Przypomnienie: $I = (f_1, \dots, f_s) \triangleleft k[\bar{X}]$, $\bar{X} = (X_1, \dots, X_n)$.

(ciało $\to k$)

Dany $f \in k[\bar{X}]$. Czy $f \in I$?

$$\Updownarrow$$

$$f = \sum g_i f_i, \quad g_i \in k[\bar{X}]$$

$$f = \sum_{\bar{\beta}} a_{\bar{\beta}} X^{\bar{\beta}}, \quad a_{\bar{\beta}} \in k$$

$\bar{\beta} = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$ wieloindeks

$X^{\bar{\beta}} = X_1^{\beta_1} \dots X_n^{\beta_n}$

$$\Pi^n = \{X^{\bar{\beta}} : \bar{\beta} \in \mathbb{N}^n\} \xleftrightarrow[\text{na}]{1-1} \mathbb{N}^n$$

$$X^{\bar{\beta}} \longleftrightarrow \bar{\beta}$$

Jak dzielić z resztą w $k[\bar{X}]$?

Def. 13.2. (1) $\leq_0$: porządek na $\mathbb{N}^n$, po osiach:

$\bar{\alpha} \leq \bar{\beta} \iff \alpha_i \leq \beta_i$ dla $i = 1, \dots, n$.

(2) $\preccurlyeq$: porządek liniowy na $\mathbb{N}^n$ jest <u>dopuszczalny</u>, gdy:

(a) $\bar{0}$: najmniejszy

(b) $\bar{\alpha} \preccurlyeq \bar{\beta} \Rightarrow \bar{\alpha} + \bar{\gamma} \preccurlyeq \bar{\beta} + \bar{\gamma}$

(3). $\preccurlyeq \rightsquigarrow \prec$ ścisła wersja

- $\preccurlyeq$ na $\mathbb{N}^n$ indukuje $\preccurlyeq$ na Π^n (przez $\Pi^n \longleftrightarrow \mathbb{N}^n$)

Uwaga 13.3. $\preccurlyeq$: dopuszczalny $\Rightarrow \preccurlyeq$ dobry (i $ot(\mathbb{N}^n, \preccurlyeq) \leq \omega^n$)

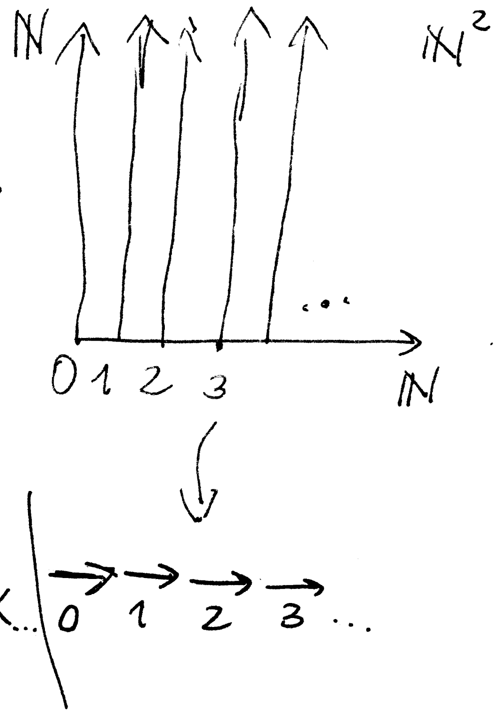
<u>Przykłady</u>:

1. $\prec_{lex}$ na $\mathbb{N}^n$, $\mathbb{T}^n$

leksykograficzny $\langle 2,3\rangle \longleftrightarrow x_1^2 x_2^3$

<u>wsc np</u> $\langle 0,1\rangle \prec_{lex} \langle 1,0\rangle$

tzn: $x_2 \prec_{lex} x_1$



$\prec_{lex}$ na $\mathbb{T}^2$:

$(1 \prec x_2 \prec x_2^2 \prec \ldots) \prec (x_1 \prec x_1x_2 \prec x_1x_2^2 \prec \ldots) \prec \ldots$

