Wykład 2
Podgrupa grupy

Definicja 2.1. *Podgrupą* grupy $(G, \cdot, e)$ nazywamy taki podzbiór $H \subseteq G$, że $e \in H$, $h^{-1} \in H$ dla każdego $h \in H$ oraz $h_1 \cdot h_2 \in H$ dla dowolnych $h_1, h_2 \in H$. Jeśli H jest podgrupą grupy G, to będziemy pisali $H \leq G$.

Przykład 2.2. Centrum grupy. Zbiór

$$Z(G) = \{a \in G : \ a \cdot g = g \cdot a \ \text{ dla kadego } g \in G\}$$

nazywamy *centrum* grupy G. Pokażemy, że $Z(G)$ jest podgrupą grupy G. Ponieważ dla każdego $g \in G$ jest $g \cdot e = e \cdot g = g$, więc $e \in Z(G)$. Niech $h \in Z(G)$. Wtedy dla każdego $g \in G$ jest $h \cdot g = g \cdot h$, skąd $g = h^{-1}gh$ oraz $h^{-1} \cdot g = g \cdot h^{-1}$, a więc $h^{-1} \in Z(G)$. Weźmy dowolne $h_1, h_2 \in Z(G)$. Wtedy dla dowolnego $g \in G$, $(h_1h_2)g = h_1(h_2g) = h_1(gh_2) = (h_1g)h_2 = (gh_1)h_2 = g(h_1h_2)$, skąd $h_1h_2 \in Z(G)$. Zatem $Z(G)$ jest podgrupą grupy G. Zauważmy jeszcze, że grupa G jest abelowa wtedy i tylko wtedy, gdy $G = Z(G)$.

Z Definicji 2.1 mamy od razu, że każda podgrupa H grupy $(G, \cdot, e)$ tworzy grupę ze względu na ograniczenie do H działania $\cdot$. Na odwrót, niech $(G, \cdot, e)$ będzie grupą i niech H będzie takim podzbiorem G, że H tworzy grupę ze względu na ograniczenie do H działania $\cdot$. Wtedy istnieje $f \in H$ będące elementem neutralnym grupy H. Zatem $f \cdot f = f$, skąd po skróceniu przez f, $f = e$, czyli $e \in H$. Ponadto z założenia $h_1 \cdot h_2 \in H$ dla dowolnych $h_1, h_2 \in H$. Niech $h \in H$. Wtedy istnieje $x \in H$ takie, że $h \cdot x = x \cdot h = e$. Ale $h, x \in G$, więc $x = h^{-1}$, skąd $h^{-1} \in H$. Wobec tego H jest podgrupą grupy G. W ten sposób udowodniliśmy następujące

Stwierdzenie 2.3. *Niech $(G, \cdot, e)$ będzie grupą. Podzbiór $H \subseteq G$ jest podgrupą grupy G wtedy i tylko wtedy, gdy H tworzy grupę ze względu na ograniczenie do H działania $\cdot$.* □

Przykład 2.4. Ze stwierdzenia 2.3 wynika od razu, że G i $\{e\}$ są podgrupami grupy $(G, \cdot, e)$. Pierwszą z nich nazywamy *podgrupą niewłaściwą*, zaś drugą — *trywialną*. Z definicji podgrupy wynika też, że **podgrupa trywialna jest jedyną podgrupą jednoelementową grupy** G.

Stwierdzenie 2.5. *Niepusty podzbiór $H \subseteq G$ jest podgrupą grupy $(G, \cdot, e)$ wtedy i tylko wtedy, gdy $h_1 \cdot h_2^{-1} \in H$ dla dowolnych $h_1, h_2 \in H$.*

Dowód. Niech H będzie podgrupą grupy $(G, \cdot, e)$. Weźmy dowolne $h_1, h_2 \in H$. Wtedy $h_2^{-1} \in H$, skąd $h_1 \cdot h_2^{-1} \in H$.

Na odwrót, niech H będzie niepustym podzbiorem zbioru G takim, że $h_1 \cdot h_2^{-1} \in H$ dla dowolnych $h_1, h_2 \in H$. Wtedy istnieje $x \in H$, skąd $e = x \cdot x^{-1} \in H$, czyli $e \in H$. Weźmy

dowolne $h \in H$. Wtedy $h^{-1} = e \cdot h^{-1} \in H$, więc $h^{-1} \in H$. W końcu dla dowolnych $h_1, h_2 \in H$ mamy, że $h_1 \cdot h_2 = h_1 \cdot (h_2^{-1})^{-1} \in H$, czyli $h_1 \cdot h_2 \in H$. Zatem H jest podgrupą grupy G. $\square$

