

# Grupy

definicja: (Grupa przekształceń (automorfizmów) obiektu)

Dla danego obiektu kombinatorycznego  $S$  jest jego grupa przekształceń (symetrii, automorfizmów)  $G = \text{Aut}(S)$  powinna spełnić następujące warunki:

1. przekształcenie identycznościowe ' $e$ ' jest w  $G$
2. jeśli  $\varphi_1, \varphi_2 \in G$  to te przekształcenia można łączyć uzyskując  $\varphi = \varphi_1 \circ \varphi_2 \in G$
3. dla każdego  $\varphi \in G$  istnieje  $\varphi^{-1}$  taki, iż  $\varphi \varphi^{-1} = \varphi^{-1} \varphi = e$

Definicja (grupy).

Zbiór  $(G, \cdot)$ , gdzie  $\cdot : G \times G \rightarrow G$  jest działaniem dwuargumentowym, jest grupą gdy:

- |           |   |
|-----------|---|
| aksiomaty | <p>1. Łączność - działanie <math>\cdot</math> jest łączne</p> <p>2. Element neutralny - <math>\exists e \in G \forall g \in G \quad eg = ge = g</math></p> <p>3. Element odwrotny - <math>\forall g \in G \exists g' \in G \quad gg' = g'g = e</math></p> |
|-----------|---|

Jesli  $\cdot$  jest przemienne, to mówimy o grupie przemiennej (abelowej)

Lematy:

1. Element odwrotny do danego  $g \in G$  jest jedyny.
2. Element prawostronne odwrotny jest też lewostronne odwrotny.
3. Solątyczność jest jedyna.
4. Równania  $a x = b$  oraz  $x a = b$  mają określone jedno rozwiązanie

Definicja (półgrupy):

W ogólnosci rozważa się tez monoidy (półgrupy), w których nie zakładamy istnienia elementu odwrotnego (elementa odwrotnego ani identyczności)

Definicja (Tabelka działania)

Tabelka działania dla grupy  $G$  podaje wprost wszystkie możliwe  $16!^2$  wyników operacji  $\circ$ .

Przykład dla grupy Kleina ( $\{1, 3, 5, 7\}, \cdot \text{ mod } 8$ )

•	1	3	5	7	8
1	1	3	5	7	
3	3	1	7	5	
5	5	7	1	3	
7	7	5	3	1	
x			↑		
			X = y		

Także:

1. Kolejny wiersz i kolejna kolumna w tabelce działania jest permutacją elementów z  $G$

2. Dwa różne wiersze (dwie różne kolumny) są różne

3. Musi być dokładnie jeden wiersz (kolumna) w którym permutacja jest identycznością

Definicja (Iloczyn kartezjański grup; produkt prosty)

Dla grup  $G, H$  przez  $G \times H$  oznaczamy grupę zbiór zbiorek  $G \times H$  i działania po współrzędnych

$$(g, h) \circ (g', h') = (gg', hh')$$

Definiując tą iścieńie naturalnie rozszerzyć na ilorazach dowolnej ilości grup.

Definicja (Homomorfizm, izomorfizm grup)

Operację  $\varphi: G \rightarrow H$  nazywamy homomorfizmem grup, jeśli zachowuje działanie grupowe, tj.  $\varphi(a \cdot b) = \varphi(a) \varphi(b)$ .

$\varphi$  jest izomorfizmem, jeśli istnieje  $\varphi^{-1}$  które jest przekształceniem odwrotnym i homomorfizmem (wówczas szeregiem):  $\varphi \circ \varphi^{-1}$  są bijekcjami)

Przykład:

• Izomorfizm: grupa Kleina oraz  $\mathbb{Z}_2 \times \mathbb{Z}_2$

• Homomorfizm: mnożenie odwrotnymi liczbami nad  $F$ :  $H \rightarrow \text{Aut}(M)$

- Lemat:

Homomorfizm  $\varphi$  przeprowadza element neutralny (odwracalny) w neutralny (odwracalny).

Dekinija (Potęga, nad)

Potęgą elementu  $a$  nazywamy dowolny element postaci  $a^n$ , gdzie  $n \in \mathbb{Z}$ . Dla  $n=0$  oznacza on  $e$ , dla  $n > 1$ :  $a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{-razy}}$ , dla  $n < 0$ :

$$a^n = (a^{-1})^{-n}$$

Rząd elementu to najmniejsza dodatnia potęga  $n$  taka, że  $a^n = e$ . Rząd elementu jest nieskończony (nieokreślony), jeśli nie ma takiego skończonego  $n$ .

Rząd grupy to ilość jej elementów (może pole nie musi być skończonym)

Fakty:

1. W gr. skończonej każdy element ma rząd skończony.

2. Jeśli  $a \in G$  ma skończony rząd  $p$ , to  $a^l = e \Leftrightarrow p | l$ .

Dekinija (Podgrupy)

$H$  jest podgrupą  $G$ , co oznacza, że  $H \subseteq G$ , gdy  $H \subseteq G$  i  $H$  jest grupą, z tym samym działaniem.

