

WYKŁAD 16

Rozdział 22

$\mathbb{F}$ - ciało

$\mathbb{F}^*$ - zbiór el. odwr. $\mathbb{F} \setminus \{0\}$

Skończone $\mathbb{F}^*$ jest cykliczne

$(\mathbb{F}^*, \cdot)$

C_n

$g^n = e$

$x^n = 1$

Chcemy pokazać, że jeśli $\mathbb{F}$ jest skończone, to $\mathbb{F}^*$ jest cykliczna. Dowód opiera się na wykazaniu, że istnieje w niej element rzędu $n = |\mathbb{F}| - 1$, co daje, że jest on generatorem. Aby to pokazać, będziemy dla każdego $k \leq n$ zliczać w grupie cyklicznej n elementowej oraz w grupie $\mathbb{F}^*$ elementy, które są rzędu k . Zauważmy, że wystarczy pokazać, że w grupie $\mathbb{F}^*$ jest nie więcej, niż w C_n (grupa cykliczna o n elementach).

Lemat 22.1. Niech $R(G, k)$ oznacza liczbę elementów rzędu k w grupie abelowej G . Jeśli dla grupy skończonej G o n elementach zachodzi dla każdego k

$$R(G, k) \leq R(C_n, k)$$

to G jest izomorficzne z C_n .

$$R(G, n) = R(C_n, n)$$

$$\sum_k R(G, k) = n \leq \sum_k R(C_n, k) = n$$

$$g^k = e$$

Niestety, zliczanie elementów rzędu k jest dość kłopotliwe. Łatwiej jest zliczyć elementy, których rząd *dzieli* k .

22.1 Rzędy elementów w grupie cyklicznej

Lemat 22.2. Niech g będzie generatorem grupy cyklicznej G o n elementach. Wtedy g^m jest jej generatorem $\iff \gcd(m, n) = 1$. W szczególności G ma $\varphi(n)$ generatorów.

$\Rightarrow$
 g^m jest generatorem

$$\begin{aligned} (g^m)^a &= g \\ g^{am} &= g^{n \cdot h + r} = (g^{nm})^h \cdot g^r = g^r = g^1 \end{aligned}$$

$\underbrace{(g^{nm})^h}_e$ $r < n$ $r = 1$

$$\begin{aligned} a \cdot m &= n \cdot h + 1 \\ \gcd(m, n) & \mid 1 \\ &= 1 \end{aligned}$$

$$\Leftarrow \gcd(m, n) = 1 \quad am + bn = 1$$

$$\langle g^m \rangle \ni g \Rightarrow \langle g^m \rangle \supseteq \langle g \rangle = G$$

$$(g^m)^a = g^{-bm+1} = \underbrace{g^{-bm}}_e \cdot g^1 = g$$

Na ćwiczeniach pokazaliśmy lemat:

Lemat 22.3 (Przypomnienie). Jeśli G jest cykliczna, to każda jej podgrupa jest cykliczna.

Lemat 22.4. Niech G będzie grupą cykliczną rzędu n .



1. W G istnieje element rzędu d wtedy i tylko wtedy, gdy $d \mid n$.
2. Niech $d' \mid d$, $d \mid n$. Wtedy podgrupa $G_d \leq G$ generowana przez element rzędu d zawiera dokładnie $\varphi(d')$ elementów rzędu d' , są to wszystkie elementy rzędu d' z grupy G .
3. Grupa G zawiera dokładnie d elementów spełniających równanie $x^d = e$, są to dokładnie elementy podgrupy G_d .