2. stopniowo-leksykograficzny:

$\prec_{deglex}$ na $\mathbb{T}^n$, $\mathbb{N}^n$:

$$x^{\bar\alpha} \prec_{deglex} x^{\bar\beta} \overset{def}{\Longleftrightarrow} \left[\deg x^{\bar\alpha} < \deg x^{\bar\beta} \vee \left(\deg x^{\bar\alpha} = \deg x^{\bar\beta} \wedge x^{\bar\alpha} \prec_{lex} x^{\bar\beta}\right)\right]$$

Ustalamy $\preceq$: dopuszczalny na $\mathbb{N}^n$, $\mathbb{T}^n$.

$$k[\bar X] \ni \underset{\underset{0}{\#}}{f}(\bar X) = a_1 x^{\bar\alpha_1} + a_2 x^{\bar\alpha_2} + \ldots + a_r x^{\bar\alpha_r},$$

$$\bar\alpha_1 \succ \bar\alpha_2 \succ \ldots \succ \bar\alpha_r, \quad a_i \in k.$$

- $lp(f) = x^{\bar\alpha_1}$: jednomian wiodący w f
- $lc(f) = a_1$: współczynnik wiodący w f
- $lt(f) = a_1 x^{\bar\alpha_1}$: wyraz wiodący w f.

Dzielenie z resztą wg $\prec_0$:

Def. 13.4. ($f, \overset{\neq 0}{g}, h \in k[\bar{X}]$)

$f \xrightarrow{g} h$ (f redukuje się do h modulo g, w 1 kroku),

gdy : $lp(g)$ dzieli pewien niezerowy wyraz v w f

oraz $h = f - \frac{v}{lt(g)} g$

tzn: h powstaje z f przez : $\begin{cases} \text{usunięcie z } f \text{ wyrazu } v \\ \text{k wyrazy } v' \text{ z } f \text{ t.że } v' \succ v \\ \quad \text{bez zmiany} \end{cases}$

<u>Przykład</u> ($\prec = lex)_2$

$f = 6x_1^2x_2 - x_1 + 4x_2^3 - 1 \qquad g = \underbrace{2x_1x_2}_{lt(g)} + x_2^3$

$v = 3x_1 \cdot lt(g)$

$h = f - 3x_1 g = -3x_1x_2^3 - x_1 + 4x_2^3 - 1.$

Def. 13.5. ($f, h, \overset{\neq 0}{f_1}, \dots, \overset{\neq 0}{f_s} \in k[\bar{X}]$, $F = \{f_1, \dots, f_s\}$)

$f \xrightarrow{F}_+ h$ (f redukuje się do h modulo F), gdy :

$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \dots h_{t-1} \xrightarrow{f_{i_t}} h$ dla pewnego t i pewnych $i_1, \dots, i_t$, $h_1, \dots, h_{t-1}$.

• gdy h już dalej nie można redukować mod F : (nieredukowalny)

$h = r_F(f)$: pełna redukcja f modulo F.

(Ćw) $r_F(f)$ wyznaczona jednoznacznie.

Przykład $f_1 = x_1x_2 - x_2$, $f_2 = x_2^2 - x_1 \in \mathbb{Q}[X_1, X_2]$

$< \,=\, <_{deglex}$ $F = \{f_1, f_2\}$, $f = x_1x_2^2$

$$x_1x_2^2 \xrightarrow{f_1} x_2^2 \xrightarrow{f_2} x_1 \qquad x_1 = r_F(f).$$

$$x_1x_2^2 - x_2f_1 = x_2^2 \qquad x_2^2 - 1\cdot f_2 = x_1$$

Def. 13.6. ($I \lhd k[\bar{X}]$, $G = \{g_1, \ldots, g_t\} \subseteq I \setminus \{0\}$).

G: baza Gröbnera ideału I, gdy:

$(\forall f \in I \setminus \{0\})(\exists i \in \{1, \ldots, t\})\ lp(g_i) \mid lp(f)$.

