

WYKŁAD 14

Rozdział 20

Wielomiany

20.1 Pierścień wielomianów

Definicja 20.1 (Wielomian). *Wielomian* f to ciąg $(a_0, a_1, \dots, a_n)$, myślimy o nich jako o $\sum a_i x^i$. Zwykle zakładamy, że $a_n \neq 0$, w przeciwnym razie dla $n > 0$ utożsamiamy $a_0, \dots, a_{n-1}$ z $a_0, \dots, a_{n-1}$ (formalnie wielomiany to klasy abstrakcji, ale nie będziemy się tym specjalnie przejmować).

Mnożenie wielomianów definiujemy tak, jak się spodziewamy, tzn. dla wielomianów $(a_0, \dots, a_n)$ oraz $(b_0, \dots, b_m)$ ich iloczyn to $(c_0, \dots, c_{n+m})$, gdzie:

$$\left(\sum_{i=0}^n a_i x^i \right) \left(\sum_{j=0}^m b_j x^j \right) = \sum_{k=0}^{n+m} c_k x^k \quad (20.1)$$

$c_k = \sum_{i=0}^k a_i b_{k-i}$

Zbiór wielomianów o współczynnikach z pierścienia R oraz naturalnym dodawaniem

i mnożeniem (tj. po współrzędnych) to *pierścień wielomianów* $R[x]$. Zerem w tym pierścieniu jest wielomian (0) .

Liczby $a_0, \dots, a_n$ to *współczynniki wielomianu*, jeśli $a_n \neq 0$ to jest on *współczynnikiem wiodącym*.

Stopień wielomianu $\deg(a_0, \dots, a_n)$ dla $a_n \neq 0$ to n . W przypadku wielomiany zerowego stopień to $-\infty$.

Zauważmy, że mnożenie takie jak w (20.1) jest dobrze określone nawet dla pier-

ścienia nieprzemienne. Jeśli myślimy o wielomianach jak o ciągach, to tę operację nazywamy *splotem* dwóch ciągów (i często oznaczamy przez $*$).

Możemy też myśleć że wielomiany to ciągi nieskończone, które mają tylko skończenie wiele niezerowych wyrazów. Wynik mnożenia z dodanymi wiodącymi zerami jest taki sam.

Lemat 20.2 (Poprawność definicji). *$R[x]$ z mnożeniem zdefiniowanym jako splot jest pierścieniem.*

Jeśli R jest pierścieniem przemennym (z jednością), to $R[x]$ też jest pierścieniem przemennym (z jednością).

Zwykle zajmujemy się wielomianami o współczynnikach z ciała.

Lemat 20.3. Niech $f, g \in R[x]$. Wtedy

$$\deg(f + g) \leq \max(\deg(f), \deg(g))$$

$$\deg(f \cdot g) \leq \deg(f) + \deg(g).$$

$$R[x] \\ \sum a_i x^i$$

Jeśli R jest ciałem, to

$$\deg(f \cdot g) = \deg(f) + \deg(g).$$

Uwaga. W ostatnim punkcie założenie, że R jest ciałem jest istotne: np. w $\mathbb{Z}_6$ mamy $2 \cdot 3 = 0$ i iloczyn tych dwóch wielomianów stopnia 0 ma stopień $-\infty$.

$$\begin{array}{l} a_0, \dots, a_n \\ b_0, \dots, b_m \end{array} \quad \max(n, m) \quad \left| \quad \mathbb{Z}_6 \quad \begin{array}{l} 1 \\ 2 \times \quad 3 \times \\ 0 \times^2 = 0 \end{array} \right.$$

$$n = m \quad a_m = -a_m$$

$$c_k = \sum_{i=0}^k a_i b_{k-i}$$

$$k > n+m$$

$$i + (k-i) > n+m$$

$$\forall i \text{ lub } k-i > m$$

$$c_{n+m} = \sum_{i=0}^{n+m} a_i b_{n+m-i} = a_n b_m \neq 0 \quad \deg(fg) = n+m$$

