Dziedziny z jednoznacznością rozkładu.

Def. Dziedzina całkowitości P nazywamy dziedziną z jednoznacznością rozkładu gdy:

Dwa elementy nierozkładalne $p_1, p_2 \dots p_k, q_1, q_2 \dots q_l \in P$ jeśli $\prod_{i=1}^{k} p_i = \prod_{i=1}^{l} q_i$ to

- $k = l$
- po pewnym przenumerowaniu elementów $p_1 \dots p_k$ mamy $(\forall i)\ p_i \sim q_i$

Tw. Każda dziedzina ideałów głównych jest dziedziną z jednoznacznością rozkładu. NP $(\mathbb{Z}, +, \cdot)$

Fakt. Niech P dziedzina z jedn. rozkład. oraz, $n = a \cdot \prod_{i=1}^{k} p_i^{\alpha_i}$, $m = b \cdot \prod_{i=1}^{k} p_i^{\beta_i}$ takie, że

$a, b \in P^*$ p_i - nierozkładalne, $\forall i \neq j$ $p_i \not\sim p_j$.

Wtedy: $n \mid m \iff (\forall i=1..k)\ \beta_i \geq \alpha_i$.

D-d. ćw.

Fakt Niech P dziedzina z j.r. $a \in P$.
Wtedy a pierwszy $\iff$ a nierozkładalny

D-d. ćw

NWD, NWW.

Przykład $NWD(15,9) = \{3, -3\}$

$NWW(15,9) = \{45, -45\}$

Fakt. Niech P - dziedzina jedn. rozkł.

$n = a \cdot \prod_{i=1}^{k} p_i^{\alpha_i}$, $m = b \cdot \prod_{i=1}^{k} p_i^{\beta_i}$. Wtedy:

a, b, p_i jak wyżej

$NWD(n,m) \ni \prod_{i=1}^{k} p_i^{\min\{\alpha_i, \beta_i\}}$

$NWW(n,m) \ni \prod_{i=1}^{k} p_i^{\max\{\alpha_i, \beta_i\}}$

Uwaga. Dla P, m, n jw. Wtedy $NWD(n,m) \cdot NWW(n,m) \ni n \cdot m$

D-d. $NWD(n,m) \cdot NWW(n,m) \ni \prod_{i=1}^{k} p_i^{\min\{\alpha_i,\beta_i\}} \cdot \prod_{i=1}^{k} p_i^{\max\{\alpha_i,\beta_i\}} =$

$\prod_{i=1}^{k} p_i^{\min\{\alpha_i,\beta_i\} + \max\{\alpha_i,\beta_i\}} = \prod_{i=1}^{k} p_i^{\alpha_i+\beta_i} = \prod_{i=1}^{k} p_i^{\alpha_i} \cdot \prod_{i=1}^{k} p_i^{\beta_i} \sim$

$a \prod_{i} p_i^{\alpha_i} \cdot b \prod_{i} p_i^{\beta_i} = m \cdot n$

Więc $m \cdot n \in NWD(n,m) \cdot NWW(n,m)$ □

1 2 3 4 5 6 7 8 9 10 11 12

D. Euklidesowe $\subseteq$ D. ideał głównych $\subseteq$ D. jednozn. rozł. $\subseteq$ D. całkowitości

Sito Eratostenesa	$\forall p,q$ - pierwszych $\exists x,y$ $px+qy=1$	• pierwszy $\equiv$ nierozkładalny • jednoznaczność rozkładu • $NWD(m,n) =$	pierwszy $\Rightarrow$ nierozkł. $xy \in NWD(m,n)$	element pierwszy element nierozkł. NWD NWW
Algorytm Euklidesa.	$NWD(m,n)$ - generator ideału $\langle m,n \rangle$	$\prod_{p \in \mathbb{P}} p^{\min\{\alpha_m(p), \alpha_n(p)\}}$ • $NWD(m,n)\,NWD(n,n) \sim mn$	$x \sim y$	

CIAŁA.

Def. Ciałem nazywamy pierścień przemienny z 1 taki że $P^* = P \setminus \{0\}$.

Przykład $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_p, +_p, \cdot_p)$ $p \in \mathbb{P}$. ~~$(\mathbb{Z}, +, \cdot)$~~

Def. Niech K ciało. Charakterystyką ciała nazywamy liczbę naturalną

$$\operatorname{char}(K) = \begin{cases} \min\{n \in \mathbb{N}^+, \underbrace{1+1+\dots+1}_{n\text{x}} = 0\} & \text{o ile } \neq 0 \\ 0 & \text{przeciwnie.} \end{cases}$$

Przykład $\operatorname{char}(\mathbb{C}) = \operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{Q}) = 0$.