Def. 13.7. Dla $S \subseteq k[\bar{X}]$,

$Lt(S) = (\{lt(s) : s \in S\}) \lhd k[\bar{X}]$.

Tw. 13.8. Zał, że $\{0\} \neq I \lhd k[\bar{X}]$, $G = \{g_1, .., g_t\} \subseteq I \setminus \{0\}$.

NWSR:

(1) G: baza Gröbnera dla I.

(2) $\forall f \in k[\bar{X}]\ (f \in I \Leftrightarrow f \xrightarrow{G}_+ 0)$ $\Big\} \Rightarrow I = (G)$

(3) $\forall f \in k[\bar{X}]\ (f \in I \Leftrightarrow f = \sum_{i=1}^{t} h_ig_i$ dla pewnych $h_i \in k[\bar{X}]$

t. że $lp(f) = \max_i (lp(h_i) lp(g_i))$)

(4) $Lt(G) = Lt(I)$.

D-d (ćw)

Wn. 13.9. Jeśli G: baza Gröbnera dla I, to $I = (G)$ i mamy algorytm rozstrzygający, czy
$$f \in I \;\; (\Leftrightarrow \; f \xrightarrow[+]{G} 0).$$

Wn. 13.10 $\forall I \triangleleft k[\bar{X}] \; \exists G$: baza Gröbnera dla I.

<u>D-d</u>. Niech $G \underset{\text{sk.}}{\subseteq} I$ t.że $Lt(G) = Lt(I)$.

Niech $I = (f_1, \dots, f_s) \triangleleft k[\bar{X}]$. Problem: Jak znaleźć bazę Gröbnera dla I?

Def. 13.11.

Niech $f, g \in k[\bar{X}] \setminus \{0\}$, $\underset{\mathbb{T}^n}{\ell} = NWW(lp(f), lp(g))$
$$S(f,g) = \frac{\ell}{lt(f)} \cdot f - \frac{\ell}{lt(g)} \cdot g$$
S-wielomian dla pary (f,g), wielomian syzygii.

Lemat 13.12. Zał, że $f_1, \dots, f_s \in k[\bar{X}]$, $\bar{0} \neq \bar{\beta} \in \mathbb{N}^n$, $lp(f_i) = x^{\bar{\beta}}$ dla $i = 1, \dots, s$.
Niech $f = \sum_{i=1}^{s} \underset{k}{c_i} f_i$. Jeśli $lp(f) < x^{\bar{\beta}}$, to $f = \sum_{i<j} \underset{k}{d_{ij}} S(f_i, f_j)$

Tw. 13.13. (Buchberger, ~1964). Niech $G = \{g_1, \dots, g_t\} \subseteq k[\bar{X}]$, $g_i \neq 0$.
Wtedy G: baza Gröbnera dla $I = (G) \Leftrightarrow$
$$\forall i \neq j \;\; S(g_i, g_j) \xrightarrow[+]{G} 0.$$

Algorytm Buchbergera.

Dane $I=(f_1,\dots,f_s) \triangleleft k[\bar{X}]$. Cel: baza Gröbnera G dla I.

Konstruujemy $H_0 \subseteq H_1 \subseteq H_2 \subseteq \dots$ (skończone) rekurencyjnie.

- $H_0 = \{f_1,\dots,f_s\}$
- Zał., że H_n dane.

  1°. dla pewnych $f \neq g \in H_n$ $\quad h_{f,g} := r_{H_n}(S(f,g)) \neq 0$

  Wtedy $H_{n+1} = H_n \cup \{h_{f,g}\}$.

  2°. Jeśli $\neg 1°$, to STOP i $G = H_n$.

To działa

1. Algorytm się zatrzymuje, bo:

jeśli nie, to dostajemy $H_0 \subsetneq H_1 \subsetneq H_2 \subsetneq \dots$ nieskończony.