Przykład 2.6. Podgrupa cykliczna. Niech $(G, \cdot, e)$ będzie grupą i niech $a \in G$. Udowodnimy, że podzbiór

$$\langle a \rangle = \{a^k : \ k \in \mathbb{Z}\}$$

jest najmniejszą (w sensie inkluzji) podgrupą grupy G zawierającą element a. Ponieważ $a = a^1$, więc $a \in \langle a \rangle$. W szczególności $\langle a \rangle \neq \emptyset$. Weźmy dowolne $h_1, h_2 \in \langle a \rangle$. Wtedy istnieją liczby całkowite k_1, k_2 takie, że $h_1 = a^{k_1}$ i $h_2 = a^{k_2}$. Zatem $h_1 \cdot h_2^{-1} = a^{k_1} \cdot (a^{k_2})^{-1} = a^{k_1} \cdot a^{-k_2} = a^{k_1 - k_2} \in \langle a \rangle$. Zatem ze Stwierdzenia 2.5, $\langle a \rangle$ jest podgrupą grupy G oraz dodatkowo $a \in \langle a \rangle$. Niech H będzie dowolną podgrupą grupy G taką, że $a \in H$. Wtedy ze Stwierdzenia 2.3 mamy, że $a^k \in H$ dla każdego $k \in \mathbb{Z}$, czyli $\langle a \rangle \subseteq H$. Zatem $\langle a \rangle$ jest najmniejszą podgrupą grupy G zawierającą element a. Nazywamy ją *podgrupą cykliczną generowaną przez element a*. Natomiast a nazywamy *generatorem* podgrupy $\langle a \rangle$.

Definicja 2.7. Powiemy, że grupa G jest *cykliczna*, jeżeli istnieje element $a \in G$ (zwany *generatorem* tej grupy) taki, że $G = \langle a \rangle$, tzn. $G = \{a^k : k \in \mathbb{Z}\}$.

Stwierdzenie 2.8. *Każda grupa cykliczna jest abelowa.*

Dowód. Niech G będzie grupą cykliczną o generatorze a. Wtedy $G = \{a^k : k \in \mathbb{Z}\}$. Weźmy dowolne $x, y \in G$. Wtedy istnieją $k, l \in \mathbb{Z}$ takie, że $x = a^k$ oraz $y = a^l$. Zatem $x \cdot y = a^k \cdot a^l = a^{k+l} = a^{l+k} = a^l \cdot a^k = y \cdot x$, czyli grupa G jest abelowa. $\square$

Twierdzenie 2.9. *Niech H będzie podgrupą grupy skończonej G. Wtedy $|H|$ jest dzielnikiem $|G|$.*

Dowód. Dla dowolnego $g \in G$ niech

$$gH = \{g \cdot h : \ h \in H\}.$$

Ponieważ $g = g \cdot e$ i $e \in H$, więc $g \in gH$, skąd

$$G = \bigcup_{g \in G} gH. \tag{1}$$

Z prawa skracania równości w grupie wynika, że odwzorowanie $h \mapsto \ g \cdot \ h$ dla $h \in H$ jest bijekcją H na gH, czyli

$$|H| = |gH| \ \text{ dla każdego } g \in G. \tag{2}$$

Niech $a, b \in G$ będą takie, że $aH \cap bH \neq \emptyset$. Wtedy istnieją $h_1, h_2 \in \ H$ takie, że $a \cdot h_1 = b \cdot h_2$. Zatem $b = a h_1 h_2^{-1}$ oraz dla dowolnego $h \in H$, $b \cdot h = a \cdot (h_1 h_2^{-1} h) \in aH$, gdyż $h_1 h_2^{-1} h \in H$. Stąd $bH \subseteq aH$. Ale zbiory aH i bH są skończone, więc z (2),

$bH = aH$. Stąd i z (1) oraz ze skończoności grupy G wynika, że istnieją $a_1, a_2, \ldots, a_k \in G$ takie, że zbiory $a_1H, a_2H, \ldots, a_kH$ są parami rozłączne oraz $G = \bigcup_{i=1}^{k} a_iH$. Zatem $|G| = \sum_{i=1}^{k} |a_iH| = k \cdot |H|$, czyli $|H|$ dzieli $|G|$. □

Stwierdzenie 2.10. *Niech $H \subseteq G$ będzie skończonym niepustym podzbiorem grupy $(G, \cdot, e)$. Wówczas H jest podgrupą grupy G wtedy i tylko wtedy, gdy $h_1 \cdot h_2 \in H$ dla dowolnych $h_1, h_2 \in H$.*

Dowód. Jeśli H jest podgrupą grupy G, to $h_1 \cdot h_2 \in H$ dla dowolnych $h_1, h_2 \in H$.

