Wykład 15.

Uwaga 14.14.

Załóżmy, że char $F = p > 0$. Wtedy w ciele F:

$$(x+y)^p = x^p + y^p$$

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

$0 < i < p \Rightarrow p \mid \binom{p}{i} = \frac{p!}{i!(p-i)!}$

Wn. (char $F = p$)

Funkcja $x \longmapsto x^p$ jest homomorfizmem ciał.

(tzw. funkcja Frobeniusa) Fr

Fakt. F: ciało skończone $\Rightarrow$ F^*: grupa cykliczna.

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

Wn. Załóżmy, że char $F = p > 0$.

Wtedy $F^p = \{x^p : x \in F\}$: podciało ciała F.

Jeśli F: skończone, to $F^p = F$.

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

Przykład $Fr : \mathbb{F}_p(X) \longrightarrow \mathbb{F}_p(X)^p = \mathbb{F}_p(X^p) \subsetneq \mathbb{F}_p(X)$.

Równania algebraiczne w ciałach. AII.15 (2

$x^2+1=0$: nie ma rozwiązań w $\mathbb{R}$
$\cap\!\!|$
ma rozwiązania w $\mathbb{C}$

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 $F[X]$

Wystarczy znaleźć ciało $F_1 \supseteq F$ t. że V_1 ma pierwiastek w F_1.

BSO $W = V_1$: nierozkładalny.

$W(X) = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0$, $a_n \neq 0$, $a_i \in F$.

Niech $I = (W) \lhd F[X]$

maksymalny, bo $F[X]$: PID i W : nierozkładalny.

$\underset{\text{ciało}}{F_1} = F[X]/I = \{c_0 + c_1X + \ldots + c_{n-1}X^{n-1} + I : c_i \in F\}$

bez powtórzeń.

Niech $i : F \longrightarrow F_1$ $\quad i$: homomorfizm ciał, $\neq 0$ $(1 \notin I)$

$c \longmapsto c+I$ $\quad\Downarrow$ monomorfizm

$F \cong i[F] \subseteq F_1$ podciało.

Utożsamiamy F z $i[F] \Rightarrow F \subseteq F_1$

rozszerzenie ciał.

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

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

bo: w F_1:

$a_n (X+I)^n + \dots + a_1 (X+I) + a_0 =$

$= (a_n X^n + \dots + a_1 X + a_0) + I = W(X) + I = I = 0 + I = 0_{F_1}$.

Def. 14.16. Ciało F jest <u>algebraicznie domknięte</u>, gdy każdy $W \in F[X]$ stopnia > 0 ma pierwiastek w F.

<u>Przykład</u>. $\mathbb{C}$, $\mathbb{Q}^{alg} = \{z \in \mathbb{C} : z$ l. algebraiczna$\}$

TW. Każde ciało F jest podciałem pewnego ciała F' alg. domkniętego.
(idea: F' uzyskujemy w ciągu rozszerzeń jak w Lemacie 14.15)

Uwaga 14.17. Ciało algebr. domknięte jest nieskończone.

<u>D-d</u>. Zał., że $F = \{a_0, \dots, a_n\}$ skończone ciało alg. domknięte.

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

wielomian bez pierwiastka w F $\lightning$.

Kody korygujące błędy.

<u>Idea:</u>

Nadawca $\longrightarrow$ Odbiorca

$$\underbrace{\mathbb{Z}_2^k \ni w \longrightarrow vw \in \mathbb{Z}_2^n}_{\text{Nadawca}} \longrightarrow (vw)' \text{ : tu mogą być błędy.}$$

kodowanie

f : (n,k)-koder

$w \longrightarrow vw$

$|w|=k$ $\quad$ $|v|=k$

$$f : \mathbb{Z}_2^k \xrightarrow{1-1} \mathbb{Z}_2^n \quad ; (n,k)\text{-kod}$$

(n,k)-koder

- kod jest liniowy, gdy f liniowe (np: kody Hammonda)

Def. dla $w_1, w_2 \in \mathbb{Z}_2^n$

$$d(w_1,w_2) = |\{i \in \{1,\dots,n\} : w_1(i) \neq w_2(i)\}|$$

odległość Hamminga,

Niech $f: \mathbb{Z}_2^k \longrightarrow \mathbb{Z}_2^n$ (n,k)-kod

<u>Def.</u> (1) Kod f rozpoznaje do t błędów, gdy dla każdego $w \in \mathbb{Z}_2^k$ Odbiorca potrafi rozpoznać, czy w $f(w)'$ są błędy, jeśli tylko $\underbrace{\text{liczba błędów jest} \leq t}$

tzn. $d(f(w)', f(w)) \leq t$.

(2) $C(f) = \{f(w) : w \in \mathbb{Z}_2^k\}$; zbiór słów kodowych z $\mathbb{Z}_2^n$.

Uwaga 15.1

Kod f rozpoznaje do t błędów $\Leftrightarrow$ $\forall w_1 \neq w_2 \in \mathbb{Z}_2^k$ $d(f(w_1), f(w_2)) \geq t+1$.