Niech $I_n = Lt(H_n) \triangleleft k[\bar{X}]$

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$$

- $I_n \neq I_{n+1}$, bo: niech $h \in H_{n+1} \setminus H_n$. $h = h_{f,g}$ dla pewnych $f \neq g \in H_n$
- $lt(h) \in I_{n+1}$, $lt(h) \notin I_n$

  (bo jeśli $lt(h) \in I_n$, to h można zredukować mod H_n)

sprzeczność z noetherowskością $k[\bar{X}]$.

2. Gdy algorytm się zatrzyma, to $G = H_n$: baza Gröbnera dla I (tw. 13.13)

Metoda Kroneckera.

R: dziedzina nieskończona t.że
$(\forall a \in R \setminus \{0\})$ a ma skończenie wiele podzielników w R

Przykład $\mathbb{Z}$, $\mathbb{Z}[\sqrt{d}]$ $(d<0)$

Dla takich R można efektywnie stwierdzić, czy $f \in R[X]$ jest nierozkładalny (w $R_0[X]$). BSO f: pierwotny $(1 = c(f))$ $\Leftrightarrow$ w $R[X]$ ← Lemat Gaussa

- Zał, że f: rozkładalny (w $R_0[X]$),

$$f = g(X) \cdot h(X), \quad g, h \in R_0[X], \ \deg g, \deg h > 0.$$

Niech $k = \lfloor \frac{1}{2} \deg(f) \rfloor$. Np. $\deg g \leq k$.

Niech $c_0, \dots, c_k \in R$ t.że $f(c_i) \neq 0$.

$$f(c_i) = g(c_i) \cdot h(c_i) \Rightarrow g(c_i) \mid f(c_i) \text{ w } R.$$

Niech $(d_0, \dots, d_k)$: układ dzielników $(f(c_0), \dots, f(c_k))$ (odpowiednio)

[takich układów jest skończ. wiele]

Niech $W(X) \in R_0[X]$: wielomian interpolacyjny Lagrange'a:
$W(c_i) = d_i$, $i = 0, \dots, k$ $\quad \deg W \leq k$ (patrz lista ~~13~~ 12)

g musi być $= W$ dla pewnego takiego W

Metoda polega na sprawdzeniu, czy któreś W należy do $R[X]$ i czy wtedy dzieli f w $R[X]$.

Wn. 14. 1. Metodę można stosować do pierścieni

$R' = R[X],\ R[X_1, X_2],\ R[X_1, X_2, X_3], \dots$

(algorytm pokazuje, że pierścienie ~~te~~ R' też mają żądaną własność)

~~Przykład. Czy $f(X) = X^5 - 3X^4 + 3X^3$~~

Wn. 14.2. W ten sposób można znajdować rozkłady wielomianów w $\mathbb{Q}[X_1, \dots, X_n]$ lub $R_0[X_1, \dots, X_n]$, gdy dodatkowo R: UFD.

Przykład.

Czy $f(X) = X^5 - 3X^4 + 3X^3 + 2X^2 - 8X + 3$ jest rozkładalny w $\mathbb{Q}[X]$?

$\Updownarrow$

—— || —— w $\mathbb{Z}[X]$

$k = \lfloor \frac{5}{2} \rfloor = 2.\quad c_0 = 0,\ c_1 = 1,\ c_2 = 2$

	$f(c_0) = 3$	$f(c_1) = -2$	$f(c_2) = 3$	
dzielniki:	± 3	± 2	± 3	64 wybory
w $\mathbb{Z}$	± 1	± 1	± 1	(d_0, d_1, d_2)
	d_0	d_1	d_2	

Ale: gdy $(d_0', d_1', d_2') = -(d_0, d_1, d_2)$, to

$W' = -W$, więc $W' \sim W$ w $\mathbb{Z}[X]$

wystarczy rozpatrzyć 32

Ze wzoru Lagrange'a:

$$W(X) = \frac{d_0}{2}(X-1)(X-2) - d_1 X(X-2) + \frac{d_2}{2} X(X-1) =$$

$$\left[\text{wzór: } W(X) = \sum_{i=0}^{k} d_i \cdot \frac{\prod_{j \neq i}(X - c_j)}{\prod_{j \neq i}(c_i - c_j)},\quad W(c_i) = d_i \right]$$

$$= \left(\frac{d_0+d_2}{2} - d_1\right)X^2 + \left(2d_1 - \frac{3d_0+d_2}{2}\right)X + d_0$$

dla $d_0=3,\ d_1=2,\ d_2=3$ $\longleftarrow$ tylko jedna z tych 32 możliwości

$\Downarrow$

$W(X) = (X^2-2X+3) \mid f(X)$ $\longleftarrow$ jedyny podzielnik f stopnia ≤ 2, oraz

