Algebra I

Wykład XV

Grzegorz Bobiński (UMK)

Definicja

Jeśli G jest grupą, która działa na zbiorze X, to definiujemy

$$X^G := \{x \in X : G * x = \{x\}\}.$$

Elementy zbioru X^G nazywamy punktami stałymi dla działania grupy G na X.

Lemat 4.8

Jeśli grupa G działa na zbiorze skończonym X, $p \in \mathbb{P}$ oraz $|G| = p^n$, $n \in \mathbb{N}_+$, to

$$|X^G| \equiv |X| \pmod{p}.$$

Przypomnienie

(4.6): Orbity tworzą podział zbioru X.
(4.7): Liczba elementów orbity dzieli rząd grupy.

Dowód

(4.6) $\implies$ istnieją $x_1, \ldots, x_k \in X$ takie, że

$$|X| = |X^G| + |G * x_1| + \cdots + |G * x_k|,$$

zbiory X^G, $G * x_1$, $\ldots$, $G * x_k$ są parami rozłączne oraz $|G * x_i| > 1$ dla każdego i.
(4.7) $\implies$ $|G * x_i| \mid |G|$ dla każdego i.
Ponieważ $|G * x_i| > 1$, $|G| = p^n$, oraz $p \in \mathbb{P}$ jest liczbą pierwszą, więc $p \mid |G * x_i|$, $i = 1, \ldots, n$, co kończy dowód. $\square$

Lemat 4.8

Jeśli grupa H działa na zbiorze skończonym X, $p \in \mathbb{P}$ oraz $|H| = p^n$, $n \in \mathbb{N}_+$, to

$$|X^H| \equiv |X| \pmod{p}.$$

Twierdzenie 4.9 (Cauchy)

Jeśli $p \in \mathbb{P}$ oraz $p \mid |G|$, to istnieje $g \in G$ taki, że $\operatorname{ord}(g) = p$.

Dowód

Niech

$$X := \{(g_1, \ldots, g_p) \in G^p : g_1 \cdots g_p = 1\}.$$

Zauważmy, że $|X| = |G|^{p-1}$, zatem $p \mid |X|$.

Rozważmy działanie grupy $\mathbb{Z}_p$ na zbiorze X dane wzorem

$$k * (g_1, \ldots, g_p) \mapsto (g_{k+1}, \ldots, g_p, g_1, \ldots, g_k) \qquad (k \in \mathbb{Z}_p,\ (g_1, \ldots, g_p) \in X).$$

(Należy sprawdzić, że jeśli $g_1 \cdots g_p = 1$, to $g_{k+1} \cdots g_p g_1 \cdots g_k = 1$).

Zauważmy, że

$$X^{\mathbb{Z}_p} = \{(g, \ldots, g) \mid g \in G \text{ i } g^p = 1\}.$$

(4.8) $\implies$ $p \mid |X^{\mathbb{Z}_p}|$.

Ponieważ $(1, \ldots, 1) \in X^{\mathbb{Z}_p}$, więc $|X^{\mathbb{Z}_p}| \geq p > 1$.

Zatem istnieje $g \neq 1$ takie, że $g^p = 1$.

Ponieważ $p \in \mathbb{P}$ jest liczbą pierwszą, więc (3.8) $\implies$ $\operatorname{ord}(g) = p$. $\square$

Twierdzenie 4.9 (Cauchy)

Jeśli $p \in \mathbb{P}$ oraz $p \mid |G|$, to istnieje $g \in G$ taki, że $\mathrm{ord}(g) = p$.

Definicja

Jeśli $p \in \mathbb{P}$, to grupę G nazwiemy *p*-grupą, jeśli dla każdego $g \in G$, $\mathrm{ord}(g) = p^n$ dla pewnego $n \in \mathbb{N}$.

Jeśli $H \leq G$ i H jest p-grupą, to H nazywamy *p*-podgrupą grupy G.

Wniosek 4.10

Jeśli $p \in \mathbb{P}$ oraz $|G| < \infty$, to

$$G \text{ jest } p\text{-grupą} \iff |G| = p^n \text{ dla pewnego } n \in \mathbb{N}.$$

Dowód

$\Leftarrow$: Twierdzenie Lagrange'a.