Na odwrót, załóżmy, że $h_1 \cdot h_2 \in H$ dla dowolnych $h_1, h_2 \in H$. Ponieważ $H \neq \emptyset$, więc istnieje $x \in H$. Wtedy $x^2 = x \cdot x \in H$ i jeśli dla pewnego naturalnego n, $x^n \in H$, to także $x^{n+1} = x^n \cdot x \in H$. Zatem $\{x, x^2, x^3, \ldots\} \subseteq H$ i zbiór H jest skończony, więc istnieją liczby naturalne $m > n$ takie, że $x^m = x^n$. Stąd $x^{m-n} = e$ i $m - n \in \mathbb{N}$, więc $e \in H$. Ponadto z tego rozumowania wynika, że dla każdego $h \in H$ istnieje $n \in \mathbb{N}$ takie, że $h^n = e$ oraz $n > 1$. Zatem $h^{-1} = h^{n-1} \in H$. Stąd ostatecznie mamy, że H jest podgrupą grupy G. □

Wniosek 2.11. *Jeżeli rząd grupy G jest liczbą pierwszą, to grupa G jest cykliczna (a więc jest abelowa).*

Dowód. Niech liczba pierwsza p będzie rzędem grupy G. Ponieważ $p > 1$, więc istnieje $a \in G$, $a \neq e$. Zatem podgrupa $\langle a \rangle$ ma co najmniej dwa różne elementy: e i a oraz z Twierdzenia 2.9, $|\langle a \rangle|$ dzieli liczb pierwszą p. Zatem $|\langle a \rangle| = p$, czyli $|\langle a \rangle| = |G|$, skąd $G = \langle a \rangle$ i grupa G jest cykliczna. Zatem ze Stwierdzenia 2.8 grupa G jest abelowa. □

Uwaga 2.12. Z dowodu Wniosku 2.11 wynika, że jeśli rząd grupy G jest liczbą pierwszą, to $G = \langle a \rangle$ dla każdego $a \in G \setminus \{e\}$ (tzn. każdy element $a \neq e$ tej grupy jest jej generatorem).

Stwierdzenie 2.13. *Część wspólna dowolnej niepustej rodziny podgrup grupy G jest podgrupą grupy G.*

Dowód. Niech $\{H_t\}_{t \in T}$ będzie dowolną niepustą rodziną podgrup grupy $(G, \cdot, e)$. Wtedy $e \in H_t$ dla każdego $t \in T$, więc $e \in \bigcap_{t \in T} H_t$. Niech $h_1, h_2 \in \bigcap_{t \in T} H_t$. Wtedy $h_1, h_2 \in H_t$ dla każdego $t \in T$. Zatem ze Stwierdzenia 2.5, $h_1 \cdot h_2^{-1} \in H_t$ dla każdego $t \in T$. Stąd $h_1 \cdot h_2^{-1} \in \bigcap_{t \in T} H_t$. Zatem ze Stwierdzenia 2.5, $\bigcap_{t \in T} H_t$ jest podgrupą grupy G. □

Przykład 2.14. Podgrupa generowana przez podzbiór grupy. Niech $(G, \cdot, e)$ będzie grupą i niech X będzie dowolnym podzbiorem zbioru G. Oznaczmy przez $\mathcal{X}$

rodzinę wszystkich podgrup grupy G zawierających zbiór X. Ponieważ $G \in \mathcal{X}$, więc rodzina $\mathcal{X}$ jest niepusta. Zatem ze Stwierdzenia 2.13, $\langle X\rangle = \bigcap_{H\in\mathcal{X}} H$ jest podgrupą grupy G zawierającą zbiór X. Ponadto z określenia $\langle X\rangle$ wynika, że jeśli H jest podgrupą grupy G zawierającą zbiór X, to $H \in \mathcal{X}$ oraz $\langle X\rangle \subseteq H$. Zatem $\langle X\rangle$ jest najmniejszą (w sensie inkluzji) podgrupą grupy G zawierającą zbiór X. Nazywamy ją *podgrupą generowaną przez podzbiór* X i oznaczamy przez $\langle X\rangle$. Natomiast X nazywamy *zbiorem generatorów podgrupy* $\langle X\rangle$. Wobec tego:

$$\langle X\rangle \leq G \text{ i } X \subseteq \langle X\rangle \text{ i } \forall_{H\leq G}(X \subseteq H \Rightarrow \langle X\rangle \subseteq H). \tag{3}$$

Oczywiście $\langle\emptyset\rangle = \{e\}$, bo $\{e\}$ jest najmniejszą podgrupą grupy G. Jeśli zbiór X jest skończony i $X = \{x_1, \ldots, x_n\}$, to zamiast $\langle\{x_1, \ldots, x_n\}\rangle$ będziemy pisali $\langle x_1, \ldots, x_n\rangle$.

Stwierdzenie 2.15. Niech X będzie niepustym podzbiorem grupy G. Wówczas najmniejsza w sensie inkluzji podgrupa $\langle X\rangle$ grupy G zawierająca zbiór X jest zbiorem wszystkich elementów postaci $x_1^{k_1}\cdot x_2^{k_2}\cdot\ldots\cdot x_n^{k_n}$, gdzie $x_1, \ldots, x_n \in X$, $k_1, \ldots, k_n \in \{1, -1\}$ oraz $n \in \mathbb{N}$.