20.2 Ewaluacja (wartościowanie) wielomianów

Wielomian $f \in R[x]$ równy $(a_0, \dots, a_n)$ możemy też potraktować jako funkcję z R w R , zdefiniowaną w naturalny sposób:

$$\bar{f}(p) = \sum_{k=0}^n a_k p^k$$

$\bar{f}$

Lemat 20.4. Niech $f, g \in R[x]$ i $p \in R$. Wtedy

$$\overline{f+g}(p) = \overline{f}(p) + \overline{g}(p)$$

Jeśli R jest przemienny, to dodatkowo

$$\overline{f \cdot g}(p) = \overline{f}(p) \cdot \overline{g}(p)$$

$$\overline{f+g}(p)$$

$$\overline{f}(p) + \overline{g}(p)$$

$$\begin{aligned} f &= (f_0, \dots, f_m) \\ g &= (g_0, \dots, g_m) \\ m \geq m \end{aligned}$$

$$\overline{f}(p) = \sum_{i=0}^m f_i p^i$$

$$\overline{g}(p) = \sum_{j=0}^m g_j p^j$$

$$\overline{f}(p) + \overline{g}(p) = \sum_{i=0}^m f_i p^i + \sum_{i=0}^m g_i p^i = \sum_{i=0}^m (f_i + g_i) p^i = \overline{f+g}(p)$$

$$\begin{aligned} \overline{f}(p) \cdot \overline{g}(p) &= \left(\sum_{i=0}^m f_i p^i \right) \left(\sum_{j=0}^m g_j p^j \right) = \sum_{i=0}^m \left(f_i p^i \sum_{j=0}^m g_j p^j \right) = \sum_{i=0}^m \sum_{j=0}^m f_i p^i g_j p^j \\ &= \sum_{i=0}^m \sum_{j=0}^m (f_i g_j) p^{i+j} = \sum_{k=0}^{m+m} \left(\sum_{i=0}^k f_i g_{k-i} \right) p^k = \overline{f \cdot g}(p) \end{aligned}$$

20.3 Dzielenie, podzielność i największy wspólny dzielnik wielomianów

Lemat 20.5 (Dzielenie wielomianów). Niech $\mathbb{F}$ będzie ciałem a $\mathbb{F}[x]$ pierścieniem wielomianów o współczynnikach z $\mathbb{F}$. Dla wielomianów f, g z tego pierścienia, o stopniach $m = \deg(f)$ oraz $n = \deg(g) \neq -\infty$ istnieje dokładnie jedna para wielomianów q, r , taka że $f = gq + r$, gdzie $\deg(r) < \deg(g)$.¹ Wielomiany te można efektywnie wyliczyć.

Wielomiany q, r z Lematu 20.5 nazywamy ilorazem oraz resztą z dzielenia f przez g .

¹Dla $\deg(g) = 0$ korzystamy z tego, że $\deg(0)$ to $-\infty$

Induktion $\deg(f)$

$$1) \deg(f) < \deg(g) \Rightarrow q=0 \\ r=f$$

$$q \cdot g + f = f \\ \deg(f) = \deg(r) < \deg(g)$$

2) voraus. d.h. $\deg(f) < n$

$$\deg(f) = n \geq \deg(g)$$

$$f = (f_0, \dots, f_n) \quad g = (g_0, \dots, g_m) \quad n \leq m$$

$$f - ? \cdot g \rightarrow f' \quad \deg(f') < \deg(f)$$

$$f' = f - \left(f_n \cdot g_m^{-1} \cdot x^{n-m} \right) \cdot g \quad \deg = n$$

$$\deg(f') < \deg(f)$$

$$\begin{aligned} \deg(f_n \cdot g_m^{-1} \cdot x^{n-m}) &= n-m \\ \deg(\text{---} / \text{---} \cdot g) &= \deg(\text{---} / \text{---}) + \deg(g) \\ &= n-m + m = n \end{aligned}$$

$$\deg(f') \leq n = \deg(f)$$

wsp. n

$$\Rightarrow f_n - f_n \cdot g_m^{-1} \cdot g_m = f_n - f_n = 0 \\ \deg(f') \leq n-1$$

$$2. \text{ nat. ind. } \exists q', r' \quad f' = g \cdot q' + r'$$

$$(g \cdot q' + r') = f - f_n \cdot g_m^{-1} \cdot x^{n-m} \cdot g$$

ALGORITHM

$$f = r' + g \cdot q' + g \cdot (f_n \cdot g_m^{-1} \cdot x^{n-m})$$

$$f = \left[r' + g \cdot \left(q' + f_n \cdot g_m^{-1} \cdot x^{n-m} \right) \right]$$

Da sie?