$\Leftarrow$

$f(X) = (X^2-2X+3)(X^3-X^2-2X+1)$

nierozkładalne, bo: $X^2-2X+3 \nmid X^3-X^2-2X+1$

Chińskie tw. o resztach:

$k_1,\dots,k_r \in \mathbb{Z}^+$ parami wzgl. pierwsze, $l_1,\dots,l_r \in \mathbb{Z}$, $0 \leq l_i < k_i$.

<u>Wtedy</u> $\exists n \in \mathbb{Z}\ \forall i=1,\dots,r\ \ n \equiv l_i \pmod{k_i}$

Ogólniej:

R: pierścień przemienny z $1 \neq 0$, $I \triangleleft R$, $a, b \in R$

$$a \equiv b \pmod I \overset{\text{def}}{\iff} a-b \in I \iff a+I = b+I.$$

Tw. 14.3. (chińskie tw. o resztach)

Załóżmy, że $I_1,\dots,I_r \triangleleft R$ t. że $\forall i \neq j\ \ I_i + I_j = R$, oraz $l_1,\dots,l_r \in R$.

Wtedy $\exists n \in R\ \forall i=1,\dots,r\ \ n \equiv l_i \pmod{I_i}$

<u>D-d</u> Indukcja wzgl. r.

1° $r=1$ jasne. $n=l_1$ dobre

2° $r=2$: $R = I_1 + I_2$, $1 = a_1 + a_2$ ($1 \in R$, $a_1 \in I_1$, $a_2 \in I_2$) $\Longrightarrow$ $a_1 \equiv 1 \pmod{I_2}$, $a_2 \equiv 1 \pmod{I_1}$

$\Downarrow$

$n = l_2 a_1 + l_1 a_2$ dobre.

2°. Krok indukcyjny: Zał, że $r > 2$ i dla $r' < r$ teza zachodzi. AII 13/10

• dla $i = 1, \ldots, r-1$: $I_i + I_r \in R$

$$\underset{a_i}{\underset{\cup}{ }} + \underset{b_i}{\underset{\cup}{ }} = 1$$

$$\Rightarrow 1 = \prod_{i=1}^{r-1} (a_i + b_i) \equiv a_1 \cdot \ldots \cdot a_{r-1} \pmod{I_r}$$

$\cap$ $I_1 \cdot \ldots \cdot I_r$, więc $1 \in \underbrace{(I_1 \cdot \ldots \cdot I_{r-1})}_{I \triangleleft R} + I_r = R$

Z zał. indukc. istnieje $m_r \in R$ t. że:

$$\begin{cases} m_r \equiv 0 \pmod{(I_1 \cdot \ldots \cdot I_{r-1})} \\ m_r \equiv 1 \pmod{I_r} \end{cases} \qquad (I_1 \cdot \ldots \cdot I_{r-1}) \subseteq \bigcap_{i=1}^{r-1} I_i.$$

więc $m_r \in \bigcap_{j \neq r} I_j$.

Analogicznie: $(\exists m_i \in \bigcap_{j \neq i} I_j)\ m_i \equiv 1 \pmod{I_i}$
dla $i = 1, \ldots, r$

$$n := m_1 l_1 + \ldots + m_r l_r \equiv l_i \pmod{I_i}. \quad \square$$

Pierścienie wielomianów jako "algebry wolne"

R: pierścień przemienny z $1 \neq 0$.