$\Rightarrow$:

Załóżmy, że G jest p-grupą.

Niech $q \in \mathbb{P}$ i $q \mid |G|$.

(4.9) $\implies$ istnieje $g \in G$ taki, że $\mathrm{ord}(g) = q$.

Stąd $q = p$, bo G jest p-grupą, co kończy dowód. $\square$

Definicja

Niech $H \leq G$.

Definiujemy normalizator $N_G(H)$ podgrupy H w grupie G wzorem

$$N_G(H) := \{g \in G : gHg^{-1} = H\}.$$

Uwaga

Jeśli $H \leq G$, to $N_G(H) \leq G$ oraz $H \trianglelefteq N_G(H)$.

Lemat 4.11

Jeśli $p \in \mathbb{P}$ oraz H jest p-podgrupą grupy skończonej G, to

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Lemat 4.8

Jeśli $p \in \mathbb{P}$ i p-grupa skończona H działa na zbiorze skończonym X, to $|X^H| \equiv |X| \pmod{p}$.

Dowód

H działa na G/H przez (lewe) przesunięcia zgodnie ze wzorem

$$h * (gH) := (h \cdot g)H \qquad (h \in H,\ g \in G).$$

(Trzeba sprawdzić, że gdy $g' \sim_H g''$, to $h \cdot g' \sim_H h \cdot g''$ dla wszystkich $h \in H$ oraz $g', g'' \in G$.)

Zauważmy, że $gH \in (G/H)^H$ wtedy i tylko wtedy, gdy $g \in N_G(H)$.

Stąd $|(G/H)^H| = [N_G(H) : H]$, co kończy dowód na mocy (4.8). $\square$

Twierdzenie 4.9 (Cauchy)

Jeśli $p \in \mathbb{P}$ oraz $p \mid |G|$, to istnieje $g \in G$ taki, że $\operatorname{ord}(g) = p$.

Lemat 4.11

Jeśli $p \in \mathbb{P}$ oraz H jest p-podgrupą grupy skończonej G, to

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Wniosek 4.12

Jeśli $p \in \mathbb{P}$ i H jest p-podgrupą grupy skończonej G taką, że $p \mid [G : H]$, to $p \mid [N_G(H) : H]$.
W szczególności istnieje p-podgrupa K grupy G taka, że $H \trianglelefteq K$ oraz $[K : H] = p$.

Dowód

Ponieważ $[N_G(H) : H] \equiv [G : H] \pmod{p}$ na mocy (4.11), więc $p \mid [N_G(H) : H]$.
Ponieważ $p \mid [N_G(H) : H]$, więc (4.9) $\implies$ istnieje podgrupa $L \leq N_G(H)/H$ rzędu p.
Niech $K = \pi^{-1}(L)$, gdzie $\pi \colon N_G(H) \to N_G(H)/H$ jest naturalnym rzutowaniem.
Wtedy $K \leq N_G(H)$ na mocy (1.11), a więc także $K \leq G$.
Ponadto $[K : H] = |L| = p$, zatem $|K| = p|H|$, więc K jest p-grupą.
Wreszcie $H \trianglelefteq K$, gdyż $K \subseteq N_G(H)$. $\square$

Wniosek 4.12

Jeśli $p \in \mathbb{P}$ i H jest p-podgrupą grupy skończonej G taką, że $p \mid [G : H]$, to istnieje p-podgrupa K grupy G taka, że $H \trianglelefteq K$ oraz $[K : H] = p$.

Twierdzenie 4.13 (Pierwsze Twierdzenie Sylowa)

Niech $p \in \mathbb{P}$ oraz $|G| = p^n m$, $n, m \in \mathbb{N}$ oraz $p \nmid m$.

Wtedy

(1) dla każdego $i \in \{0, \ldots, n\}$ istnieje podgrupa grupy G rzędu p^i oraz

(2) dla każdego $i \in \{1, \ldots, n\}$ każda podgrupa grupy G rzędu p^{i-1} jest dzielnikiem normalnym pewnej podgrupy grupy G rzędu p^i.

Dowód

Wynika natychmiast z (4.12) przez indukcję ze względu na i. □

Twierdzenie 4.13 (Pierwsze Twierdzenie Sylowa)

Niech $p \in \mathbb{P}$ oraz $|G| = p^n m$, $n, m \in \mathbb{N}$ oraz $p \nmid m$.