4. Induktion

$$r' + g \cdot q' = r + g \cdot q$$

$$(r' - r) = -g \cdot (q' - q)$$

$$\deg(r' - r) \leq \deg(q)$$

$$\deg(g) > \deg(r' - r) \quad \underline{\underline{=}}$$

$$\deg(g \cdot (q - q')) = \deg g + \boxed{\deg(q - q')} = -\infty$$

Przykład 20.6. Podzielmy wielomiany $f = x^5 - 3x^4 - x^3 + 7x^2 - 4$ oraz $g = x^3 - 3x^2 + 2x$ z $\mathbb{R}[x]$ z resztą:

$$\begin{array}{r}
 x^2 + 1 \\
 \hline
 x^5 - 3x^4 - x^3 + 7x^2 - 4 \quad : \quad x^3 - 3x^2 + 2x \\
 \underline{x^5 - 3x^4 - 2x^3} \\
 = \quad = \quad x^3 + 7x^2 - 4 \\
 \underline{\quad \quad x^3 - 3x^2 - 2x} \\
 = \quad \quad \quad (10x^2 + 2x - 4)
 \end{array}$$

$x^5 - 3x^4 - x^3 + 7x^2 - 4$ przez $x^3 - 3x^2 + 2x$
 $= x^2 + 1$ reszta $10x^2 + 2x - 4$

Definicja 20.7 (Podzielność wielomianów). Wielomian f jest *podzielny przez wielomian g* , jeśli reszta dzielenia f przez g wynosi 0. Zapisujemy to jako $f|g$.

Fakt 20.8. $f|g \iff$ istnieje wielomian q taki że $g = fq$.

$$g = f \cdot q + 0$$

Lemat 20.9. *Każdy wielomian dzieli 0.*

Jeśli f dzieli $g \neq 0$, to $0 \leq \deg(f) \leq \deg(g)$.

Jeśli f dzieli g i g ma stopień 0, to f też ma stopień 0.

Jeśli f dzieli g i g dzieli f , to $f = cg$ dla pewnego $c \in \mathbb{F} \setminus \{0\}$.

• $0 \quad f \quad f \cdot 0 = 0$

• $f|g \quad g \neq 0 \quad \Rightarrow 0 \leq \deg(f) \leq \deg(g)$

$\exists q \quad g = f \cdot q$

$$\deg(f \cdot q) = \deg(f) + \deg(q) = \deg(g) \geq 0$$

$$\deg(f) \leq \deg(g)$$

• $\deg(g) = 0 \Rightarrow \deg(f) = 0$

$f|g, \deg(g) = 0 \Rightarrow \deg(f) = 0$

• $f|g, g|f \Rightarrow \exists c \in \mathbb{F}_{\neq 0}$

$f = c \cdot g \Rightarrow g = c^{-1} f$

Definicja 20.10 (Wielomian nierozkładalny). Wielomian $f \in R[x]$ jest *nierozkładalny* w $R[x]$, jeśli $\deg(f) > 0$ i nie istnieją wielomiany $g, h \in R[x]$ takie że $f = gh$ oraz $\deg(g), \deg(h) < \deg(f)$.

Wielomiany stopnia 1 są nierozkładalne. Ale mogą być też większego stopnia: np. wielomian $x^2 + 1$ w $\mathbb{R}[x]$

Definicja 20.11 (Największy wspólny dzielnik (gcd) wielomianów). Największy wspólny dzielnik dwóch wielomianów f, g to taki wielomian h , że $h|f, h|g$ oraz jeśli $h'|f, h'|g$, to $h'|h$.

Zauważmy, że gcd wielomianów jest określone z dokładnością do stałej multiplikatywnej.

Liczymy to przy użyciu algorytmu Euklidesa. (Cały algorytm i dowód jego poprawności działa dokładnie tak jak w przypadku liczb całkowitych).

