Wykład 14.

Metoda Kroneckera

sprawdzania, czy wielomian jest nierozkładalny.

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

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

Dla takich R można efektywnie stwierdzić, czy $f \in R[X]$ jest rozkładalny (w $R_0[X]$)

- Zał. że $f \in R[X]$ i f jest rozkładalny (w $R_0[X]$)

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

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

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

$f(c_i) = g(c_i) \cdot h(c_i)$, więc $g(c_i) | f(c_i)$ dla $i = 0, \dots, k$.

- Niech $(d_0, \dots, d_k)$: układ dzielników $f(c_0), \dots, f(c_k)$ (takich układów jest skończenie wiele)

- Niech $W(X) \in R_0[X]$: wielomian interpolacyjny Lagrange'a t. że $W(c_i) = d_i$, $i = 0, \dots, k$, $\deg W \leq k$.

AII.14 (2

g musi być $= W$ dla pewnego takiego W.

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

(skończenie wiele takich W, więc to działa).

Wn. 14.1 Metodę można stosować ~~do~~ również do pierścieni $R[X], R[X_1,X_2], R[X_1,X_2,X_3],\dots$

[Algorytm pokazuje, że jeśli R spełnia założenia metody, to $R[X]$ też]

<u>Przykład</u> Czy $f(X) = X^5-3X^4+3X^3+2X^2-8X+3$ jest rozkładalny w $\mathbb{Q}[X]$, w $\mathbb{Z}[X]$?

Wn. 14.2. Można też znajdować w ten sposób rozkłady w $\mathbb{Q}[X_1,\dots,X_n]$ lub $R_0[X_1,\dots,X_n]$, gdy <u>dodatkowo</u> R: UFD.

<u>Przykład c.d.</u> $\frac{5}{2} = 2.5$, $k=2$

$c_0 = 0$, $c_1 = 1$, $c_2 = 2$.

$f(c_0) = 3$, $f(c_1) = -2$, $f(c_2) = 3$

Podzielniki w $\mathbb{Z}$:

$f(c_0)=3$: $\pm 3, \pm 1$: d_0

$f(c_1)=-2$: $\pm 2, \pm 1$: d_1

$f(c_2)=3$: $\pm 3, \pm 1$: d_2

64 możliwe wybory (d_0, d_1, d_2)

[ale gdy $(d_0', d_1', d_2') = -(d_0, d_1, d_2)$, to

$W' = -W$,

$W' \sim W$, więc wystarczy

rozpatrzyć $\underline{\underline{32}}$]

Ze wzoru Lagrange'a:

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

$$\left[\underset{i=0,\dots,k}{W(c_i)=d_i} \rightsquigarrow W(X) = \sum_{i=0}^{k} \left(d_i \frac{\prod_{j\neq i}(X-c_j)}{\prod_{j\neq i}(c_i-c_j)} \right) \right]$$

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

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

⇓

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

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

nierozkładalne, bo:

$$X^2-2X+3 \nmid X^3-X^2-2X+1$$

Chińskie tw. o resztach:

$k_1,\ldots,k_r \in \mathbb{Z}^+$ parami względnie pierwsze,

$l_1,\ldots,l_r \in \mathbb{Z}$, $0 \le l_i < k_i$. <u>Wtedy</u>

$\exists n \in \mathbb{Z}\ \forall i=1,\ldots,r \quad n \equiv l_i \pmod{k_i}$

$(\Leftrightarrow k_i \mid n-l_i)$

<u>Ogólniej</u>: R: pierścień przemienny z $1 \neq 0$,

$I \triangleleft R$, $a, b \in R$

$a \equiv b \pmod I \iff a-b \in I$

$\iff a+I = b+I$

TW. 14. 3. Załóżmy, że

$I_1,\ldots,I_r \triangleleft R$ t. że $(\forall i \neq j \quad I_i + I_j = R)$ oraz

$l_1,\ldots,l_r \in R$. Wtedy

$(\exists n \in R)(\forall i=1,\ldots,r) \quad n \equiv l_i \pmod{I_i}$

D-d indukcja wzgl. r AII.14 (5

1. $r=1$: $n=l_1$ dobre

2. $r=2$: $\begin{matrix} R & = & I_1 & + & I_2 \\ \Psi & & \Psi & & \Psi \\ 1 & = & a_1 & + & a_2 \end{matrix} \Rightarrow$ $a_1 \equiv 1 (\mathrm{mod}\ I_2), a_2 \equiv 1 (\mathrm{mod}\ I_1)$

$n = l_2 a_1 + l_1 a_2$

dobre.

3. krok indukcyjny : $r > 2$ i zał., że

$\forall r' < r$ jest OK.

$I_1, \ldots, I_r \triangleleft R$, $l_1, \ldots, l_r \in R$

- dla $i = 1, \ldots, r-1$: $\begin{matrix} I_i & + & I_r & = R \\ \Psi & & \Psi & \\ a_i & + & b_i & = 1 \end{matrix}$

$$1 = \prod_{i=1}^{r-1} (a_i + b_i) \equiv \underset{\underset{\displaystyle I_1 \cdot \ldots \cdot I_r}{\cap}}{a_1 \cdot \ldots \cdot a_{r-1}} (\mathrm{mod}\ I_r)$$

więc

$$1 \in (I_1 \cdot \ldots \cdot I_{r-1}) + I_r = R$$

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

$$m_r \equiv 0 \quad (\mathrm{mod}\ \underset{\underset{\displaystyle \bigcap_{i=1}^{r-1} I_i}{\cap\!\shortparallel}}{(I_1 \cdot \ldots \cdot I_{r-1})})$$

$$m_r \equiv 1 \quad (\mathrm{mod}\ I_r)$$

więc: $m_r \in \bigcap_{j\neq r} I_j$

Analogicznie istnieje $m_i \in \bigcap_{j\neq i} I_j$ t. że $m_i \equiv 1 \pmod{I_i}$
dla $i=1,\dots,r$

$n := m_1 l_1 + m_2 l_2 + \dots + m_r l_r \equiv l_i \pmod{I_i}$

Pierścienie wielomianów jako "algebry wolne".