Lematy

W grupie skończonej  $G$  zbiór  $H$  jest podgrupa, gdy jest zamknięty na działanie

2. W grupie, w której każdy elementu jest skończony,  $H$  jest podgrupa, gdy jest zamknięty na działanie.

## Definicja (Generowana)

Dla grupy  $G$  oraz zbioru  $A \subseteq G$  podgrupa generowana przez  $A$ , oznaczana jako  $\langle A \rangle$ , to najmniejsza podgrupa  $G$  zawierająca  $A$ . W takim wypadku mówimy, że  $A$  to zbiór generatorów tej podgrupy.

$$\text{Fakt: } (x_1^{2_1} \cdot x_2^{2_2} \cdot x_3^{2_3} \cdots x_k^{2_k})^{-1} = (x_k^{-1})^{2_k} (x_{k-1}^{-1})^{2_{k-1}} \cdots (x_1^{-1})^{2_1}$$

## Definicja (Postać zredukowana).

Niech  $a_1, \dots, a_k \in G$ , o iloczynie elementów  $a_1^{l_1} a_2^{l_2} \cdots a_k^{l_k}$  mówimy, że jest w postaci zredukowanej, jeśli  $a_i \in \{a_{i+1}^{-1} a_{i+1},\}$  dla każdego możliwego i oraz  $l_i \neq 0$  dla każdego  $i$ .

Lemat: Rozważmy ciąg elementów  $a_1^{l_1} a_2^{l_2} \cdots a_k^{l_k}$  oraz następujące reguły przepisywanie:

1.  $a_i^{l_i} a_{i+1}^{l_{i+1}} \rightarrow a_i^{l_i + l_{i+1}}$ , jeśli  $a_i = a_{i+1}$
2.  $a_i^{l_i} a_{i+1}^{l_{i+1}} \rightarrow a_i^{l_i - l_{i+1}}$ , jeśli  $a_i = a_{i+1}^{-1}$
3.  $a_i^0 = e$

Wtedy wynikął koncowy ciąg  $a_1^{l_1} a_2^{l_2} \cdots a_j^{l_j}$ :

1. Jest w postaci zredukowanej
2. Nie zależy od kolejności wykonywania redukcji
3.  $a_1^{l_1} a_2^{l_2} \cdots a_k^{l_k} = a_1^{l_1} a_2^{l_2} \cdots a_j^{l_j}$

Ponadto,  $a_1, a_2, a_3, \dots, a_j$  jest podciągiem  $a_1, a_2, \dots, a_k$

lemat:

Dla zbioru generatorów  $X$  podgrupa  $\langle X \rangle$  to obliczanie zbioru elementów postaci:  $\langle X \rangle = \{x_1^{2_1} x_2^{2_2} \cdots x_k^{2_k} : k \geq 0, x_1, \dots, x_k \in X, 2_1, \dots, 2_k \in \mathbb{Z}\}$ .

Bez zmniejszenia ogólnosu można dodatkowo założyć, że wszystkie elementy są w postaci zredukowanej.

Definicja (grupa cykliczna)

Grupa  $G$  jest grupą cykliczną, gdy  $G = \langle \{a\} \rangle$  dla pewnego  $a \in G$ , tzn. jest generowana przez jeden element.

Grupa cykliczna nie musi być skończona:  $\mathbb{Z} = \langle 1 \rangle$ .

Fakt

Każda grupa cykliczna jest przemienne

Lemat:

Dla każdego  $n < \infty$  wszystkie grupy cykliczne tego samego rozmiaru ( $2(2n+1)$ ) są izomorficzne. Wszystkie grupy cykliczne tego samego rozmiaru są izomorficzne ( $2(2,+)$ ).

Definicja (grupa wolna)

Niech  $\Sigma^{-1} = \{\alpha^{-1} : \alpha \in \Sigma\}$  będzie rozwarcie z  $\Sigma$ .

Grupa  $G$  o zbiorze generatorów  $\Sigma$  jest wolna (wolna generowana przez  $\Sigma$ ) jeśli dla dowolnego słowa  $w \in (\Sigma \cup \Sigma^{-1})^*$  w postaci zredukowanej zachodzi  $w =_G e \Rightarrow w = e$ .  
Przy tym pierwsza równość oznacza równosć w grupie, a druga równosć słów w  $(\Sigma \cup \Sigma^{-1})^*$ .

Poniżej  $nf(w)$ , oznacza postać zredukowaną  $w$ .

Lemat (Konstrukcja grupy wolnej)

Niech  $\Sigma$  to zbiór różnych elementów (liter),  $\Sigma^{-1} = \{\alpha^{-1} : \alpha \in \Sigma\}$  będzie rozwarcie z  $\Sigma$ . Rozpatrzymy zbiór  $nf((\Sigma \cup \Sigma^{-1})^*)$  wszystkich słów zredukowanych npt. z  $(\Sigma \cup \Sigma^{-1})^*$ .

Mnożenie elementów  $u \cdot w$  to postać zredukowana  $nf(uw)$

Słowa  $uw$ . Jako zdefiniowana grupa jest grupą wolną o generatorach  $\Sigma$ . Każda grupa wolna jest izomorficzna z tak skonstruowaną grupą wolną.