Lemat 20.12. Każde dwa wielomiany $p, q \in \mathbb{F}[x]$ mają *największy wspólny dzielnik*. Jest on postaci $ap + bq$ dla pewnych wielomianów $a, b \in \mathbb{F}[x]$.

$$\begin{aligned} \text{gcd}(f, g) &= \text{gcd}(r, g) & f &= g \cdot q + r & r &\leftarrow \text{resida} \\ \text{Polować!} & & \deg(r) &< \deg(g) \leq \deg(f) \end{aligned}$$

$$\begin{aligned} h|f, h|g &\Rightarrow h|r \\ h|r, h|g &\Rightarrow h|f \end{aligned}$$

Ubiór wspólnych
dzielników (f, g)
oraz (r, g) są takie same

$$(f, g) \rightarrow \dots \rightarrow (0, r)$$

$$\text{gcd}(0, r) = r$$

$$\begin{aligned} r|0, r|r \\ h|0, h|r \Rightarrow h|r \end{aligned} \quad \text{gcd}$$

$$f = g \cdot q + r$$

$$h|f, h|g$$

$$\begin{aligned} f &= g \cdot q + r & r &= f - g \cdot q = \\ f &= hf' & g &= hg' \end{aligned}$$

$$\begin{aligned} hf' - h \cdot g' \cdot q &= \\ = h(f' - g' \cdot q) &\Rightarrow h|r \end{aligned}$$

$$\begin{aligned} h|r, h|g &\Rightarrow \\ r = hr' & g = hg' \end{aligned}$$

$$h| \overbrace{(g \cdot q + r)}^f$$

$$\begin{aligned} f = g \cdot q + r &= hg'q + hr' = h(g'q + r') \\ h|f \end{aligned}$$

Wzrostko w alg Euklidesa to kom f, g

$$f = 1 \cdot f + 0 \cdot g$$

$$g = 0 \cdot f + 1 \cdot g$$

$$(f, g) \rightarrow (r, g')$$

$r \leftarrow \text{reszta z dzielenia } f \text{ przez } g'$

$$\begin{aligned} f' &= a \cdot f + b \cdot g \\ g' &= a' \cdot f + b' \cdot g \end{aligned}$$

$$r = f' - q \cdot g'$$

$$af + bg - q(a' \cdot f + b' \cdot g)$$

Przykład 20.13. Znajdźmy największy wspólny dzielnik wspomnianych już wielomianów $f = x^5 - 3x^4 - x^3 + 7x^2 - 4$ oraz $g = x^3 - 3x^2 + 2x$ z $\mathbb{R}[x]$ przy użyciu algorytmu Euklidesa. Pierwszy krok to jak poprzednio podzielenie tych wielomianów z resztą.

$$\begin{array}{r}
 x^3 - 3x^2 + 2x \overline{) \begin{array}{r} x^5 - 3x^4 - x^3 + 7x^2 - 4 \\ - x^5 + 3x^4 - 2x^3 \\ \hline - 3x^3 + 7x^2 \\ 3x^3 - 9x^2 + 6x \\ \hline - 2x^2 + 6x - 4 \end{array}} \\
 \end{array}
 \begin{array}{l}
 x^2 - 3 \\
 - 4
 \end{array}$$

Czyli $x^5 - 3x^4 - x^3 + 7x^2 - 4 = (x^3 - 3x^2 + 2x)(x^2 - 3) + (-2x^2 + 6x - 4)$.

Dalej korzystamy z:

$$\gcd(af + b, f) = \gcd(b, f).$$

Tym samym pozostaje nam policzenie $\gcd(-2x^2 + 6x - 4, x^3 - 3x^2 + 2x)$.

$$\begin{array}{r}
 x^3 - 3x^2 + 2x : x^2 - 3x + 2 \\
 \underline{x^3 - 3x^2 + 2x} \\
 0
 \end{array}$$

$\left. \begin{array}{l} \text{?} \text{ dda} \\ \text{gcd}(x^2 - 3x + 2; x^3 - 3x^2 + 2x) \end{array} \right\}$

$$\gcd = x^2 - 3x + 2$$

$$= -\frac{1}{2}f + \frac{1}{2}(x^2 - 3)g$$

W pewnym sensie prawdziwe jest też „twierdzenie odwrotne” jeśli wspólny dzielnik p, q można przedstawić jako ich kombinację, to h jest $\gcd(p, q)$:

Lemat 20.14. Niech $a, b, h \in \mathbb{F}[x]$. Jeśli $h|f, h|g, h = af + bg$ to $h = \gcd(f, g)$.

Dowód pozostawiamy jako ćwiczenie.

Największy wspólny dzielnik dla wielomianów ma podobne własności, jak dla liczb całkowitych.