<u>D-d.</u> $\Leftarrow$: Załóżmy, że $\underset{w \in \mathbb{Z}_2^k}{\cancel{\ }}$ i $d(f(w)', f(w)) \leq t$

Wtedy $f(w)' = f(w)$ (nie ma błędów)

$\Updownarrow$

$f(w)' \in C(f)$ (a to Odbiorca umie rozpoznać)

Bo: $\Uparrow$: jeśli $f(w)' \in C(f)$ i $f(w)' \neq f(w)$

to $f(w)' = f(w_1)$ dla pewnego $w_1 \in \mathbb{Z}_2^k$, więc

$d(f(w)', f(w)) = d(f(w_1), f(w)) \underset{w}{\overset{\neq}{}} \geq t+1$ ↯.

$\Rightarrow$, nie wprost.

Zał, że $w_1 \neq w_2 \in \mathbb{Z}_2^k$ i $d(f(w_1), f(w_2)) \leq t$.

Wtedy jeśli ~~$f(w_1)' = f(w_2)$, to~~:

Odbiorca uzyskuje ~~kom~~ przekaz $f(w_2)$, to możliwe są następujące przypadki:

1°. Nadawca zakodował słowo $w = w_2$ i Odbiorca dostał przekaz $f(w)' = f(w_2)$ bez błędów

2°. Nadawca zakodował słowo $w = w_1$ i Odbiorca dostał przekaz $f(w)' = f(w_2)$ z $\leq t$ błędami.

Odbiorca nie ~~o~~ umie rozstrzygnąć, czy zaszło 1° czy 2°.

Nie umie poprawnie odpowiedzieć na pytanie: "Czy przekaz zawiera błędy".

Uwaga 15,2.

Kod f może korygować do t błędów $\Leftrightarrow$

$\forall w_1 \neq w_2 \in \mathbb{Z}_2^k \quad d(f(w_1), f(w_2)) \geq 2t+1$.

<u>Def</u>. Kod f może korygować do t błędów, gdy $\forall w \in \mathbb{Z}_2^k$, jeśli $d(f(w)', f(w)) \leq t$, to ~~odz~~ Odbiorca potrafi skorygować $f(w)'$ i odtworzyć $f(w)$.

D-d 15.2

$\Leftarrow$ Zał. że $w \in \mathbb{Z}_2^k$ i $d(f(w)', f(w)) \leq t$.

Wtedy $f(w)$ = jedyne słowo $x \in C(f)$ t. że

$$d(f(w)', x) \leq t$$

więc Odbiorca może odtworzyć $f(w)$ z $f(w)'$.

$\Rightarrow$ nie wprost. Zał. że $w_1 \neq w_2 \in \mathbb{Z}_2^k$ i

$$d(f(w_1), f(w_2)) \leq 2t.$$

Wtedy istnieje $x \in \mathbb{Z}_2^n$ t. że

$$d(x, f(w_1)) \leq t \text{ i } d(x, f(w_2)) \leq t$$

Zał. że Odbiorca uzyskał przekaz x jakiegoś słowa $w \in \mathbb{Z}_2^k$ i wie, że $d(x, f(w)) \leq t$.

Wtedy możliwe jest zarówno $w = w_1$, jak i $w = w_2$ i Odbiorca nie może odtworzyć w i $f(w)$.

Kody wielomianowe

Słowa $a_0 a_1 \ldots a_{n-1} \in \{0,1\}^*$

$$\wr$$

$$a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} \in \mathbb{Z}_2[X]$$

Niech $p(X) \in \mathbb{Z}_2[X]$, $\deg(p) = n-k$

(n,k) - kod wielomianowy generowany przez p:

wiadomość $m \in \mathbb{Z}_2^k \longrightarrow m(x) \in \mathbb{Z}_2[x]$, $\deg(m) \le k-1$

$m = a_0 a_1 \ldots a_{k-1}$

$$X^{n-k} \cdot m(X) = a_0 X^{n-k} + a_1 X^{n-k+1} + \ldots + a_{k-1} X^{n-1}$$

Niech $r(X) = r_{p(X)}\left(X^{n-k} \cdot m(X)\right)$

$$X^{n-k} m(X) = q(X) \cdot p(X) + r(X), \ \deg(r) < n-k$$

$$\underbrace{r(X)}_{\text{początek}} + \underbrace{X^{n-k} m(X)}_{\text{koniec}} = q(X) \cdot p(X)$$

przekazu

$$f(m(X)) = r(X) + X^{n-k} m(X) \leftrightarrow \text{słowo} \in \mathbb{Z}_2^n.$$

Wiadomość otrzymana przez odbiorcę:

$f(m(X))'$

weryfikacja: sprawdzenie, czy $p(X) \mid f(m(X))'$

$$\Updownarrow$$

$$f(m(X))' \in C(f)$$

Uwaga Kod f jest liniowy

d-d: ćw.