Dowód. Oznaczmy przez H zbiór wszystkich elementów postaci $x_1^{k_1} \cdot x_2^{k_2} \cdot \ldots \cdot x_n^{k_n}$, gdzie $x_1, \ldots, x_n \in X$, $k_1, \ldots, k_n \in \{1, -1\}$ oraz $n \in \mathbb{N}$. Weźmy dowolne $x \in X$. Wtedy $x \in H$, bo wystarczy wziąć $n = 1$, $k_1 = 1$, $x_1 = x$. Zatem $X \subseteq H$. Ale $X \neq \emptyset$, więc też $H \neq \emptyset$. Weźmy dowolne $a, b \in H$. Wtedy istnieją $n, m \in \mathbb{N}$, $x_1, \ldots, x_n, y_1, \ldots, y_m \in X$ oraz $k_1, \ldots, k_n, l_1, \ldots, l_m \in \{1, -1\}$ takie, że $a = x_1^{k_1} \cdot x_2^{k_2} \cdot \ldots \cdot x_n^{k_n}$ i $b = y_1^{l_1} \cdot y_2^{l_2} \cdot \ldots \cdot y_m^{l_m}$. Stąd $a \cdot b^{-1} = x_1^{k_1} \cdot x_2^{k_2} \cdot \ldots \cdot x_n^{k_n} \cdot y_m^{-l_m} \cdot \ldots \cdot y_2^{-l_2} \cdot y_1^{-l_1} \in \langle X\rangle$, bo $-l_i \in \{1, -1\}$ dla każdego $i = 1, 2, \ldots, m$. Zatem H jest podgrupą grupy G i $X \subseteq H$.

Niech teraz K będzie dowolną podgrupą grupy G taką, że $X \subseteq K$. Weźmy dowolne $x_1, \ldots, x_n \in X$ i dowolne $k_1, \ldots, k_n \in \{1, -1\}$. Wówczas $x_1, \ldots, x_n \in K$, skąd $x_1^{-1}, \ldots, x_n^{-1} \in K$, więc $x_1^{k_1}, \ldots, x_n^{k_n} \in K$. Zatem ze Stwierdzenia 2.3, $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} \in K$. Wobec tego $H \subseteq K$. Zatem H jest najmniejszą w sensie inkluzji podgrupą grupy G zawierającą zbiór X, czyli $H = \langle X\rangle$. □

Stwierdzenie 2.16. *Jeżeli a jest elementem grupy $(G, \cdot, e)$ i n jest najmniejszą liczbą naturalną taką, że $a^n = e$, to podgrupa $\langle a\rangle$ ma dokładnie n elementów oraz*

$$\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Dowód. Oczywiście $\{e, a, \ldots, a^{n-1}\} \subseteq \langle a\rangle$. Niech $h \in \langle a\rangle$. Wtedy $h = a^k$ dla pewnego $k \in \mathbb{Z}$. Dzieląc z resztą liczbę k przez liczbę n uzyskamy, że $k = qn + r$ dla pewnych $q, r \in \mathbb{Z}$ takich, że $r \in \{0, 1, \ldots, n-1\}$. Zatem $h = a^{qn+r} = a^{qn} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r \in \{e, a, \ldots, a^{n-1}\}$. Stąd $\langle a\rangle \subseteq \{e, a, \ldots, a^{n-1}\}$ i ostatecznie $\langle a\rangle = \{e, a, \ldots, a^{n-1}\}$. Gdyby podgrupa $\langle a\rangle$ nie miała dokładnie n elementów, to istniałyby liczby całkowite k, s takie, że $0 \leqslant k < s < n$ oraz $a^s = a^k$. Ale wtedy $a^{s-k} = e$ i $s - k \in \mathbb{N}$

oraz $s - k < n$, więc otrzymalibyśmy sprzeczność z minimalnością liczby n. Kończy to dowód naszego stwierdzenia. □

Stwierdzenie 2.17. *Niech $n \in \mathbb{N}$ i niech a będzie elementem grupy $(G, \cdot, e)$ takim, że podgrupa $\langle a \rangle$ ma dokładnie n elementów. Wówczas $a^n = e$ oraz $a^k \neq e$ dla dowolnej liczby naturalnej $k < n$.*

Dowód. Z dowodu Stwierdzenia 2.10 wynika, że istnieje najmniejsza liczba naturalna s taka, że $a^s = e$. Wtedy ze Stwierdzenia 2.16 podgrupa $\langle a \rangle$ ma dokładnie s elementów, skąd $s = n$ i nasze stwierdzenie jest udowodnione. □

Stwierdzenie 2.18. *Jeżeli $a^2 = e$ dla każdego elementu a grupy $(G, \cdot, e)$, to grupa G jest abelowa.*

Dowód. Weźmy dowolne $a, b \in G$. Wtedy $(ab)^2 = e$, $a^2 = e$ i $b^2 = e$. Zatem $abab = aabb$, skąd z praw skracania równości w grupie, $ba = ab$. Zatem grupa G jest abelowa. □

Stwierdzenie 2.19. Niech $(G, \cdot, e)$ będzie grupą i $H \subseteq G$. Wówczas równoważne są warunki:

(i) H jest podgrupą rzędu 4 grupy G,

(ii) $H = \{e, a, a^2, a^3\}$ dla pewnego elementu $a \in G$ takiego, że $a^2 \neq e$ i $a^4 = e$ lub $H = \{e, a, b, ab\}$ dla pewnych $a, b \in G$ takich, że $a \neq b$, $a \neq e$, $b \neq e$, $ab = ba$ i $a^2 = b^2 = e$.