Lemat 20.15. Niech $f, f', g, g', h, a, b \in \mathbb{F}[x]$. Jeśli $f = f'h, g = g'h$ to

$$\gcd(f, g) = h \gcd(f', g') .$$

Jeśli $f = f'h$ oraz $\gcd(h, g)$ jest stałą, to:

$$\gcd(f, g) = \gcd(f', g) .$$

$\mathbb{F}[x]$

Lemat 20.16. Jeśli f jest nierozkładalny oraz $f|p_1 p_2 \dots p_k$ to $f|p_i$ dla pewnego i .

$\gcd$
Indukcja

$$f|p_1 p_2 \Rightarrow f|p_1 \vee f|p_2$$

$$\gcd(f, p_1) = h = \begin{cases} 1 & \text{z doł. do} \\ f & \text{z doł. do } f. \end{cases}$$

↑
nierozk.

$$2) \quad \gcd(f, p_2) = f \Rightarrow f|p_2$$

$$1) \quad \gcd(f, p_1) = \begin{cases} 1 = af + bp_1 \\ p_2 = afp_1 + bp_1 p_2 \end{cases} \quad / p_2$$

$f|$

$$f|p_2$$

Indukcja

$$f|p_1 \dots p_{n+1}$$

$p_1 \quad p_{n+1}$

$$f|p \cdot p_{n+1} \rightarrow \begin{cases} f|p_{n+1} \text{ ok} \\ f|p_1 \dots p_n \text{ z zol. ind.} \end{cases}$$

Lemat 20.17. Jeśli f_i są nierozkładalne oraz $\gcd(f_i, f_j)$ jest stałą dla $i \neq j$ oraz $f_i|g$ to $f_1 \dots f_k|g$.

Przez indukcję

$$f_1 | g \quad f_2 | g$$

$$n \quad f_1, f_2, \dots, f_n | g \Rightarrow (f_1 \dots f_n) | g$$

$$f_1 \dots f_n | g \quad g = \underbrace{f_1 \dots f_n}_{f_{n+1}} \cdot g'$$

$$2 \quad \text{popr. lemat} \quad f_{n+1} | f_1 \dots f_n \cdot g' \quad \leftarrow \text{fakt dzięki h'ogry's}$$

$$f_{n+1} | f_i$$

$$f_{n+1} | g' \quad g' = f_{n+1} g''$$

$$g = f_1 \dots f_n \cdot g' = \underbrace{(f_1 \dots f_n \cdot f_{n+1})}_{f_1 \dots f_{n+1}} \cdot g''$$

$$f_1 \dots f_{n+1} | g$$

Wniosek 20.22. Jeśli waluacje dwóch wielomianów stopnia co najwyżej n mają te same wartości w $n+1$ punktach, to są równe. $f \quad g \quad (f-g)(p) = 0$

W ciele nieskończonym dwa wielomiany mają skończoną liczbę wartości wspólnych.

Przykład/Zastosowanie 20.23 (Interpolacja wielomianu). Jeśli dla danego wielomianu $f \in \mathbb{F}[x]$ stopnia n mamy podane jego wartości $\bar{f}(p_i)$ dla różnych $p_0, \dots, p_n \in \mathbb{F}$, to jest on jednoznacznie wyznaczony.

$$\begin{array}{l} \left\{ \begin{array}{l} p_0 \\ p_1 \\ \vdots \\ p_n \end{array} \right\} \quad \begin{array}{l} \bar{f}(p_0) \\ \bar{f}(p_1) \\ \vdots \\ \bar{f}(p_n) \end{array} \end{array} \quad \begin{array}{l} \deg(f) \leq n \\ \rightarrow \text{maksymalnie jeden taki} \\ \text{wiel.} \\ \nwarrow b_0, \dots, b_n \end{array}$$

Układ równań

$$\begin{array}{l} f \quad (f_0, \dots, f_n) \\ m+1 \times m+1 \rightarrow \begin{bmatrix} p_0^0 & p_0^1 & \dots & p_0^m \\ p_1^0 & \dots & p_1^m \\ \vdots & \ddots & \vdots \\ p_n^0 & \dots & p_n^m \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \\ \vdots \\ f_n \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_n \end{bmatrix} \end{array}$$

$\sum_{i=0}^m f_i p_0^i = \bar{f}(p_0)$

Jedno rozwiązanie $\Leftrightarrow \det \neq 0$

macierz Vandermonde'a $p_0, \dots, p_n \leftarrow$ różne $\rightarrow \det \neq 0$.