Stwierdzenie (Nielsen - Schreier)

Każda podgrupa grupy wolnej jest wolna.

Fakty:

- - - Lemot

Niech  $w_1, \dots, w_l \in (\Sigma \cup \Sigma^{-1})^*$  będą w postaci zredukowanej (jako słowa nad  $\Sigma \cup \Sigma^{-1}$ ). Niech  $w_1^{l_1}, w_2^{l_2}, \dots, w_n^{l_n}$  będą w postaci zredukowanej oraz  $n/(w_1^{l_1} w_2^{l_2} \dots w_n^{l_n}) = c$ .  
Według istnieje  $u, v, w \in \{w_1, w_1^{-1}, \dots, w_l, w_l^{-1}\}$ , takie, że  
 $w \leq v w$  istnieje ciąg skróćów, który skróci całe  $v$ ,  
tj. istnieją  $u', u'', w', w''$  w postaci zredukowanej, takie, że  
 $u = u' u''$ ,  $v = (u'')^{-1} (w'')^{-1}$ ,  $w = w' w''$   
oraz  $u \neq v^{-1} \neq w$  (wszystkie równości to równości rów.)

Dekiniję (grupy permutacji)

Grupa permutacji:  $S_n$  to zbiór wszystkich bijekcji ze zbioru  $\{1, 2, \dots, n\}$  w siebie; operacja jest składanie tj.  $(\sigma \cdot \tau)(i) = \tau(\sigma(i))$   
Permutacje zapisujemy jako dwuwierszową tabelkę

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \leftarrow \text{parowa rońce } \cancel{\text{takież nieparzyste}}$$

Z dodatkodnością do izomorfizmu kaido grupa jest grupą permutacji.

Swierdzenie (Cayley)

Dla każdej grupy  $G$  ( $0 \leq n$  elementach) istnieje podgrupa  $S_n$  izomorficzna  $G$ .

Dekiniję (cykl)

Cykl  $\sigma$  to taka permutacja, i.e. istnieją elementy  $\alpha_1, \dots, \alpha_n$ , że  $\sigma(\alpha_i) = \alpha_{i+1}$  (gdzie  $\sigma(\alpha_n) = \alpha_1$ ) a nie innych.

elementów jest identyczność. Cykl taki zapisujemy jako

$(\alpha_1, \alpha_2, \dots, \alpha_n)$ . Elementy  $\{\alpha_1, \dots, \alpha_n\}$  to dwiekrótnie cyklu lub nosimy cyklu, mówimy teraz o cyklu

na elementach  $\{\alpha_1, \dots, \alpha_n\}$ . Długość cyklu  $(\alpha_1, \dots, \alpha_n)$  to  $n$ ,

czyli są rozmienne jeśli ich nośniki nie mają

iliczących ich nośników, to jest zbiorem pustym.

Transpozyje to cykle dwielementowe.

## Lematy

1. Rząd cyklu to długość k cyk.
2. Dla cyklu  $(\alpha_1 \dots \alpha_n)$  permutacja odwrotna  
to  $(\alpha_1 \dots \alpha_n)^{-1} = (\alpha_1, \alpha_{n-1}, \dots, \alpha_1) = (\alpha_1 \dots \alpha_n)^{n-1}$
3. Jeśli  $\{c_i\}_{i=1}^k$  są parami rozłącznymi cyklami  
to  $c_1 c_2 \dots c_k$  jest ta sama permutacją,  
nieważnie od wybrana permutacji  $i_1 \dots i_k$  liczb  $1 \dots k$ .
4. Jeśli  $\{c_i\}_{i=1}^k$  są parami rozłącznymi cyklami,  
to rząd  $c_1 \dots c_k$  to suma rzędów poszczególnych  
cykli  $c_1 \dots c_k$
5. Jeśli  $\sigma = c_1 c_2 \dots c_k$ , gdzie  $c_1 \dots c_k$  są parami  
rozłączne, to  $\sigma^{-1} = c_1^{-1} c_2^{-1} \dots c_k^{-1}$

## Twierdzenie

1. Kilia permutacji  $\sigma$  jednocześnie (z dokładnością  
do kolejności cykli) rozkładają się na rozłączne cykle.
2. Cykl długości k jest złożeniem k-1 transpozycji
3. Kilia transpozycja jest złożeniem nieperystej  
lub k transpozycji elementów sąsiednich (mehanizm rozłączny)
4. Kilia permutacji do sie robiącą się przedstawić  
jako złożenie transpozycji (niekoniecznie rozłącznych)
5. Kilia permutacji do sie przedstawić jako  
złożenie transpozycji sąsiednich (niekoniecznie rozłącznych)
6. Grupa  $S_n$  jest generowana przez złożoną transpozycję (sąsiednich)

- Definicja (Inwersja, parzystość permutacji)

Dla  $f$  będącej bijekcją z podzbiorem liczb naturalnych

w ten sam zbiór (czyli w szczególności permutacji)

inwersja to para  $(i, j)$ , tzn.  $i < j$  oraz  $f(i) > f(j)$ .

Parzystość permutacji to parzystość ilości jej inwersji.