Dowód. Niech H będzie podgrupą rzędu 4 grupy G. Załóżmy, że $g^2 = e$ dla każdego $g \in H$. Wtedy ze Stwierdzenia 2.18 grupa H jest abelowa. Istnieje $a \in H$ takie, że $a \neq e$ i istnieje $b \in H$ takie, że $b \neq a$ i $b \neq e$. Wtedy $a^2 = b^2 = e$ i $ab = ba$, przy czym $ab \in H$. Jeśli $ab = e$, to po pomnożeniu obu stron tej równości z prawej strony przez b i uwzględnieniu tego, że $b^2 = e$ uzyskamy, że $a = b$ wbrew założeniu. Zatem $ab \neq e$. Jeśli $ab = a$, to po skróceniu przez a otrzymamy $b = e$, co prowadzi do sprzeczności. Zatem $ab \neq a$. Jeśli $ab = b$, to po skróceniu przez b uzyskamy, że $a = e$, wbrew założeniu. Zatem $ab \neq b$. Wobec tego e, a, b, ab są czterema różnymi elementami grupy H i $|H| = 4$, więc $H = \{e, a, b, ab\}$. Teraz załóżmy, że istnieje $c \in H$ takie, że $c^2 \neq e$. Wtedy $c \neq e$ i $c^2 \neq c$. Jeśli $c^3 = e$, to ze Stwierdzenia 2.16 mamy, że $\{e, c, c^2\}$ jest podgrupą trzyelementową grupy czteroelementowej H, co przeczy Twierdzeniu 2.9. Zatem $c^3 \neq e$ i $\{e, c, c^2, c^3\}$ jest czteroelementowym podzbiorem zbioru czteroelementowego H, skąd $H = \{e, c, c^2, c^3\}$. Stąd na mocy Stwierdzenia 2.17, $c^4 = e$.

Na odwrót, niech $H = \{e, a, a^2, a^3\}$ dla pewnego $a \in G$ takiego, że $a^2 \neq e$ i $a^4 = e$. Jeśli $a^3 = e$, to $a^4 = a^3$, skąd po skróceniu przez a^3 otrzymamy, że $a = e$, a więc $a^2 = e$ wbrew założeniu. Zatem $a^3 \neq e$ i ze Stwierdzenia 2.16 $H = \{e, a, a^2, a^3\}$ jest czteroelementową podgrupą grupy G. W końcu, załóżmy, że $H = \{e, a, b, ab\}$ dla pewnych $a, b \in G$ takich, że $a \neq b$, $a \neq e$, $b \neq e$, $ab = ba$, $a^2 = b^2 = e$. Jeśli $ab = e$, to po pomnożeniu z prawej strony tej równości przez b uzyskamy, że $ab^2 = b$, skąd $ae = b$ i $a = b$, co prowadzi do sprzeczności. Zatem $ab \neq e$. Jeśli $ab = a$, to po skróceniu przez a uzyskamy, że $b = e$,

wbrew założeniu. Zatem $ab \neq a$. Jeśli $ab = b$, to po skróceniu przez b otrzymamy, że $a = e$, wbrew założeniu. Zatem $ab \neq b$ i wobec tego elementy e, a, b, ab są parami różne. Dalej, $a(ab) = a^2b = eb = b$, $ba = ab$, $b(ab) = b(ba) = b^2a = eb = b$, $(ab)a = (ba)a = ba^2be = b$, $(ab)b = ab^2 = ae = a$, $(ab)(ab) = (ab)(ba) = ab^2a = aea = a^2 = e$. Wobec tego $x \cdot y \in H$ dla dowolnych $x, y \in H = \{e, a, b, ab\}$ i na mocy Stwierdzenia 2.10, $H \leq G$. Stąd H jest podgrupą rzędu 4 grupy G. □

Stwierdzenie 2.20. *Każda skończona grupa nieabelowa ma rząd większy niż* 5.