Wielomian ten można też podać bardziej „wprost”:

$$w = (x - p_0)(x - p_1) \cdots (x - p_m)$$

$$w_i = \frac{w}{(x - p_i)} = \prod_{j \neq i} (x - p_j) \quad \nwarrow \deg(w_i) = m$$

$$w_i(p_i) \neq 0$$

$$w_i(p_j) = 0 \quad j \neq i$$

$$w'_i = w_i / \overline{w_i}(p_i)$$

$$w'_i(p_i) = 1$$

$$w'_i(p_j) = 0 \quad j \neq i$$

$$f = \sum_{i=0}^m b_i \cdot w'_i$$

$$\overline{f}(p_j) = \sum_i b_i \overline{w'_i}(p_j) = b_j \underbrace{\overline{w'_j}(p_j)}_1 = b_j$$

Przykład/Zastosowanie 20.24 (Dzielenie sekretu). Dla grupy n osób chcemy stworzyć protokół, który pozwala dowolnym $m+1$ z nich poznać wiadomość, ale każdym m już nie.

$C \leftarrow \text{sekret}$ $C \in \mathbb{F} \leftarrow \text{losowane}$

$P_1, P_2, \dots, P_n \leftarrow \text{punkty z tego ciała, nierówne}$

$C \leftarrow \text{współczynnik wielomianu}$

$f \leftarrow \overbrace{C_m, C_{m+1}, \dots, C_0}^{\text{losowe}} \leftarrow \text{stopień } m$
 $\quad \quad \quad \parallel$
 $\quad \quad \quad C$

$f(P_i) \rightarrow \text{wiadomości osoby } i$

- $m+1$ osób: wartości f w $m+1$ punktach $\Rightarrow$ potrafisz odtworzyć.
- m osób nie potrafisz.

"dodać" $n+1$ osobę $\boxed{C_0} f(0) \leftarrow \text{dowolnie}$
 $\quad \quad \quad \text{dowolne}$

$m \text{ osób}$ $m+1$ $\rightarrow$ interpolacja
 $\bar{f}(\quad)$ $\bar{f}(0)$

Rozdział 21

Ciała, rozszerzenia ciał

21.1 Charakterystyka ciała, ciało proste

Definicja 21.1 (Charakterystyka ciała; ciało proste). Dla ciała $\mathbb{F}$ jego *charakterystyka* to rząd 1 w grupie addytywnej. $1+1+\dots+1=0$

Ciało generowane przez 1 w ciele $\mathbb{F}$ to *ciało proste*.

Lemat 21.2. *Charakterystyka* ciała to albo $+\infty$ albo liczba pierwsza p . W pierwszym przypadku ciało proste to $\mathbb{Q}$, w drugim: $\mathbb{Z}_p$.

$$\cdot 1, 1+1, \dots, 1+\dots+1, \dots$$

rozł. niek. $+\infty$

$$\cdot \underbrace{1+\dots+1}_m = 0$$

$$m = p \cdot q$$

$$\underbrace{(1+1+\dots+1)}_p + \underbrace{(1+\dots+1)}_p + \dots + \underbrace{(1+1+\dots+1)}_p = 0$$

$$p \cdot 1 + p \cdot 1 + \dots + p \cdot 1 = p \cdot \underbrace{(1+1+\dots+1)}_q = p \cdot q = 0$$

$\Downarrow$

$$p = 0 \quad q = 0$$

(w $\mathbb{F}$)

$$p=1, q=n \text{ lub } p=n, q=1$$

$$\text{char}(\mathbb{F}) = p$$

$$\mathbb{Z}_p \subseteq \mathbb{F}$$

$$0, 1, 1+1, 1+1+1, \dots, \underbrace{1+1+\dots+1}_{p-1} \subseteq \mathbb{F} \text{ p.d.}$$

$$\underbrace{1+1+\dots+1}_p = 0$$

$$\begin{array}{c}
 \mathbb{Z}_{p^1} \\
 0 \\
 1 \\
 \hline 1+1 \\
 \hline 1+1+1 \\
 \vdots \\
 1+1+\dots+1 \\
 p-1
 \end{array}
 \quad
 \begin{array}{c}
 \mathbb{Z}_p \\
 0 \\
 1 \\
 2 \\
 3 \\
 \vdots \\
 p-1
 \end{array}$$