Znak  $\text{sgn}(\sigma)$  permutacji  $\sigma$  to  $+1$ , gdy  $\sigma$  jest parzysta  
 $i - 1$  gdy jest nieparzysta.

Lemat

Niech  $\sigma, \sigma' \in S_n$  będą permutacjami. Wtedy

$$\text{sgn}(\sigma' \sigma) = \text{sgn}(\sigma') \text{sgn}(\sigma)$$

$\text{sgn}$  jest homomorfizmem z  $S_n$  w  $\{-1, +1\}$

Lemat:

1. Czyli parzysty jest permutacją nieparzystą.

2. Czyli nieparzysty jest permutacją parzystą.

3. Parzystość permutacji to parzystość ilości wszystkich  
w rozwidleniu nie uglełek

4. Permutacja parzysta stanowi podgrupę  $A_n$ , która

ma  $\frac{n!}{2}$  permutacji

Wyznaczanie

Niech  $M = (\alpha_{ij})_{i,j=1 \dots n}$

$$|M| = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^n \alpha_{i, \sigma(i)} = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^n \alpha_{\sigma(i), i}$$

Działanie grupy na zbiorze

W podzbiorach grupy  $G$  definiujemy działanie:  $U \cdot W = \{uv : u \in U, v \in W\}$

jest ono lagrue, z tą zdefiniowaną dzialeńiem  $\{2^G, \circ\}$

jest monoidem. (ma jedność  $\{e\}$ ).

Ze względu na dziedzinę mnożenia względem sumy

$$U(V \cup W) = UV \cup UW \text{ oraz } (V \cup W)U = VU \cup WU$$

- - - Fakty:

Niech  $G$  grupa,  $H \leq G$  to jej podgrupa. Wtedy:

$$1. gG = Gg = G$$

$$2. gh = H \Leftrightarrow Hg = H \Leftrightarrow gh \in H \Leftrightarrow hg \in H \Leftrightarrow g \in H$$

Definicja (działanie grupy na zbiorze)

Mamy zbiór obiektów kombinatorycznych  $C$  oraz grupę permutacji

jego elementów  $S(C)$ , oznaczoną przez  $S$ . Działanie grupy

$G$  na  $C$  to homomorfizm z  $G$  w  $S$ . Zwykle zapisujemy  
to działanie jako  $g(c)$  lub nawet  $gc$ , pomijając homomorfizm.

Będziemy

działanie bieżącym też rozszerzyć do podzbiorów  $G$

w naturalny sposób: jeśli  $G$  działa na  $C$  to dla  $U \subseteq C$  definiujemy

$$U^G = \{gc : g \in G\}$$

Orbita elementu  $c$ :  $Gc = \{g(c) : g \in G\}$

Stabilizator elementu  $c$ :  $\{g \in G : g(c) = c\}$ . Zauważmy,

iż  $G_c$  to największy zbiór taki, iż  $g_c c = c$ .

Lemdy:

1. Niech  $G$  działa na zbiorze  $C$ , zapisz  $s \in C$ . Wtedy stabilizator  $G_s$  jest podgrupą  $G$

2. Niech  $G$  działa na zbiorze  $C$ , zapisz  $c, c' \in C$ . Wtedy

$O_c, O_{c'}$  są równie lub rożne

3. Niech  $G$  działa na zbiorze  $C$ , zapisz  $s \in C$ . Wtedy  $|O_s| \cdot |G_s| = |G|$

h. lemat Burnside'a - zbiór orbit działania grupy odpowiada  
zbiorem „nietrivialnych” względem działania grupy  
obiektów, np. krokiem „nietrivialnym” ze względu na obrót.

Deklinacja (punktów stać)

Dla grupy  $G$  działającej na zbiorze  $C$  mówimy, iż  $c \in C$  jest punktem staćym  $g \in G$  jeśli  $g(c) = c$ . Zbiór punktów staćych  $g$  oznaczamy przez:

$$\text{fix}(g) = \{c \in C : g(c) = c\}$$

Jasne (Lemat Burnside'a)

Niech  $G$  działa na zbiorze  $C \neq \emptyset$  będąc  
zbioru orbit tego działania. Wtedy:

$$|O| = \frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)|$$

Worstwa:

Deklinacja (worstwa).

Godz.  $H \leq G$  to worstwa lewostronne  $H$  ( $w_G H$ )

szq. zbioru postaci

$$aH = \{ah : h \in H\}$$

zaz. prawostronne

$$Ha = \{ha : h \in H\}$$

dla  $a \in G$ .