Każda p-grupa jest zawarta w pewnej podgrupie rzędu p^n.

Definicja

Jeśli $p \in \mathbb{P}$, to podgrupę P grupy G nazywamy p-podgrupą Sylowa, jeśli P jest maksymalną (w sensie zawierania) p-podgrupą grupy G.

Uwaga

Każda p-podgrupa jest zawarta w pewnej p-podgrupie Sylowa.

W szczególności w każdej grupie istnieje p-podgrupa Sylowa.

Wniosek 4.14

Niech $p \in \mathbb{P}$ oraz $|G| = p^n m$, $n, m \in \mathbb{N}$ oraz $p \nmid m$.

(1) Podgrupa H grupy G jest p-podgrupą Sylowa wtedy i tylko wtedy, gdy $|H| = p^n$.

(2) Jeśli H jest sprzężona z p-podgrupą Sylowa, to H jest p-podgrupą Sylowa.

Dowód

Natychmiast z Pierwszego Twierdzenia Sylowa. □

Lemat 4.8

Jeśli $p \in \mathbb{P}$ i p-grupa skończona Q działa na zbiorze skończonym X, to $|X^Q| \equiv |X| \pmod{p}$.

Twierdzenie 4.15 (Drugie Twierdzenie Sylowa)

Niech $p \in \mathbb{P}$ będzie liczbą pierwszą.
Dowolne dwie p-podgrupy Sylowa grupy skończonej G są ze sobą sprzężone.

Dowód

Niech P i Q będą dwoma p-podgrupami Sylowa grupy G.
Grupa Q działa na G/P zgodnie ze wzorem

$$q * (gP) \mapsto (q \cdot g)P \qquad (q \in Q,\ g \in G).$$

(4.8) $\implies$ $|(G/P)^Q| \equiv [G : P] \pmod{p}$.
Ponieważ P jest p-podgrupą Sylowa, więc $p \nmid [G : P]$, skąd $(G/P)^Q \neq \varnothing$.
Zauważmy, że jeśli $gP \in (G/P)^Q$, to $Q \subseteq gPg^{-1}$.
Istotnie, jeśli $q * (gP) = gP$, to $g^{-1} \cdot q \cdot g \in P$, więc $q \in gPg^{-1}$.
Ponieważ $|Q| = |P| = |gPg^{-1}|$, więc wtedy $Q = gPg^{-1}$. $\square$

Lemat 4.8

Jeśli $p \in \mathbb{P}$ i p-grupa skończona P działa na zbiorze skończonym X, to $|X^P| \equiv |X| \pmod{p}$.

Twierdzenie 4.16 (Trzecie Twierdzenie Sylowa)

Niech $p \in \mathbb{P}$ oraz N będzie liczbą p-podgrup Sylowa grupy skończonej G.
Wtedy N dzieli $|G|$ oraz $N \equiv 1 \pmod{p}$.

Dowód

Niech X będzie zbiorem wszystkich p-podgrup Sylowa grupy G i wybierzmy $P \in X$.
Wtedy $N = |X|$.
Grupa G działa na zbiorze X przez sprzężenia, tzn.

$$g * Q := gQg^{-1} \qquad (g \in G,\ Q \in X).$$

Z Drugiego Twierdzenia Sylowa wiemy, że $X = G * P$, zatem z (4.7) wynika, że

$$N = |X| = [G : G_P],$$

więc N dzieli $|G|$ na mocy (1.30).
Przez ograniczenie powyższego działania otrzymujemy działanie grupy P na zbiorze X.
Oczywiście $P \in X^P$.
Z drugiej strony, jeśli $Q \in X^P$, to $P \subseteq G_Q = N_G(Q)$.
Wtedy P jest p-podgrupą Sylowa grupy $N_G(Q)$, więc na mocy Drugiego Twierdzenia Sylowa istnieje $g \in N_G(Q)$ takie, że $gQg^{-1} = P$.
Ale $gQg^{-1} = Q$, gdyż $g \in N_G(Q)$, zatem $Q = P$.
Ostatecznie $X^P = \{P\}$, co kończy dowód twierdzenia wobec (4.8). $\square$