R: przemienny z 1.

Lemat 14.4. $f: R \to R_1$ homomorfizm pierścieni z 1.
$g: \{X_1,\dots,X_n\} \to R_1$ funkcja.

Wtedy $\exists!\, f': R[X_1,\dots,X_n] \to R_1^E$ homomorfizm
t. że $f'|_R = f$, $f'|_{\{X_1,\dots,X_n\}} = g$.

D-d. $f'(W(X_1,\dots,X_n)) = f(W)(g(X_1),\dots,g(X_n))$. OK

Wn. 14.5. Każdy pierścień R (przemienny z 1) jest homomorficznym obrazem pewnego pierścienia wielomianów nad $\mathbb{Z}$.

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

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

$g: \{X_i : i \in I\} \longrightarrow R$

$g(X_i) = a_i$

$f': \mathbb{Z}[X_i : i \in I] \longrightarrow R$ jest "na",

bo $f'(X_i) = a_i$ i A generuje R.

Ciała

Def. 14.6 $(F, \underset{\text{dodawanie}}{+}, \underset{\text{mnożenie}}{\cdot})$ ciało, gdy: (dodawanie, mnożenie ciała F)

(a) $(F, +)$ gpa abelowa (tzw. grupa addytywna ciała F)

el. neutralny: 0 (zero ciała).

(b) $(F \setminus \{0\}, \cdot)$ — " — (tzw. gpa multyplikatywna ciała F)

$\overset{\shortparallel}{F^*}$ el. neutralny: 1 (jedność ciała)

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

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

$F_1 \subseteq F$ 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

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

charakterystyka ciała F

<u>Przykłady</u>

$\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$

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

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

Uwaga 14.8. Jeśli $\operatorname{char} F = n > 0$, to n jest l. pierwsza i dla każdego $x \in F$, $n \cdot x = \underbrace{x + \ldots + x}_{n} = 0$.

<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 pierwsza.

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

Niech $a = \underbrace{1 + \ldots + 1}_{m}$, $b = \underbrace{1 + \ldots + 1}_{k}$, $a, b \in F \setminus \{0\}$,

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

<u>Uwaga</u> Jeśli F_1 ; podciało ciała F, to
$\operatorname{char} F_1 = \operatorname{char} F$.

Uwaga 14.~~10~~9. Zał, że $n > 0$ i $\operatorname{char} F \nmid n$.
Wtedy dla każdego $x \in F$ istn. jedyny $y \in F$ t. że $ny = x$. <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 $F' = \{0, 1, 1+1, \dots, \underbrace{1+\dots+1}_{p-1}\} < (F, +)$

- $(F', +) \cong (\mathbb{Z}_p, +_p)$
- F' zamkn. na $\cdot$: $(n \cdot 1)(m \cdot 1) = nm \cdot 1 = r_p(nm) \cdot 1 \in F'$.
- $f : \mathbb{Z}_p \to F'$, $f(n) = n \cdot 1$ — • bijekcja • izomorfizm: $+$: OK

$f(n) \cdot f(m) = r_p(n \cdot m) \cdot 1 = f(n \cdot_p m)$.

(2) Ćw.

char $F = 0 \Rightarrow \forall n > 0 \ \exists! y_n \in F \ n \cdot y = 1$

Dla $\frac{m}{n} \in \mathbb{Q}$ niech $\frac{m}{n} \cdot 1 \stackrel{def}{=} m \cdot y_n$, (

$m \in \mathbb{Z}, n > 0$ $\quad f : \mathbb{Q} \to F \quad f(\frac{m}{n}) = \frac{m}{n} \cdot 1$ monomorfizm ciał.

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

Def. 14.11: F ciało proste, gdy F nie ma podciał właściwych.

Uwaga 14.12

(1) Z dokł. do $\cong$ ciała proste to $\mathbb{Z}_p$, $\mathbb{Q}$.

(2) Każde ciało F zawiera ~~[illegible]~~ 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 później.)

Niech $F_1 \subseteq F_2$ rozszerzenie ciał. Wtedy F_2: przestrzeń liniowa nad ciałem F_1

$$\overset{\shortparallel}{(F_2, +, 0, r\cdot)}_{r \in F_1}$$

z ciała

np. $\mathbb{R}$: p. lin. $/\mathbb{Q}$
baza: "baza Hamela".

D-d tw. 14.13: $\underset{\text{podciało proste}}{F_0 \subseteq F}$ $\quad F_0 \cong \mathbb{Z}_p$

Niech $n = \dim_{F_0}(F) < \infty$. $F \cong \underbrace{F_0 \times \ldots \times F_0}_{n} \Rightarrow |F| = p^n$.

Uwaga (p l. pierwsza)
Dla każdego n istnieje jedyne ciało F_{p^n}, $|F_{p^n}| = p^n$.
(~~[illegible]~~ patrz Algebra 2R)

Uwaga $f: F_1 \longrightarrow F_2$ homomorfizm struktur ciała
$\Rightarrow f = 0$ lub f monomorfizm.

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