$$\begin{array}{c}
 \underline{k} + \underline{l} \\
 \nearrow \quad \nwarrow \\
 (1 \dots 1) \quad (1 \dots 1)
 \end{array}
 \quad
 \underbrace{1+1+\dots+1}_{n+l} = \underline{n+l}$$

$$\begin{aligned}
 \underline{k} \circ \underline{l} &= (1+\dots+1)(1+\dots+1) \\
 &= \binom{n}{n} + \binom{n}{n} + \dots + \binom{n}{n} \quad \text{1 row} \\
 &= \underbrace{1+1+\dots+1}_{n \text{ times}}
 \end{aligned}$$

char ∞

$$1, 1, \dots, 1$$

$$\begin{aligned}
 \underline{n} &= \underbrace{1+\dots+1}_n \\
 -\underline{n} &= \underbrace{-1-\dots-1}_n
 \end{aligned}$$

$$\frac{1}{n} \in \text{o dividing } \underline{n}$$

$$\frac{\underline{n}}{\underline{n}} \quad \underbrace{\frac{1}{n} + \dots + \frac{1}{n}}_{n \text{ rows}}$$

Lemat 21.3. *Ciało jest przestrzenią liniową nad swoim ciałem prostym.*

$$\mathbb{Z}_p \leq \mathbb{F} \quad \begin{matrix} p \\ p^k \end{matrix} \quad \text{przestrzeń liniowa nad } \mathbb{Z}_p$$

Wniosek 21.4. Każde ciało skończone ma p^k elementów dla pewnych p —pierwsze i $k \in \mathbb{N} \setminus \{0\}$.

21.2 Konstrukcja ciał (skończonych)

Naszym celem obecnie jest konstrukcja ciała skończonego. Takie ciało uzyskamy przez wydzielenie pierścienia $\mathbb{F}[x]$ przez odpowiednią kongruencję. Jest to analogiczna konstrukcja do konstrukcji $\mathbb{Z}_p$ jako wydzielenia $\mathbb{Z}$ przez kongruencję podzielności przez liczbę pierwszą. Naszym ciałem zwykle jest ciało skończone (np. $\mathbb{Z}_p$), ale wszystko działa też dla ciał o charakterystyce $+\infty$.

Definicja 21.5 (Kongruencja modulo wielomian). Dla ciała $\mathbb{F}$ oraz pierścienia wielomianów $\mathbb{F}[x]$ o współczynnikach z tego ciała oraz wielomianu $h \in \mathbb{F}[x]$ definiujemy kongruencję $\equiv_h$ na $\mathbb{F}[x]$:

$$f \equiv_h g \iff h \mid (f - g).$$

Kongruencja:

• rel. równ

$$\begin{aligned} f &\equiv g \\ f' &\equiv g' \end{aligned}$$

$$\begin{aligned} f &\equiv_h g \\ f' &\equiv_h g' \end{aligned}$$

$$h \mid f - g$$

$$h \mid f' - g'$$

$$\begin{aligned} f &\equiv_h f \\ f' &\equiv_h f' \end{aligned}$$

$$f + f' \equiv_h g + g'$$

$$f \cdot f' \equiv_h g \cdot g'$$

$$f + f' \equiv_h g + g'$$

$$h \mid (f - g) + (f' - g')$$

$$f \cdot f' - g \cdot g' = \underbrace{f \cdot f' - f'g + f'g - gg'}_{=}$$

$$= \frac{f'(f - g) + g(f' - g')}{h}$$

$$h \mid f \cdot f' - g \cdot g'$$

$$ff' \equiv_h gg'$$

$$\frac{f-f'}{f'f}$$

$$f \equiv g \implies f' \equiv g'$$

$$h \mid f - g$$

$$h \mid g - g'$$

$$h \mid f + g - g'$$

Lemat 21.6. Dla pierścienia wielomianów o współczynnikach z ciała $\mathbb{F}[x]$ oraz wielomianu $h \in \mathbb{F}[x]$ z tego pierścienia relacja $\equiv_h$ na $\mathbb{F}[x]$ jest relacją równoważności.