Przykład Wielomian $p(X) = 1 + X$

generuje $(n, n-1)$ - kod parzystości:

$$f(w) = \begin{cases} 0w, & \text{gdy w } w \text{ jest parzyście wiele jedynek} \\ 1w, & \text{gdy w } w \text{ jest nieparzyście wiele} \dots \end{cases}$$

BCH - kod długości $n = 2^{m-1}$ korygujący

↑1960 t błędów $(t < 2^{m-1})$

Bose

(n, k) - kod, gdzie k: pewna liczba

$$\geq n - m \cdot t,$$

Jest to kod generowany przez wielomian $p(X) \in \mathbb{Z}_2[X]$ określony następująco:

$F = F_{2^m} \supseteq F_2 = \mathbb{Z}_2$. F^*: cykliczna.

α generator

dla $\beta \in F$ niech

$W_\beta(X) \in \mathbb{Z}_2[X]$ t.że $W_\beta(\beta) = 0$ i

$0 < \deg W_\beta$ minimalny.

(wielomian minimalny dla β nad $\mathbb{Z}_2$)

$\deg W_\beta \leq m$.

(np. $\beta^{2^m-1}+1=0$, bo $\underset{\text{w } F^*}{\mathrm{ord}(\beta)} \mid 2^m-1$)

Niech $p_i(X)$: wielomian minimalny dla α^i nad $\mathbb{Z}_2$

$$p(X) := NWW(p_1(X), \dots, p_{2t}(X))$$

$$(= NWW(p_1(X), p_3(X), \dots, p_{2t-1}(X)))$$

$\deg p \leq t \cdot m$, $k = n - \deg p$.

Ten kod koryguje do t błędów (na mocy Uwagi 5.2)

F: ciało, równania w ciele F:

1. stopień 2: $X^2 + aX + b$

$\operatorname{char} F \neq 2$

$$\Updownarrow$$

$$\left(X^2 + 2\frac{a}{2}X + \frac{a^2}{4}\right) = \frac{a^2}{4} - b$$

$$\Updownarrow$$

$$\left(X + \frac{a}{2}\right)^2 = \frac{a^2}{4} - b$$

$$\Updownarrow$$

$$X + \frac{a}{2} = \pm\sqrt{\frac{a^2}{4} - b}$$ o ile ten pierwiastek istnieje w F.

2. stopień 3: $X^3 + aX^2 + bX + c = 0$

$\operatorname{char} F \neq 2,3$

metoda Cardana (Cardano, wł.)

$$\Updownarrow \quad y = X + \frac{a}{3}$$

$$y^3 + \underbrace{\left(b - \frac{1}{3}\right)}_{p} y + \underbrace{\left(c - \frac{1}{3}ab + \frac{2}{27}a^3\right)}_{q} = 0$$

$$\Updownarrow$$

$$y^3 + py + q = 0$$

$$\Updownarrow \quad y = u - \frac{p}{3u}$$

$$u^6 + qu^3 - \frac{p^3}{27} = 0$$

$$\Downarrow \quad z = u^3$$

$$z^2 + qz - \frac{p^3}{27} = 0$$

$z_1 = \dots$ $\qquad$ $z_2 = \dots$

u_1, u_2, u_3 $\qquad$ u_1', u_2', u_3' | pierwiastki z powtórzeniami, jeśli istnieją w F.

(3) stopień 4:
char $\neq 2, 3$
Ferrari

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

$$\Updownarrow \quad y = x + \frac{a}{4}$$

$$y^4 + py^2 + qy + r = 0$$

$\Updownarrow$ parametr u dodatkowy

kwadrat sumy $\quad (y^4 + uy^2 + \frac{u^2}{4}) = (u-p)y^2 - qy + (\frac{u^2}{4} - r)$

dobieramy u tak, by prawa strona też była kwadratem wielomianu zmiennej y stopnia 1, tzn

$$q^2 - 4(u-p)\left(\frac{u^2}{4} - r\right) = 0$$

$$\downarrow$$

$$u^3 - pu^2 - 4ru + (4pr - q^2) = 0 \quad \Leftarrow \text{równanie rozwiązujące}$$

$$\rightsquigarrow \left(y^2 + \frac{u}{2}\right)^2 = (u-p)\left(y - \frac{q}{2(u-p)}\right)^2$$

$$y^2 + \frac{u}{2} = \pm\sqrt{u-p}\left(y - \frac{q}{2(u-p)}\right)$$

$$\Downarrow$$

$$y = \ldots$$

④ <u>stopień 5</u> : .... $\rightsquigarrow$ Galois: nie da rady!

<u>Idea</u>: Wielomian $W(X) \in F[X]$ nierozkładalny

$F \subseteq F' \leftarrow$ tu W ma pierwiastki.

Czy te pierwiastki można uzyskać "wzorem" używając działań z F' i pierwiastkowania? $\sqrt[n]{\cdot}$?

<u>BSO</u> $F' = F(\text{pierwiastki } W)$

Jeśli TAK, to $Gal(F'/F) = \{f \in Aut(F') : f|_F = id_F\}$

"rozwiązalna".

Ale: pokażemy, że dla pewnego W stopnia 5

$Gal(F'/F) \cong S_5$: nie jest rozwiązalna!