Zbiór worstw lewostronnych  $H \leq G$  oznaczamy przez  $G/H$

Lemat:

Niech  $H \leq G$

1. Kiedy działa worstwa  $H \leq G$  szq. rozłóżone.

2. Kiedy działa worstwa lewostronne (prawostronne)

$H \leq G$  szq. rozłączne lub identyczne

3.  $g_0 H = g_1 H \Leftrightarrow g_1^{-1} g_0 \in H \Leftrightarrow g_0^{-1} g_1 \in H$

4.  $Hg_0 = Hg_1 \Leftrightarrow g_1^{-1} g_0 \in H \Leftrightarrow g_0^{-1} g_1 \in H$

W grupie

W grupie skończonej:

Twierdzenia:

1. (Twierdzenie Lagrange'a) Rząd podgrupy dzieli rząd grupy
2. Rząd elementów którymi są grupy.
3. Rząd grupy o  $p$ -pierwszych elementach jest wykazany i kiedyż jej element (przez  $e$ ) jest generatorem.
4. Dla każdego  $e \in G$  zachodzi  $e^{|G|} = e$
5. (Małe twierdzenie Fermata'a) Jeśli  $p \nmid e$  to  $e^{p-1} \bmod p = 1$

Definicja (Indeks podgrupy)

Indeks podgrupy  $H$  względem grupy  $G$  to ilość  
wersji lewostronnych  $H$  w  $G$ , oznaczamy przez  $G:H$

Wartość jest taka sama, jeśli weźmiemy wersje prawostronne.

Zwykle zajmujemy się przypodobni, kiedyż indeks podgrupy  
jest skończony (a najczęściej tym, że obie grupy są  
skończone)

Pierścienie, ciała, ciała tylk modularne

Definicja (Pierścieni)

Pierścieniem, oznaczonym zwykle przez  $R$ , to zbiór z dwoma  
działaniami:  $+$ ,  $\cdot$ , spełniającymi warunki:

1.  $(R, \cdot)$  jest podgrupą (niekomutacyjne premiennosć)
2.  $(R, +)$  jest grupą premienną.

Ponadto zachodzi kolejność mnożenia względem dodawania

$$3. \alpha(b+c) = \alpha b + \alpha c; (b+c)\alpha = b\alpha + c\alpha$$

Pierścieniem jest z jednostką, jeśli ma element neutralny  
dla mnożenia. Pierścieniem jest premienny jeśli  $ab = ba$ .

### Definicje (cięcie)

Cięcie  $\mathbb{F}$  to pierścieniem przemiennej z jednością, w którym  $(\mathbb{F}, \cdot)$  jest grupą, tzn. każdy element ma element odwrotny oraz elementy neutralne dodawania i mnożenia się różne ( $0 \neq 1$ )

### Definicje (kongruencja modulo, $\mathbb{Z}_m$ )

$a \equiv b$  modulo  $m$  gdy  $m | (a - b)$  oznaczenie  $a \equiv_m b$

Rzeczywiście dla  $a \mod m = b \Leftrightarrow a \equiv_m b \quad \forall b \in \{1, 2, \dots, m-1\}$

Lemat:

Dla dowolnego  $m \in \mathbb{Z}_+$  relacja  $\equiv_m$  jest luoguwnością ze względu na mnożenie i dodawanie tzn.

Punktostoczenie  $n \mapsto n \mod m$  jest homomorfizmem pierścienia  $\mathbb{Z} : \mathbb{Z}_m$ .

So waine o tyle, iż wglomujec działanie mod m mnożymy dowolnie przekształcać się między  $\mathbb{Z}$  i  $\mathbb{Z}_m$ .

Prawo z  $\mathbb{Z}$  do  $\mathbb{Z}_m$  przechodzi jeśli nie uigwaja negacji.

### Definicje (formuły pozytywne)

Niech  $t_1, t_2$  będą wyrażeniami zbudowanymi z niewiadomych zmiennych  $x_1, x_2, \dots, x_n$ , elementów z A oraz działań  $+, \cdot$ .

Wtedy formuła  $\psi$  składająca się spójników  $\wedge, \vee$  oraz równości  $t_1 = t_2$ , gdzie  $t_1, t_2$  są jolej wgliej, nazywamy formułą pozytywną

Lemat:

Niech  $\varphi$  będzie formułą pozytywną iżas'  $\varphi : A \rightarrow B$  będzie homomorfizmem na pierścieniu B. Jeśli

$$Q_1 x_1 Q_2 x_2 \dots Q_n x_n \varphi (x_1, \dots, x_n)$$

zachodzi w A, to w B zachodzi:

$$Q_1 x_1 Q_2 x_2 \dots Q_n x_n \varphi' (x_1, \dots, x_n)$$

gdzie  $\varphi'$  jest uzyskanie z  $\varphi$  przez zamianę steigd  $z \in w$  wyrażenach przez  $\varphi(z)$  zas'  $Q_i$  jest koniugatorem uniwersalnym bądż egzystencjalnym.

## Definicja (NWD)

Liczba  $0 \neq k \in \mathbb{N}$  jest największym wspólnym dzielnikiem  $a, b \in \mathbb{Z}$ , jeśli  $k | a$ ,  $k | b$  i dla każdego  $l$  zachodzi  $|l|a, |l|b \rightarrow |l|k$ .