Operacje $+$, $\cdot$ są dobrze zdefiniowane w $\mathbb{F}[x]/\equiv_h$. W szczególności, $\mathbb{F}[x]/\equiv_h$ jest pierścieniem przemiennym z jednością.

$$\mathbb{F}[x]/\equiv_h$$

$$[f] + [g] = [f+g]$$

$$[f'] + [g'] = [f'+g']$$

$$\mathbb{F}[x] \text{ przem, z } 1 \quad f+g=g+f$$

$$\mathbb{F}[x]/\equiv_h \quad [f+g]=[g+f]$$

$$f \circ g = g \circ f$$

$$[f \circ g] = [g \circ f]$$

$$[f] \circ [g] = [g] \circ [f]$$

$$[1] \quad [1 \cdot f] = [f \cdot 1] = [f]$$

$$[1] \circ [f] = [f] \circ [1] = [f]$$

Lemat 21.7. Jeśli wielomian $h \in \mathbb{F}[x]$ jest nierozkładalny, to w $\mathbb{F}[x]/\equiv_h$ istnieje element odwrotny dla $f \not\equiv_h 0$.

$h \leftarrow$ nierozkładalny
 $f \not\equiv_h 0$ $h \nmid f$

$$\gcd(f, h) = \begin{cases} 1 \\ h \end{cases} \quad \text{tj. } h \nmid f \quad \&$$

$$\gcd(f, h) = 1 = a \cdot f + b \cdot h$$

$$[1] = [a f + b h]_h = [a f] + \underbrace{[b h]}_0 = [a] \cdot [f]$$

$[a] \leftarrow$ d. odw. do $[f]$

Twierdzenie 21.8. Jeśli wielomian h jest nierozkładalny, to ciało $\mathbb{F}[x]/\equiv_h$ (jako przestrzeń liniowa nad $\mathbb{F}$) ma wymiar $\deg(h)$. Jeśli $\mathbb{F}$ jest skończone, to takie rozszerzenie ma $|\mathbb{F}|^{\deg h}$ elementów.

$h \leftarrow \deg(h) = k$
 $x^0, x^1, x^1, \dots, x^{k-1}$ k

$[x^0], \dots, [x^{k-1}] \leftarrow$ tworzą b. p., $\deg(p) < k$ jest ich kombin.

$$\left[\sum_{i < k} a_i x^i \right]$$

$[f] \equiv_h [f'] \Rightarrow f = f'$ $\deg(f), \deg(f') < k$

$[f] \equiv_h$ $f = q \cdot h + r$ $h \mid \underbrace{f - f'}_0$ $f \equiv_h r \leftarrow \deg(r) < k$

Twierdzenie 21.9 (bez dowodu). Dwa ciała skończone o p^k elementach są izomorficzne.

Przykład 21.10. Wielomian nierozkładalny $x^2 + 1 \in \mathbb{R}[x]$; wychodzi izomorficzne z $\mathbb{C}$.

$$\begin{array}{l} \mathbb{R}[x]/x^2+1 \quad \mathbb{C} \\ x^2+1 \equiv 0 \\ x^2 \equiv -1 \end{array} \quad \begin{array}{l} x \\ x^2 = -1 \end{array}$$

Przykład 21.11. Zbudujmy ciało 4-elementowe. $4 = 2^2$, więc bierzemy $\mathbb{F} = \mathbb{Z}_2$ i potrzebujemy wielomianu nierozkładalnego stopnia 2.

$$\begin{array}{l} \mathbb{F} = \mathbb{Z}_2 \\ \mathbb{Z}_2[x]/\equiv_{x^2+x+1} \end{array} \quad \begin{array}{l} x^2+x+1 \\ \nearrow \text{nierozk.} \end{array}$$

$$\begin{array}{l} 0, 1 \\ x, x+1 \end{array} \quad \begin{array}{l} x^2+x+1 = 0 \\ x \cdot x = \underbrace{x^2}_{x+1} = x+1 \\ x \cdot (x+1) = x^2+x = x+1+x = 1 \\ (x+1)(x+1) = x^2+1 = x \end{array}$$

Lemat 21.12. W $\mathbb{Z}_p[x]$ jest wielomian nierozkładalny dowolnego stopnia większego niż 0.

Dowód polega na podaniu konkretnego wielomianu lub na zliczaniu wielomianów rozkładalnych i nierozkładalnych. Szczegółów nie podamy.