Lemat 14.4. Zał, że $f: R \longrightarrow R_1$ homomorfizm p. z 1.
$g: \{X_1, \ldots, X_n\} \longrightarrow R_1$ dowolna. Wtedy

$\exists!\ f': R[X_1, \ldots, X_n] \longrightarrow R_1$ homomorfizm pierścieni.
$\cup$
$f \cup g$

D-d $f'(W(X_1, \ldots, X_n)) = f(W)(g(X_1), \ldots, g(X_n))$ $\square$

Wn. 14.5. Każdy pierścień przemienny R jest homomorficznym obrazem $\mathbb{Z}[\overline{X}]$ dla pewnego $\overline{X}$.
pierścienia

D-d. Niech $A = \{a_i : i \in I\}$ zbiór generujący R (jako pierścień)
(np. $A = R$ dobry)

$f : \mathbb{Z} \to R$, $f(n) = n \cdot 1_R$ homomorfizm pierścieni.

$g : \{X_i : i \in I\} \to R$, $g(X_i) = a_i$.

$$f' : \mathbb{Z}[X_i : i \in I] \xrightarrow[\text{epi}]{} R$$

$\cup\!|$

$f \cup g$

Ciała

Def. 14.6. (1) $(F, +, \cdot)$ ciało, gdy

(a) $(F, +)$ gpa abelowa (tzw. gpa addytywna ciała F)
0: el. neutralny, zero ciała.

(b) $(F \setminus \{0\}, \cdot)$: gpa abelowa (tzw. gpa multiplikatywna ciała F)
1 : el. neutralny, jedność ciała F.

(c) $\cdot$ rozdzielne wzgl. $+$

W szczególności ciało F to pierścień przemienny z $1 \neq 0$ w którym $F^* = F \setminus \{0\}$.

(2) $F_1 \subseteq F$ podciało ciała F, gdy F_1 : ciało względem działań $+, \cdot$ z F.

Wtedy: $0_{F_1} = 0_F$, $1_{F_1} = 1_F$

Def. 14.7. (F : ciało)

$$\operatorname{char} F \doteq \begin{cases} \operatorname{ord}(1) \text{ w } (F,+), & \text{gdy } \operatorname{ord}(1) < \infty \\ 0, & \text{w p.p.} \end{cases}$$

charakterystyka

<u>Przykłady</u> · $\mathrm{char}\,\mathbb{Q} = \mathrm{char}\,\mathbb{R} = \mathrm{char}\,\mathbb{C} = 0$

$\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

podciała

· $\mathrm{char}\,\mathbb{Z}_p = p = \mathrm{char}(\underbrace{\mathbb{Z}_p(X)}_{\text{nieskończone}})$

· $\mathrm{char}\,\mathbb{Z}_3[X]/(X^3+2X+1) = 3$

X^3+2X+1 nierozkładalny w $\mathbb{Z}_3[X] \Rightarrow \mathbb{Z}_3[X]/(X^3+2X+1)$ ciało.

Uwaga 14.8.

Jeśli $\mathrm{char}\,F = n > 0$, to n: l. pierwsze i dla każdego ~~Dla ka~~ $x \in F$, $n \cdot x = \underbrace{x + \ldots + x}_{n} = 0$.

<u>D-d</u> . . $\underbrace{x + \ldots x}_{n} = \underbrace{x \cdot 1 + \ldots + x \cdot 1}_{n} = x(\underbrace{1 + \ldots + 1}_{n}) = x \cdot 0 = 0$

· Zał. nie wprost, że n ~~...~~ nie jest pierwsze. $n > 1$, więc n: złożona

$n = m \cdot k, \quad 1 < m, k < n$

Niech $\overset{\neq 0}{a} = \underbrace{1 + \ldots + 1}_{m}$, $\overset{\neq 0}{b} = \underbrace{1 + \ldots + 1}_{k}$. Wtedy

$0 \neq a \cdot b = (\underbrace{1 + \ldots + 1}_{m})(\underbrace{1 + \ldots + 1}_{k}) = \underbrace{1 \cdot 1 + \ldots + 1 \cdot 1}_{m \cdot k} = 0$, ~~...~~ ↯.

