \mathbb{Z}_p \longrightarrow F$$

$$\bar{k} \longmapsto k.1$$

$k \in \mathbb{Z}$ → коректност: $\bar{k} = \bar{l} \Rightarrow p \mid k - l \Rightarrow k.1 = l.1$

φ - ХММ $\quad \varphi(\bar{k} + \bar{l}) = \varphi(\overline{k+l}) = (k+l).1 = k.1 + l.1$

$\varphi(\bar{k}\bar{l}) = \ldots = \varphi(\bar{k})\varphi(\bar{l})$

$\operatorname{Ker} \varphi = \{\bar{0}\} \quad (k.1 = 0 \Rightarrow p \mid k \Rightarrow \bar{k} = \bar{0})$

$\operatorname{Im} \varphi \cong \mathbb{Z}_p \Rightarrow \operatorname{Im} \varphi$ – просто подполе на F, $\cong \mathbb{Z}_p$

Сл. F - просто поле $\Rightarrow$ $F \cong \mathbb{Q}$ $(\operatorname{char} F = 0)$ или

$F \cong \mathbb{Z}_p$ $(\operatorname{char} F = p)$

Полиноми на една променлива

K - комутативен пръстен с 1

$$K^{\mathbb{N}} = \{ f : \mathbb{N} \cup \{0\} \to K \} = \{ \{ \underbrace{f(i)}_{\in K} \}_{i=0}^{\infty} \} = \{ (\underbrace{\overset{f_0}{f(0)}}_{\in K}, \overset{f_1}{f(1)}, \dots) \}$$

Зад. $f \to \sum_{i=0}^{\infty} f_i x^i \;;\; g \to \sum_{i=0}^{\infty} g_i x^i$

$$f+g \to \sum_{i=0}^{\infty} (f_i + g_i) x^i \;;\; fg \to \sum_{i=0}^{\infty} \Big(\sum_{j+k=i} f_j g_k \Big) x^i$$

$f, g \in K^{\mathbb{N}}$

$h := f + g$; $\forall i \in \mathbb{N} \cup \{0\}$ $\quad h_i = f_i + g_i$

$s = fg$: $\forall i \in \mathbb{N} \cup \{0\}$ $\quad s_i = \sum\limits_{j+k=i} f_j \cdot g_k$

$$s_i = \sum_{j=0}^{i} f_j \cdot g_{i-j} = \sum_{k=0}^{i} f_{i-k}\, g_k$$

<u>Тв.</u> $(K^{\mathbb{N}}, +, \cdot)$ – ком. пр. с 1

<u>Д-во</u> $+$ ... – ясно

асоциативност на $\cdot$

$f, g, h \in K^{\mathbb{N}}$

$i \in \mathbb{N} \cup \{0\}$

$$[(fg)h](i) = \sum_{j+k=i} (fg)(j) \cdot h_k =$$

$$= \sum_{j+k=i} \left(\sum_{p+q=j} f_p g_q \right) h_k = \sum_{p+q+k=i} f_p g_q h_k =$$

$$= \dots = [f(gh)](i)$$

дистрибутивності — аналог.

комутативності

единичен ел. e $(1,0,0,\dots) = e \mid e(i) = \begin{cases} 1 & i=0 \\ 0 & i\neq 0 \end{cases}$

<u>Опр:</u> $K^{\mathbb{N}} = K[[x]]$ – пръстен от формални степенни редове с коефиц. от K

$x = (0,1,0,\dots)$; $x(i) = \begin{cases} 1 & i=1 \\ 0 & i\neq 1 \end{cases}$

$$x^2 = x \cdot x \quad x^2(i) = \sum_{j+k=i} x(j)\cdot x(k) = \begin{cases} 1 & i=2 \\ 0 & i\neq 2 \end{cases}$$

$x^2 = (0,0,1,0,\dots)$

По инд. $x^n(i) = \begin{cases} 1 & i=n \\ 0 & i\neq n \end{cases}$