Dowód. Niech G będzie grupą rzędu co najwyżej 5. Wtedy $|G| \in \{1, 2, 3, 4, 5\}$. Jeśli $|G| = 1$, to $G = \{e\}$, więc G jest abelowa. Jeśli $|G| \in \{2, 3, 5\}$, to z Wniosku 2.11 grupa G też jest abelowa. Niech dalej $|G| = 4$. Jeśli istnieje w G element a taki, że $\langle a \rangle = G$, to grupa G jest abelowa (bo jest grupą cykliczną). Załóżmy zatem, że $\langle a \rangle \neq G$ dla każdego $a \in G$. Weźmy dowolne $a \in G$, $a \neq e$. Wtedy podgrupa $\langle a \rangle$ ma co najmniej 2 różne elementy: e, a i jest różna od G, więc z Twierdzenia 2.9, $|\langle a \rangle| = 2$. Zatem ze Stwierdzenia 2.17, $a^2 = e$. Ponieważ dodatkowo $e^2 = e$, więc $x^2 = e$ dla każdego $x \in G$. Zatem ze Stwierdzenia 2.18 grupa G jest abelowa i nasze stwierdzenie zostało udowodnione. □

Przykład 2.21. Udowodnimy, że wszystkimi różnymi podgrupami grupy Kleina K są: $\{e\}$, $\{e, S_a\}$, $\{e, S_b\}$, $\{e, S_O\}$, K.

Rzeczywiście, jeśli H jest podgrupą grupy K, to na mocy Twierdzenia 2.9, $|H|$ jest dzielnikiem $|K| = 4$, skąd $|H| = 1$ lub $|H| = 2$ lub $|H| = 4$. Jeśli $|H| = 1$, to $H = \{e\}$. Jeśli $|H| = 4$, to $H = K$. Niech $|H| = 2$. Wtedy z Wniosku 2.11, $H = \langle x \rangle$ dla pewnego $x \in K$. Wtedy ze Stwierdzenia 2.17, $x \neq e$ i $x^2 = e$. Z tabelki grupy K odczytujemy, że $x \in \{S_a, S_b, S_O\}$ i na mocy Stwierdzenia 2.16 wszystkimi podgrupami rzędu 2 grupy K są: $\{e, S_a\}$, $\{e, S_b\}$, $\{e, S_O\}$.

Przykład 2.22. Udowodnimy, że wszystkimi różnymi podgrupami grupy D_3 izometrii własnych trójkąta równobocznego są: $\{e\}$, $\{e, S_a\}$, $\{e, S_b\}$, $\{e, S_c\}$, $\{e, O_1, O_2\}$, D_3.

Rzeczywiście, jeśli H jest podgrupą grupy D_3, to na mocy Twierdzenia 2.9, $|H|$ jest dzielnikiem $|D_3| = 6$, skąd $|H| = 1$ lub $|H| = 2$ lub $|H| = 3$ lub $|H| = 6$. Jeśli $|H| = 1$, to $H = \{e\}$. Jeśli $|H| = 6$, to $H = D_3$. Niech $|H| = 2$. Wtedy z Wniosku 2.11, $H = \langle x \rangle$ dla pewnego $x \in D_3$. Zatem ze Stwierdzenia 2.17, $x \neq e$ i $x^2 = e$. Z tabelki grupy D_3 odczytujemy, że $x \in \{S_a, S_b, S_c\}$ i na mocy Stwierdzenia 2.16 wszystkimi podgrupami rzędu 2 grupy D_3 są: $\{e, S_a\}$, $\{e, S_b\}$, $\{e, S_c\}$. Niech $|H| = 3$. Wtedy z Wniosku 2.11, $H = \langle x \rangle$ dla pewnego $x \in D_3$. Zatem ze Stwierdzenia 2.17, $x \neq e$, $x^2 \neq e$ i $x^3 = e$. Z tabelki grupy D_3 odczytujemy, że $x \in \{O_1, O_2\}$. Ale $\langle O_2 \rangle = \langle O_1 \rangle = \{e, O_1, O_2\}$, więc $\{e, O_1, O_2\}$ jest jedyną podgrupą rzędu 3 grupy D_3. Nazywamy ją *podgrupą obrotów*.

Przykład 2.23. Udowodnimy, że wszystkimi różnymi podgrupami grupy D_4 izometrii własnych kwadratu są: $\{e\}$, $\{e, S_1\}$, $\{e, S_2\}$, $\{e, S_3\}$, $\{e, S_4\}$, $\{e, O_2\}$, $\{e, O_1, O_2, O_3\}$, $\{e, S_1, S_2, O_2\}$, $\{e, S_3, S_4, O_2\}$, D_4.

Rzeczywiście, jeśli H jest podgrupą grupy D_4, to na mocy Twierdzenia 2.9, $|H|$ jest dzielnikiem $|D_4| = 8$, skąd $|H| = 1$ lub $|H| = 2$ lub $|H| = 4$ lub $|H| = 8$. Jeśli $|H| = 1$, to $H = \{e\}$. Jeśli $|H| = 8$, to $H = D_4$. Niech $|H| = 2$. Wtedy z Wniosku 2.11, $H = \langle a\rangle$ dla pewnego $a \in D_4$. Zatem ze Stwierdzenia 2.17, $a \neq e$ i $a^2 = e$. Z tabelki grupy D_4 odczytujemy, że $a \in \{S_1, S_2, S_3, S_4, O_2\}$ i na mocy Stwierdzenia 2.16 wszystkimi podgrupami rzędu 2 grupy D_4 są: $\{e, S_1\}$, $\{e, S_2\}$, $\{e, S_3\}$, $\{e, S_4\}$, $\{e, O_2\}$.

