Matematyka dyskretna

Wykład 9: Grupy skończone

Gniewomir Sarbicki

Grupy cykliczne

Definicja:

Jeżeli każdy element grupy G jest postaci a^n dla pewnego $a \in G$, to mówimy, że grupa G jest **grupą cykliczną** o **generatorze** a. Zapisujemy to jako $G = \langle a \rangle$

Fakt: Dla każdego elementu $a \in G$ zbiór jego potęg tworzy podgrupę cykliczną grupy G

Definicja:

Dla każdego elementu $a \in G$ określamy **rząd elementu** a jako rząd podgrupy cyklicznej generowanej przez ten element. Równoważnie: jest to najmniejsza liczba naturalna k dla której $a^k = e$.

Grupy cykliczne

Wniosek: (z tw. Lagrange'a) rząd elementu dzieli rząd grupy.

Wniosek: Każda grupa G o rzędzie pierwszym:

- jest grupą cykliczną
- ma tylko dwie podgrupy: $\{e\}$ oraz G
- każdy element różny od e jest jej generatorem

Twierdzenie: (Klasyfikacja grup cyklicznych)

Grupa cykliczna G jest izomorficzna z:

- $\mathbb{Z}_n$, gdzie $n = (G : e)$
- $\mathbb{Z}$, gdy jej rząd jest nieskończony

Możliwe grupy o rzędzie złożonym

Rozważmy grupę o 6 elementach.

Jeżeli zawiera element o rzędzie 6, to jest cykliczna i izomorficzna z $\mathbb{Z}_6$. W przeciwnym wypadku elementy mogą mieć rzędy 2 lub 3.

Twierdzenie: (Sylowa)

Jeżeli $(G : e) = p^n \cdot m$, gdzie p jest liczbą pierwszą i $NWD(p, m) = 1$, to:

- Istnieje w G podgrupa rzędu p^n. Ilość tych podgrup n_p jest równa 1 (mod p) i $n_p | m$.
- Podgrupy te są ze sobą sprzężone - jedynym elementem należącym do dwóch z nich jest e.

Wniosek: Jedyną grupą niecykliczną rzędu 6 jest grupa S_3

Ćwiczenie: Wyznacz wszystkie grupy rzędu 15.

Tabelka Cayleya

W grupie symetrii trójkąta równobocznego mamy dwa obroty (wzajemnie odwrotne) i trzy odbicia. Tabelką działania jest:

e	I_1	I_2	I_3	O_{120}	O_{240}
I_1	e	O_{120}	O_{240}	I_2	I_3
I_2	O_{240}	e	O_{120}	I_3	I_1
I_3	O_{120}	O_{240}	e	I_1	I_2
O_{120}	I_3	I_1	I_2	O_{240}	e
O_{240}	I_2	I_3	I_1	e	O_{120}

Ćwiczenie: Wypełnij tabelkę działań dla grupy symetrii kwadratu

Twierdzenie Cayleya

W tabelce, każdy wiersz jest permutacją wiersza pierwszego. Tabelka przypisuje każdemu elementowi grupy pewną permutację ciągu n elementów.

Twierdzenie: (Cayleya)

Każda grupa rzędu n jest izomorficzna z podgrupą S_n (grupy permutacji zbioru n-elementowego)

Podgrup rzędu n grupy S_n (o $n!$ elementach) nie jest tak dużo jak by się mogło wydawać

`http://en.wikipedia.org/wiki/List_of_small_groups`

Grupy $\mathbb{Z}_n^*$

Definicja:

Przez $\mathbb{Z}_n^*$ oznaczamy zbiór elementów odwracalnych pierścienia $\mathbb{Z}_n$. Zbiór ten jest grupą abelową ze względu na mnożenie.
Rząd tej grupy określa funkcja Eulera $\phi(n)$.

Definicja:

Pierwiastkiem pierwotnym z liczby p nazywamy każdy generator grupy $\mathbb{Z}_p^*$, czyli element b dla którego:

$$b^{\phi(n)} = 1 \pmod{p} \qquad \forall r < \phi(b) \;\; b^r \neq 1 \pmod{p}$$

Grupy $\mathbb{Z}_n^*$

Twierdzenie:

Jeżeli liczba p jest pierwsza, to istnieje jej pierwiastek pierwotny

W drugą stronę implikacja nie zachodzi.

Przykład: Kolejne potęgi liczby 5 w $\mathbb{Z}_6$ wynoszą $5, 1, 5, \ldots$, zatem rząd elementu wynosi 2, tyle ile $\phi(6)$.

Fakt:

Jeżeli w $\mathbb{Z}_n^*$ istnieje element rzędu $n-1$, to n jest liczbą pierwszą.

Twierdzenie:

Jeżeli G jest grupą abelową, oraz jej dwa elementy mają rzędy p i q, to ich iloczyn ma rząd $NWW(p, q)$.

Logarytm dyskretny

Definicja:

Logarytmem dyskretnym z liczby x przy podstawie b modulo n nazywamy liczbę $y \in \{0, \phi(n) - 1\}$ taką, że

$$b^y = x$$

Dziedziną logarytmu są elementy $\mathbb{Z}_n^*$.

$$\log_b : \mathbb{Z}_n^* \to \{0, \phi(n) - 1\}$$

Uwaga: Żeby logarytm był dobrze określony w $\mathbb{Z}_n^*$, za podstawę można brać tylko generator grupy $\mathbb{Z}_n^*$. Logarytm jest określony tylko dla grup cyklicznych.

Logarytm dyskretny

Przykład: Tabelka wartości logarytmu przy podstawie 2 w ciele $\mathbb{Z}_{11}$. Ciąg potęg 2: $1, 2, 4, 8, 5, 10, 9, 7, 3, 6$

0	1	2	3	4	5	6	7	8	9	10
-	0	1	8	2	4	9	7	3	6	5

Przykład: Tabelka wartości logarytmu przy podstawie 7 w ciele $\mathbb{Z}_{11}$. Ciąg potęg 7: $1, 7, 5, 2, 3, 10, 4, 6, 9, 8$

0	1	2	3	4	5	6	7	8	9	10
-	0	3	4	6	2	7	1	9	8	5

Przykład: Tabelka wartości logarytmu przy podstawie 3 w pierścieniu $\mathbb{Z}_{10}$. Ciąg potęg 3: $1, 3, 9, 7$

0	1	2	3	4	5	6	7	8	9
-	0	-	1	-	-	-	3	-	2

Logarytm dyskretny

Logarytm dyskretny jest funkcją różnowartościową.
Grupa cykliczna $(\mathbb{Z}_n^*, \cdot)$ jest izomorficzna z grupą cykliczną $(\mathbb{Z}_{\phi(n)}, +)$.
Izomorfizm ten jest zadany przez logarytm dyskretny.
Izomorfizm odwrotny zadany jest przez funkcję wykładniczą o tej samej podstawie.

Podobnie, dla liczb rzeczywistych logarytm o dowolnej podstawie $y = \log_a(x)$ ustala izomorfizm pomiędzy grupami $(\mathbb{R}_+, \cdot)$ oraz $(\mathbb{R}, +)$. Izomorfizmem odwrotnym jest funkcja $x = a^y$.