NWD jest największy w sensie poszukiwanego zdefiniowanego przez podzielność

Lemat:

Niech  $k \neq 0$ , oznaczmy  $a, b, k \in \mathbb{Z}$  wtedy:

1. Jeśli  $k | a$  i  $k | b$  to  $k | (a+b)$  i  $k | (a-b)$
2. Jeśli  $k | a$  i  $k | b$  to  $k | (a \text{ mod } b)$
3. Jeśli  $k | (a \text{ mod } b)$  i  $k | b$  to  $k | a$

Lemat:

W ramach algorytmu Euklidesa mamy przedstawione liczby reprezentowane jako kombinacje liniowe (o współczynnikach całkowitych)  $a$  oraz  $b$ :

Lemat:

Dla  $a, b \in \mathbb{Z}$  istnieją  $x, y \in \mathbb{Z}$  takie, że

$$\text{nwd}(a, b) = xa + yb$$

Dzieliąc jedna z tych liczb jest prosty, jeśli nie dzieli się drugą. Dla dalszych liczb te mamy wybrać takie, że  $|x_1| < b$ ,  $|y_1| < a$ . Jeśli  $\text{nwd}(a, b) = 1$  to są dzielone dwie takie wyrażenia.

Lemat:

W pierścieniu  $\mathbb{Z}_m$  element  $a$  ma element odwrotny, utw. goły za gnd  $(a, m) = 1$ .

## Definicja (elementy odwracalne)

Element  $a$  pierścienia  $R$  nazywamy odwracalnym, jeśli istnieje  $b \in R$  takie, że  $ab = 1$ .

Zbiór elementów odwracalnych pierścienia  $R$  oznaczamy jako  $R^*$ .

## Twierdzenie

1. Dla dowolnego pierścienia  $R$  z jednostką jedności

zbiór elementów odwracalnych  $R^*$  jest grupą na mnożenie  
(którego  $2_m^*$  nie ma struktury pierścienia)

2. Dla ciała skończonego  $F$  grupa  $F^*$  jest cykliczna

## Definicja (Szyfr Eulera)

$\varphi(m)$  to liczba liczb względnie pierwszych z  $m$ , mniejszych  
wtedy  $\varphi(m) = 1 \pmod{m}$ .

## Twierdzenie Eulera

Niech  $a, m$  są względnie pierwsze. Wtedy  $a^{\varphi(m)} = 1 \pmod{m}$

## Definicja (Produkt pierścieni)

Produkt pierścieni definiujemy standardowo.

Dla pierścieni  $R, R'$  ich produkt to  $R \times R'$   
i dzieliąc na współrzędny

## Lematy:

1.  $R \times R'$  i  $R' \times R$  są izomorficzne.

2. produkt kartezjański jest tacyż (z dodatkością

dowód izomorfizmu):  $R_1 \times (R_2 \times R_3) \cong (R_1 \times R_2) \times R_3$

szczególnie

3. jeśli  $R_1$  jest izomorficzne z  $R'_1$  i  $R_2$  jest izomorficzne

z  $R'_2$ , to  $R_1 \times R_2$  jest izomorficzne z  $R'_1 \times R'_2$

## Twierdzenie (lubiącie Twierdzenie o reszta)

### ... Świadczenie (Chin'skie twierdzenie o restach)

Jesli  $m_1, m_2, \dots, m_k$  sa pierwiastkami względnie pierwszymi, to naturalny homomorfizm z  $\mathbb{Z}_{m_1 m_2 \dots m_k}$  w  $\prod_{i=1}^{m_k} \mathbb{Z}_{m_i}$ , gdzie na ilej wyższej biernicy modulo  $\mathbb{Z}_{m_i}$ , jest izomorfizmem.

### Twierdzenie / Lematy

1. Grupa  $\mathbb{Z}_p^*$  jest cykliczna

2. Jesli  $p$  jest liczba pierwsza, to  $a^2 \equiv_p b^2$  wtedy i tylko

$$a \equiv_p b \vee a \equiv_p -b$$

3. Jesli  $p$  jest pierwsza, to w  $\mathbb{Z}_p^*$  jesli  $a$  jest

$$\text{kwadratem} \text{ to } a^{\frac{(p-1)/2}{2}} = 1 \text{ wtedy i tylko } a^{\frac{(p-1)/2}{2}} = -1$$

4. Dla  $c \in \mathbb{Z}_p$  mamy  $c^{\frac{(p-1)/2}{2}} = 1 \vee (-c)^{\frac{(p-1)/2}{2}} = 1$

### Mielomiany

#### Definicja (Mielomian)

Mielomianem  $f$  to uogół.  $(\alpha_0, \alpha_1, \dots, \alpha_n)$  myślimy

o nich jako o  $\sum \alpha_i x_i^i$ . Zwykle zauważamy, iż

$\alpha_n \neq 0$ , wpp dla  $n > 0$  mówimy

$$\alpha_0, \alpha_1, \dots, \alpha_n \in \mathbb{Q}, \alpha_0, \alpha_1, \dots, \alpha_{n-1} \in \mathbb{Q}$$

Mnożenie, dzielenie obowiązuje oraz stwierdzamy, że reszta jest znana

jedynie małe zmienne  $\deg(f) = -\infty$

Jesli o wielomianach myślimy jak o uogół.,

to mnożenie (które jest dobrze zdefiniowane nawet

jesli pierwiastek jest nieprzemieniony) jest wzajemne

splotem.