Podgrupy H rzędu 4 wyznaczymy w oparciu o Stwierdzenie 2.19. Jeśli $H = \{e, a, a^2, a^3\} = \langle a\rangle$, gdzie $a \in D_4$, $a^2 \neq e$ i $a^4 = e$, to z tabelki grupy D_4 odczytujemy, że $a \in \{O_1, O_3\}$. Ale $\langle O_1\rangle = \langle O_3\rangle = \{e, O_1, O_2, O_3\}$, więc jedyną podgrupą rzędu 4 jest $\{e, O_1, O_2, O_3\}$. Teraz pozostaje wyznaczyć podgrupy H rzędu 4 postaci $H = \{e, a, b, ab\}$, gdzie $a, b \neq e$, $a \neq b$, $a^2 = b^2 = e$ i $ab = ba$. Z tabelki grupy D_4 odczytujemy, że $a, b \in \{S_1, S_2, S_3, S_4, O_2\}$.

Jeśli $a = S_1$, to z tabelki grupy D_4 mamy, że $b \in \{S_2, O_2\}$. Ale $S_1 \circ S_2 = O_2$ i $S_1 \circ O_2 = S_2$, więc $\{e, S_1, O_2, S_1 \circ O_2\} = \{e, S_1, S_2, O_2\}$ i otrzymujemy podgrupę $H = \{e, S_1, S_2, O_2\}$.

Jeśli $a = S_2$, to z tabelki grupy D_4 mamy, że $b \in \{S_1, O_2\}$. W obu przypadkach uzyskamy podgrupę $H = \{e, S_1, S_2, O_2\}$.

Jeśli $a = S_3$, to z tabelki grupy D_4 mamy, że $b \in \{S_4, O_2\}$. W obu przypadkach uzyskamy podgrupę $H = \{e, S_3, S_4, O_2\}$.

Jeśli $a = S_4$, to uzyskamy podgrupę $H = \{e, S_3, S_4, O_2\}$. Podobnie dla $a = O_2$ uzyskamy podgrupy $\{e, S_1, S_2, O_2\}$, $\{e, S_3, S_4, O_2\}$.

Przykład 2.24. Udowodnimy, że wszystkimi różnymi podgrupami grupy kwaternionów Q_8 są: $\{e\}$, $\{e, -e\}$, $\{e, -e, i, -i\}$, $\{e, -e, j, -j\}$, $\{e, -e, k, -k\}$, Q_8.

Rzeczywiście, jeśli H jest podgrupą grupy Q_8, to na mocy Twierdzenia 2.9, $|H|$ jest dzielnikiem $|Q_8| = 8$, skąd $|H| = 1$ lub $|H| = 2$ lub $|H| = 4$ lub $|H| = 8$. Jeśli $|H| = 1$, to $H = \{e\}$. Jeśli $|H| = 8$, to $H = Q_8$. Niech $|H| = 2$. Wtedy z Wniosku 2.11, $H = \langle a\rangle$ dla pewnego $a \in Q_8$. Zatem ze Stwierdzenia 2.17, $a \neq e$ i $a^2 = e$. Z tabelki grupy Q_8 odczytujemy, że $a = -e$ i na mocy Stwierdzenia 2.16 $\{e, -e\}$ jest jedyną podgrupą dwuelementową grupy Q_8. Niech teraz $|H| = 4$. Ponieważ $-e$ jest jedynym elementem różnym od e grupy Q_8, więc ze Stwierdzenia 2.19 mamy, że $H = \{e, a, a^2, a^3\} = \langle a\rangle$, gdzie $a \in Q_8$, $a \neq e$, $a^2 \neq e$ i $a^4 = e$. Stąd $a \in \{i, -i, j, -j, k, -k\}$. Ale $\langle -i\rangle = \langle i\rangle = \{e, -e, i, -i\}$, $\langle -j\rangle = \langle j\rangle = \{e, -e, j, -j\}$, $\langle -k\rangle = \langle k\rangle = \{e, -e, k, -k\}$, więc wszystkimi różnymi podgrupami rzędu 4 grupy Q_8 są: $\{e, -e, i, -i\}$, $\{e, -e, j, -j\}$, $\{e, -e, k, -k\}$.

Przykład 2.25. Zauważmy, że grupa Kleina K nie jest cykliczna, gdyż ma rząd 4 i $g^2 = e$ dla każdego $g \in K$. Zatem $K \neq \langle g\rangle$ dla każdego $g \in K$. Ale $K = \langle S_a, S_b\rangle = \langle S_a, S_O\rangle = \langle S_b, S_O\rangle$, bo $S_a \circ S_b = S_O$, $S_a \circ S_O = S_b$ i $S_b \circ S_O = S_a$.