Uwaga. Jeśli $F_1 \subseteq F$ podciało, to $\mathrm{char}\,F_1 = \mathrm{char}\,F$.

Uwaga 14.9. Zał, że $n > 0$ i $\mathrm{char}\,F \nmid n$. Wtedy

$\forall x \in F\ \exists! y \in F \quad n \cdot y = x$

<u>D-d</u> ćw.

Lemat 14.10.

(1) Zał., że char $F = p > 0$. Wtedy ciało F zawiera podciało $F' \cong \mathbb{Z}_p$

(2) Zał., że char $F = 0$. Wtedy — // — ... $F' \cong \mathbb{Q}$.

D-d (1). Niech $F' = \{0, 1, 1+1, \dots, \underbrace{1+\dots+1}_{p-1}\} = \langle 1 \rangle < (F, +)$.

- $(F', +) \cong (\mathbb{Z}_p, +_p)$
- F' zamkn. na $\cdot$: $(n \cdot 1) \cdot (m \cdot 1) = nm \cdot 1 = r_p(nm) \cdot 1 \in F'$.
- $f : \mathbb{Z}_p \to F'$, $n \overset{f}{\longmapsto} n \cdot 1$ $\quad$ f: izomorfizm struktur (ćw.) więc: F': ciało $\cong \mathbb{Z}_p$.

(2) ćw. (podobny argument:

char $F = 0 \Rightarrow \forall m > 0 \ \exists! y \in F \ m \cdot y = 1$.

dla $\frac{n}{m} \in \mathbb{Q}$ niech $\frac{n}{m} \cdot 1_F \overset{def}{=} \underline{n \cdot y}$.

$f : \mathbb{Q} \to F$ $\quad f\left(\frac{n}{m}\right) = \frac{n}{m} \cdot 1_F \quad f : \mathbb{Q} \xrightarrow{\cong} f[\mathbb{Q}] = F'$.

Uwaga Podciało $F' \subseteq F$ z Lematu 14.10: najmniejsze podciało ciała F.

Def. 14.11. (F ciało). F: ciało proste $\Leftrightarrow$ F nie ma podciał właściwych.

Uwaga 14.12

(1) Z dokł. do $\cong$ wszystkie ciała proste to $\mathbb{Z}_p$ ($p = 2, 3, 5, \dots$) i $\mathbb{Q}$.

(2) Każde ciało F zawiera jedyne podciało proste.

Tw. 14.13.
Zał, że char $F = p > 0$ i F: skończone. Wtedy $|F| = p^n$ dla pewnego $n > 0$.

D-d Niech $F_0 \subseteq F$ podciało proste. Wtedy (lemat 14.10(1))
$F_0 \cong \mathbb{Z}_p$, $|F_0| = p$.

Ogólniej:
$F_1 \subseteq F_2$: rozszerzenie ciał $\Rightarrow$ F_2: przestrzeń liniowa nad F_1:

$$F_2 = (F_2, +, 0, r\cdot)_{r \in F_1}$$
$$\underset{F_2}{\underset{\cap}{r \cdot x}} = r \circ x \text{ liczone w } F_2.$$

np: $\mathbb{R}$: p. liniowa $/\mathbb{Q}$
(baza: tzw. baza Hamela)

U nas: F: przestrzeń liniowa nad F_0
Niech $n = \dim_{F_0} F < \infty$ (bo F: skończone

$\Rightarrow F \cong \underbrace{F_0 \times \ldots \times F_0}_{n}$, więc $|F| = p^n$.
($|F_0| = p$)

Uwaga (p: l. pierwsza) Dla każdego $n > 0$ istnieje jedyne ciało F_{p^n} t. że $|F_{p^n}| = p^n$ (z dokł. do $\cong$)

Uwaga $f: \underset{\text{ciała}}{F_1 \longrightarrow F_2}$ homomorfizm ~~ciał~~ struktur $\Rightarrow f \equiv 0$ lub f: monomorfizm.