Lemat: (Porównanie definicji)

$R[x]$  z mnożeniem zdefiniowanym jako splot jest

pierwiastkiem. Jesli  $R$  jest pierwiastkiem pierwiastkowym

(z jednostką), to  $R[x]$  ten jest pierwiastkiem przemienionym (z jednostką)

## Licze, rozszerzenie iota

- - - Lemat

Niech  $f, g \in \mathbb{R}[x]$

Wtedy :

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

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

Jesli  $\mathbb{R}$  jest ciałem to

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

Dzielenie (Evaluacja)

Wielomian  $f \in \mathbb{R}[x]$  równy  $(a_0, \dots, a_n)$  mamy

żej postrzeganej jako funkcji  $\mathbb{R} \rightarrow \mathbb{R}$  w  $\mathbb{R}$ , zdefiniowaną  
w naturalny sposób:

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

Lemat

Niech  $f, g \in \mathbb{R}[x]$  i  $p \in \mathbb{R}$ . Wtedy

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

Jesli  $\mathbb{R}$  jest pierwiastkowy to dodatkowo

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

Lemat (Dzielenie wielomianów)

Niech  $\mathbb{F}$  będzie ciałem a  $\mathbb{F}[x]$  pierścieniem wielomianów

o współczynnikach z  $\mathbb{F}$ . Dla wielomianów  $f, g$  a tego

pierścienia, o stopniach  $m = \deg(f)$  oraz  $n = \deg(g) \neq -\infty$   
istnieje dokładnie jedna para wielomianów  $q, r$ ,

takie że  $f = qg + r$ , gdzie  $\deg(r) < \deg(g)$ .

Wielomian te mamy zdefiniowane wykresami.

Dzielenie (Podzielność wielomianów)

Wielomian  $f$  jest podzielny przez wielomian  $g$ ,

jesli reszta ~~została~~ z dzielenia  $f$  przez  $g$  wynosi 0.

Zapisujemy to jako  $f \mid g$

- Fakt

$f \mid g \Leftrightarrow$  istnieje wielomian  $q$ , takie że  $g = fq$

Lematy:

1. Kolejny wielomian dzieli 0.

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

3. Jeśli  $f$  dzieli  $g$  i  $\deg(g) = 0$  to  $f \mid \deg(f) = 0$

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

Definicja (wielomian nienormatywny)

Wielomian  $f \in R[x]$  jest nienormatywny 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 nienormatywne.

Definicja (NWD wielomianów)

Największy wspólny dzielnik wielomianów  $f, g$  to

też wielomian  $h$ , że  $h \mid f$  i  $h \mid g$  oraz

jeśli  $h' \mid f$  i  $h' \mid g$  to  $h' \mid h$ .

Zauważmy, że nwd wielomianów jest określone

zgodnością do stałej mnożnikowej.

Lemat:

Kolejne dwa wielomiany  $p, q$ , mają największą wspólną

dzielnik. Jest on postaci  $a_1p + b_1q$  dla pewnych

wielomianów  $a, b$ .

Lemat:

Niech  $f, f', g, g', h \in F[x]$ . Jeśli  $f = f'h$ ,  $g = g'h$  to

$$\text{nwd}(f, g) = h \text{ nwd}(f', g')$$

jeśli  $f = f'h$  oraz  $\text{nwd}(h, g)$  jest stałe to

$$\text{nwd}(f, g) = \text{nwd}(f', g')$$

- Lemat:

Jesli  $f$  jest nierozkładalna oraz  $f(p_1, p_2, \dots, p_k)$  to  $f(p_i)$  dla którego:

lemat:

Jesli  $f_i$  sa nierozkładalne oraz para  $(f_i, f_j)$  jest stała  
dla  $i \neq j$  oraz  $f_i \mid g$  i  $f_j \mid g$ .

Zwierdzenie (Bezout)

Jesli  $\bar{f}$  jest ciętem,  $\mathbb{F}[x]$  pierścieniem wielomianów

o współczynnikach z tego ciała res'  $f$ ,  $(x-c) \in \mathbb{F}[x]$   
wielomianami z tego pierścienia, to reszta z dzielenia  
 $f$  przez  $(x-c)$  to  $\bar{f}(c)$ .

Jesli  $(x-c) \mid f$  to  $\bar{f}(c) = 0$

Zwierdzenie:

Wielomian  $0 \neq f \in \mathbb{F}[x]$  ma najwyżej  $\deg(f)$  różnych  
pierwiastków.

Wnioski:

1. Jesli ewaluacja dwóch wielomianów stopnia co najwyżej  
n maż te same wartości w n+1 punktach, to sa róznne.  
(Wiele nieskończonych dwóch ~~kontynuujących~~ wielomianów  
maż słuchowią kiedy wartości wspólnych).

2. (Interpolacja wielomianu) Jesli 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

Ciąg, rozszerzenie cięcia

- Definicja (charakterystyka cięcia; cięcie prostte)

Dla cięcia  $F$  jego charakterystyka to nad 1 w grupie oddzielnej cięcia generowane przez 1 w cięciu  $F$  to cięcie prostte.

Lemat:

(najm.) Charakterystyka cięcia to albo  $\top$  albo kielce pierwsze p.

W pierwszym przypadku cięcie prostte to  $\emptyset$ , w drugim:  $\mathbb{Z}_p$ .