Przykład 2.26. Zauważmy, że grupa D_3 nie jest cykliczna, bo D_3 nie jest abelowa. Zatem $D_3 \neq \langle g\rangle$ dla każdego $g \in D_3$. Ale $D_3 = \langle S_a, S_b\rangle = \langle S_a, S_c\rangle = \langle S_b, S_c\rangle$ oraz $D_3 = \langle S_a, O_1\rangle = \langle S_a, O_2\rangle = \langle S_b, O_1\rangle = \langle S_b, O_2\rangle = \langle S_c, O_1\rangle = \langle S_c, O_2\rangle$, gdyż w każdym przypadku generowana podgrupa ma postać $H = \langle x, y\rangle$, gdzie $x \circ y \neq y \circ x$ oraz $x \neq y$ i

$y \neq x$ i $x, y \neq e$, więc $|H| \geq 4$. Ale z Twierdzenia 2.9, $|H|$ jest dzielnikiem $|D_3| = 6$, więc $|H| = 6$, skąd $H = D_3$.

Ponadto ze Stwierdzenia 2.16 mamy, że $\{e, O_1, O_2\} = \langle O_1 \rangle = \langle O_2 \rangle$ oraz $\{e, S_x\} = \langle S_x \rangle$ dla $x = a, b, c$.

Przykład 2.27. Zauważmy, że grupa D_4 nie jest cykliczna, bo D_4 nie jest abelowa. Zatem $D_4 \neq \langle g \rangle$ dla każdego $g \in D_4$. Ale $D_4 = \langle S_1, S_3 \rangle = \langle S_1, S_4 \rangle = \langle S_1, O_1 \rangle = \langle S_1, O_3 \rangle$ oraz $D_4 = \langle S_2, S_3 \rangle = \langle S_2, S_4 \rangle = \langle S_2, O_1 \rangle = \langle S_2, O_3 \rangle = \langle S_3, O_1 \rangle = \langle S_3, O_3 \rangle = \langle S_4, O_1 \rangle = \langle S_4, O_3 \rangle$, co w prosty sposób wynika z tabelki tej grupy i ze Stwierdzenia 2.15. Ponadto $\{e, O_1, O_2, O_3\} = \langle O_1 \rangle = \langle O_3 \rangle$, $\langle O_2 \rangle = \{e, O_2\}$, $\langle \langle S_1, S_2 \rangle = \langle S_1, O_2 \rangle = \langle S_2, O_2 \rangle = \{e, S_1, S_2, O_2\}$, $\langle S_3, S_4 \rangle = \langle S_3, O_2 \rangle = \langle S_4, O_2 \rangle = \{e, S_3, S_4, O_2\}$.

Przykład 2.28. Zauważmy, że grupa Q_8 nie jest cykliczna, bo Q_8 nie jest abelowa. Zatem $Q_8 \neq \langle g \rangle$ dla każdego $g \in Q_8$. Ze Stwierdzenia 2.15 i z tabelki grupy Q_8 łatwo można uzasadnić, że np. $Q_8 = \langle i, j \rangle = \langle -i, j \rangle = \langle -i, -j \rangle = \langle i, k \rangle = \langle j, k \rangle$ oraz $\langle -e \rangle = \{e, -e\}$, $\langle i \rangle = \{e, -e, i, -i\}$.

Zagadka 1. Niech H i K będą podgrupami grupy G. Uzasadnij, że $H \cup K \leq G \iff (H \subseteq K \text{ lub } K \subseteq H)$.

Zagadka 2. Niech A i B będą skończonymi podgrupami grupy G o względnie pierwszych rzędach. Pokazać, że wówczas $A \cap B = \{e\}$.

Zagadka 3. Niech p będzie liczbą pierwszą i niech A i B będą różnymi podgrupami rzędu p grupy G. Pokazać, że wtedy $A \cap B = \{e\}$.

Zagadka 4. Wyznacz wszystkie podgrupy grupy $\mathbb{Z}_{20}^*$.

Zagadka 5. Udowodnij, że dla każdego ciała K i dla dowolnej liczby naturalnej n zbiór $SL_n(K)$ wszystkich macierzy kwadratowych stopnia n nad ciałem K o wyznaczniku równym 1 jest podgrupą grupy $GL_n(K)$.

Zagadka 6. Niech K będzie dowolnym ciałem takim, że $|K| > 2$. Udowodnij, że są podgrupami grupy $GL_2(K)$ następujące podzbiory:
(a) $A = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, c \in K \setminus \{0\}, b \in K \right\}$, (b) $B = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in K \setminus \{0\}, b \in K \right\}$,
(c) $C = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a \in K \setminus \{0\}, b \in K \right\}$, (d) $D = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in K \right\}$.
Która z tych podgrup jest abelowa?

Zagadka 7. Dla dowolnego ciała K wyznacz centrum grupy $GL_2(K)$.