D-d $\operatorname{Ker} f \lhd F_1 \Rightarrow \operatorname{Ker} f = \{0\}$ lub $\operatorname{Ker} f = F_1$.

Uwaga 14.14. Zał. że char $F = p > 0$. Wtedy w ciele F: $(x+y)^p = x^p + y^p$

D-d $(x+y)^p = x^p + \sum_{i=1}^{p-1} \underbrace{\binom{p}{i} x^{p-i} y^i}_{=0} + y^p = x^p + y^p$

$\mathbb{N} \ni \binom{p}{i} = \frac{p!}{i!(p-i)!}$ $p \mid$ licznik, $p \nmid$ mianownik $\rightarrow p \mid \binom{p}{i}$ dla $i = 1, \ldots, p-1$

Wn. (char $F = p > 0$).

Funkcja $Fr: F \longrightarrow F$ dana wzorem $Fr(x) = x^p$ jest monomorfizmem ciał. (tzw. funkcja Frobeniusa)

Fakt F: ciało skończ. $\Rightarrow F^*$: gpa cykliczna.

Wn. Grupy $\mathbb{Z}_p^* = (\{1, 2, \ldots, p-1\}, \cdot_p)$ są cykliczne.

Wn. (char $F = p > 0$) $F^p = \{x^p : x \in F\}$ podciało ciała F.
Jeśli F: skończone, to $F = F^p$.

D-d $Fr: F \xrightarrow{\cong} F^p \subseteq F$.

przykład:

~~$Fr: F_p(X) \rightarrow$~~

$Fr: \mathbb{Z}_p(X) \longrightarrow \mathbb{Z}_p(X)$
nie jest "na"

Równania w ciałach

$X^2 + 1 = 0$: nie ma rozw. w $\mathbb{R}$
ma rozw: w $\mathbb{C}$ ($\mathbb{R} \subseteq \mathbb{C}$)

Lemat 14.15

Zał, że $W(X) \in F[X]$, $\deg W > 0$. Wtedy istnieje ciało $F_1 \supseteq F$ t. że W ma pierwiastek w F_1.

D-d $W(X) = V_1(X) \cdot \ldots \cdot V_k(X)$

nierozkładalne w $F[X]$.

bso. $W = V_1$ nierozkładalny w $F[X]$.

$$\overset{\shortparallel}{a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0}, \quad a_n \neq 0, \; a_i \in F, \; n > 0.$$

Niech $I = (W) \triangleleft F[X]$, $\quad F_1 = F[X]/I$ ciało

maksymalny

$$\overset{\shortparallel}{\{c_0 + c_1 X + \ldots + c_{n-1} X^{n-1} + I : c_i \in F\}}$$

bez powtórzeń (postać normalna).

Niech $i : F \longrightarrow F_1$, $\quad a \longmapsto a + I$ $\qquad$ i : monomorfizm ciał (ćw.)

$i : F \xrightarrow{\cong} i[F] \subseteq F_1$.

podciało.

Utożsamiamy F z $i[F]$. $\rightsquigarrow F \subseteq F_1$.

Niech $b = X + I \in F_1$.

- w F_1: $W(b) = a_n b^n + \ldots + a_1 b + a_0 = 0$, bo:

$$a_n(X+I)^n + \ldots + a_1(X+I) + a_0 = (a_n X^n + \ldots + a_1 X + a_0) + I = W(X) + I = I = 0 + I = 0.$$

Def. 14.16. Ciało F jest algebraicznie domknięte, gdy każdy $W \in F[X]$ ($\deg > 0$) ma pierwiastek w F.

Tw. Każde ciało F jest podciałem pewnego ciała alg. domkn.

Uwaga 14.17. Ciało algebraicznie domknięte jest nieskończone.

D-d Nie wprost. Zał., że $F = \{a_0, \ldots, a_n\}$ skończone ciało alg. domkn.

$F[X] \ni W(X) = (X - a_0)(X - a_1) \ldots (X - a_n) + 1_F$

nie ma pierwiastka w F $\lightning$.