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

Fakt. Niech K - ciało. Wtedy $\operatorname{char}(K) \in \mathbb{P} \cup \{0\}$

D-d. Załóżmy nie wprost, że dla pewnego ciała K

$$\operatorname{char}(K) = m \cdot n \quad , \quad m, n > 1 \quad m, n \in \mathbb{N}$$

Wtedy $\underbrace{1+1+\dots+1}_{m \cdot n \text{ x}} = 0$

$$\# \quad \underbrace{(1+1+\dots+1)}_{m} + \underbrace{(1+1+\dots+1)}_{m} + \dots + \underbrace{(1+1+\dots+1)}_{m} = 0$$

$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{n\text{x}}$$

Zauważmy: $\underbrace{1+1+\dots+1}_{m} \neq 0$, bo $\dots$ minimalność $m \cdot n$

oznaczmy $\underbrace{1+1+\dots+1}_{m} = a \neq 0$

$\#$: $\underbrace{a + a + \dots + a}_{n} = 0 \quad | \cdot a^{-1}$

$\underbrace{1+1+\dots+1}_{n} = 0$ Sprzeczność bo $n < n \cdot m = \operatorname{char}(K)$ $\square$

Def. Niech K - ciało. $L \subseteq K$ nazywamy podciałem, gdy:

$\forall a,b \in L \quad a+b,\ -a,\ a \cdot b,\ a : b = a \cdot b^{-1} \in L$ ($b \neq 0$)

Zapisujemy $L \leq K$

Przykład

$\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

Fakt. Niech K ciało charakterystyki $p \in \mathbb{P}$.
Wtedy istnieje $L \leq K$ takie, że $L \cong \mathbb{Z}_p$. (izomorf. jako pierścienie)

D-d.

Niech $L = \{1, 1+1, 1+1+1, \ldots, \underbrace{1+1+\ldots+1}_{p} = 0\}$

ozn. $k = \underbrace{1+1+\ldots+1}_{k\times}$

Zauważmy
$$\left.\begin{array}{l} k+l = k +_p l \\ k \cdot l \quad k \cdot_p l \\ L = \{0, \ldots, p-1\} \end{array}\right\} \quad L \cong \mathbb{Z}_p.$$

□

Wniosek. Każde ciało skończone ma charakterystykę $p \in \mathbb{P}$ wtedy zawiera podciało izomorf z $\mathbb{Z}_p$.

Fakt Niech $L \geq K$ ciała. Wtedy
L jest przestrzenią liniową nad K.

Działania 1. dodawanie wektorów to zwykłe dodawanie z ciała L
2. mnożenie przez skalar $\cdot : K \times L \to L$
to obcięcie mnożenia z ciała L do zbioru $K \times L$

Przykład $\mathbb{C}$ jest przestrzenią liniową nad $\mathbb{R}$.
Baza $\{1, i\}$, $\dim(\mathbb{C}/\mathbb{R}) = 2$

D-d. Należy sprawdzić że zachodzi def przestrzeni liniowej:

- $(L, +)$ jest grupą abelową, TAK bo L jest ciałem.
- $\forall k, l \in K$, $v \in L$ $\quad (k+l)\cdot v = kv + l\cdot v$, bo

  $k, l, v \in L$ - ciało, równość wynika z rozdziel mnoż/+.
- Pozostałe ćw. $\square$.

Koment. Niech V skończona przestrzeń liniowa nad K - skończone.
Niech $\mathcal{B} = \{b_1 \dots b_n\}$ - baza V $\quad |K| = k \in \mathbb{N}$

Wtedy $|V| = |\{k_1 b_1 + k_2 b_2 + \dots + k_n b_n : k_i \in K\}| = k^n$

Fakt Niech K ciało skończone, $\operatorname{char}(K) = p \in \mathbb{P}$.
Wtedy $|K| = p^n$ dla pewnego $n \in \mathbb{N}$.

D-d. K jest charakterystyki p to $\mathbb{Z}_p \leq K$.

Więc K jest przestrzenią liniową nad $\mathbb{Z}_p$
Niech $n = \dim(K / \mathbb{Z}_p)$
Wtedy

$$|K| = |\mathbb{Z}_p|^n = p^n$$

$\square$

Wniosek. NIE istnieją ciała 6, 12, 93, 14, ... elementowe