Ad 1 d

$g \in \text{element}$ rzędu d
 rzędu el. drżci rzędu grupy

$$\Leftarrow d \mid m \quad m = d \cdot \frac{m}{d} \quad d \mid m$$

naturalne

$$(g^{m/d})^d = g^{m/d \cdot d} = g^m = e$$

nie może być mniejszy niż d

$$g^{n/d \cdot d'} = e \quad \frac{n \cdot d'}{d} \geq m \quad d' \geq d$$

Ad 2

Popatrzmy na podgrupę G generowaną przez wszystkie el. rzędu d .

$$\langle g_1, g_2, \dots, g_n \rangle \in G$$

te są cykliczne.

$$\langle g \rangle = \langle g_1, \dots, g_n \rangle$$

$$\text{rzd } g \leq d$$

rzędu d , grupa pr.

$$g_1 g_2 g_3 g_4 g_5 \dots$$

$$(g_1^{t_1} g_2^{t_2} \dots g_n^{t_n})^d = e$$

$$g^{d'} = e \quad d' < d$$

$$\text{rzd } d \geq d$$

< d.

$$\text{wszystko w } \langle g \rangle \quad \text{można } \text{rzd } d \leq d' < d$$

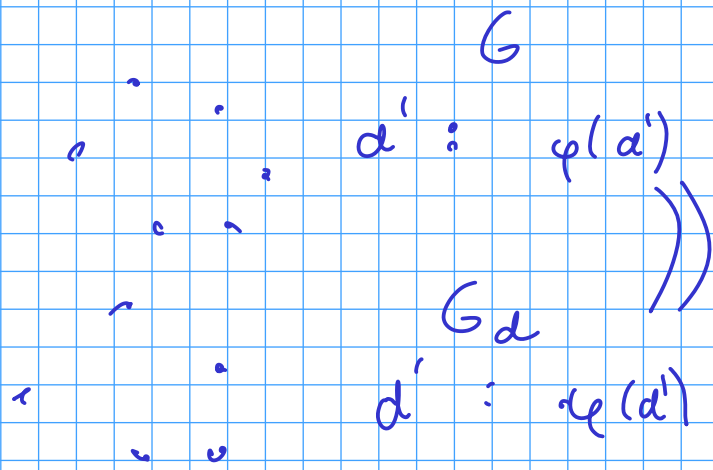
$$\text{byli } g = g_i$$

$$\langle g_i \rangle \quad \text{to może być } \varphi(d) \text{ el. rzędu } d.$$

dołączanie wszystkich el. rzędu d w grupie G .

To są dołączanie wszystkich el. rzędu d w G .

$d' | d$



Lemat 22.5. Niech G będzie grupą skończoną rzędu n . Jeśli dla dowolnego $k \in \mathbb{N}$ zbiór $\{g \in G : g^k = e\}$ ma najwyżej k elementów, to G jest cykliczna.

$$\forall k \quad R(G, k) \leq R(C_n, k) \Rightarrow G = C_n$$

$|G| = n$

k czy w G jest el. rzędu k ?

Nie ma $\Rightarrow$ ok

jest $k | n$

$g \in G$ $\langle g \rangle$ ma k elementów
 $h \in \langle g \rangle$ $h^k = e$

Nie ma innych el. sp. $h^k = e$, poza $\langle g \rangle$

Wszystkie el. rzędu k są w $\langle g \rangle$ $\varphi(k)$ el. rzędu k

w C_n to jest $\varphi(k)$ el. rzędu k ($k | n$)

$$R(k, G) = \varphi(k) = R(k, C_n) \leq$$

$$G \cong C_n$$

22.2 Rzędy elementów w $\mathbb{F}^*$

Pokazaliśmy wcześniej, że:

Lemat 22.6 (Przypomnienie). Równanie $x^k = 1$ ma w ciele skończonym $\mathbb{F}$ najwyżej k różnych pierwiastków.

Twierdzenie 22.7. Grupa $\mathbb{F}^*$ jest cykliczna.

$\mathbb{F}^*$ ustalony k

$$x^k = 1$$

$k \nmid n$ nie mo.
now.

$k \mid n$

$$x^k = 1$$

mo. $\leq k$ pierw.

$\Rightarrow$