Lemat:

Cięcie jest przednim liniowym nad swoim cięciem prostym.

Konstrukcja cięcia (skonstruowanie)

Naszym celem obecnie jest konstrukcja cięcia skonstruowanego.

Skonstruujemy cięcie wydzielone przez pierścienie  $\mathbb{F}[\lambda]$  i  $\mathbb{J}$  przez odpowiednio kongruencje. Jest to analogiczna konstrukcja do konstruowania  $\mathbb{Z}_p$  jako wydzielania  $\mathbb{Z}$  przez kongruencję podzielności przez kielce pierwsze. Naszym ciętem względem jest cięcie skonstruowane (np.  $\mathbb{Z}_p$ ) ale wszystko dla innych niż obecnie cięcia o charakterystyce  $\top$ .

Definicja (Kongruencja modelu wielomianów)

Dla ciała  $F$  oraz pierścienia wielomianów  $\mathbb{F}[\lambda]$

o współczynnikach z tego cięcia oraz wielomianu  $h \in \mathbb{F}[\lambda]$

definiujemy kongruencję  $\equiv_h$  na  $\mathbb{F}[\lambda]$ :

$$f \equiv_h g \Leftrightarrow h | (f - g)$$

Lemat:

Dla pierścienia wielomianów o współczynnikach z cięcia  $\mathbb{F}[\lambda]$

brz. wielomianu  $h \in \mathbb{F}[\lambda]$  z tego pierścienia relacja

$\equiv_h$  na  $\mathbb{F}[\lambda]$  jest relacją równoważności.

Operacje  $+$ ,  $\cdot$ ,  $\lambda^q$  dobrze zdefiniowane w  $\mathbb{F}[\lambda] / \equiv_h$

W szczególności,  $\mathbb{F}[\lambda] / \equiv_h$  jest pierścieniem przemiennym z jednostką

- - lemat:

Jesli wielomian  $h \in \mathbb{F}[x]$  jest nierozkładalny,  
to w  $\mathbb{F}[x]/\equiv_n$  istnieje element odwrotny dla  $f \in \mathbb{F}$ .

Twierdzenie

1. Jesli wielomian  $h$  jest nierozkładalny, to w  $\mathbb{F}[x]/\equiv_n$   
(jako przestrzeń liniowa nad  $\mathbb{F}$ ) ma wymiar  $\deg(h)$ .

Jesli  $\mathbb{F}$  jest skończona, to taki rozszerzenie ma  $|\mathbb{F}|^{\deg h}$  elementów.

2. Dwa ciała skończone o  $p^k$  elementach są izomorficzne

lemat

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

Definicja (odległość Hamminga)

Odległość Hamminga jest ilość pozycji, na których różnią się dwa wektory. Definicja:

$d(v, v')_2$  Odległość sprawia: "symetryczność",

spójność warunku trójkatnego i jeśli  $d(v, v') = 0$  to  $v = v'$ .

Twierdzenie (ogniwienie singleton)

Jesli w zbiorze  $\mathbb{F}^n$  wybierzmy  $|\mathbb{F}|^k$  wektorów,

to kiedyś dwa mają odległość najwyżej  $n-k+1$ .

Definicja (Error locator polynomial)

Dla zbioru pozycji błędów  $S$  zdefiniujemy (perz notatki)

$$E(x) = \prod_{i \in S} (x - \alpha_i)$$

$$\deg(E) \leq e \leq \lfloor \frac{n-k}{2} \rfloor$$

$$Q = E^{-1} \cap \text{zera}$$

- Definicja (cięto algebraiczne domknięcie)

Cięto  $\bar{F}$  jest algebraiczne domknięte, jeśli każdy wielomian niewzględny jest stopnia 1.

Folge:

1. Cięto  $\bar{F}$  jest algebraiczne domknięcie wtedy gdy

każdy wielomian ma pierwiastek.

2. Cięto algebraiczne domknięte jest nieskończone.

Zwierdzenie

Dla ciała  $\bar{F}$  istnieje  $\bar{F}' \supseteq \bar{F}$ , które jest algebraiczne domknięte over dziedziny  $\bar{F}'$  obugie do  $\bar{F}$  to dziedziny  $\bar{F}$ .

Definicja (Rozszerzenie ciała)

Dla ciała  $\bar{F}$  pier  $\bar{F} < S >$  oznaczamy najmniejsze cieło zawierające  $\bar{F}, S$ . Rozszerzenie

Rozszerzenie  $\bar{F} < \alpha >$  jest proste przestępne, jeśli ' $\alpha$ ' nie jest pierwiastkiem żadnego wielomianu z  $\bar{F}[x]$

Także ' $\alpha$ ' nowym nazywamy przesłepnym. Jest algebraiczne, jeśli ' $\alpha$ ' jest pierwiastkiem jakaś wielomianu z  $\bar{F}[x]$ .

Definicja (cięto ułamków prostych)

Rozważmy cieło  $\bar{F}$  over wielomiany nad nim  $\bar{F}[x]$ .

Należałoby  $\frac{f}{g} : f, g \in \bar{F}[x], g \neq 0$ . uprawdopodobnić

teżżej równowartości