ALGEBRA I

Marysia Nazarczuk

TEORIA GRUP

Ćwiczenia 1

Definicja: Grupa $(G, \cdot)$ to zbiór z działaniem $\cdot : G \times G \to G$ takim, że

1. $\forall_{a,b,c \in G}\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (łączność)
2. $\exists_e\ \forall_{a \in G}\ a \cdot e = e \cdot a = a$ (element neutralny)
3. $\forall_{a \in G}\ \exists_{a' \in G}$ takie, że $a \cdot a' = a' \cdot a = e$ (element odwrotny)

Przykłady:

- $(\mathbb{R}, +)$ - element neutralny to 0, natomiast element przeciwny do a to $-a$
- $(\mathbb{Z}, +)$ - element neutralny to 0, natomiast element przeciwny do a to $-a$
- $(\mathbb{Z}_n, +)$ - elementy to zbiór reszt modulo n natomiast $a+b = a+b \mod n$; element neutralny to 0, natomiast element odwrotny do $k \in \mathbb{Z}_n$ to $n - k$
- grupa dihedralna D_n o $2n$ elementach - są to izometrie n-kata foremnego z działaniem składania; element neutralny to identyczność;
- grupa permutacji S_n - jest to grupa permutacji $\{1, \dots n\}$ czyli bijekcji $\{1, \dots, n\} \to \{1, \dots, n\}$ z działaniem składania permutacji

Zadanie 1.

a) Czy zbiór elementów dowolnego ciała K różnych od 0 jest grupą względem mnożenia?

b) Czy $\mathbb{Q}$ z działaniem $\cdot$ jest grupą?

c) Czy $\mathbb{N}$ z działaniem $+$ jest grupą?

d) Czy zbiór $(\mathbb{Q}, \star)$ jest grupą z działaniem $a \star b = a + b - 2$?

Rozwiązanie:

a) Tak - mnożenie jest łączne; element neutralny to 1; element odwrotny do a to $\frac{1}{a}$

b) Nie, ponieważ 0 nie ma elementu odwrotnego

c) Nie, bo dla dowolnej liczby nie istnieje element odwrotny

d) Tak - dodawanie jest łączne i przemienne; element neutralny to 2; element odwrotny do a to $4 - a$

Zadanie 2.
Udowodnij, że w dowolnej grupie element neutralny oraz element odwrotny są wyznaczone jednoznacznie.

Rozwiązanie:
Niech e_1, e_2 to element neutralny wówczas $e_1 = e_1 \cdot e_2 = e_2 \cdot e_1 = e_2$. Czyli element neutralny jest wyznaczony jednoznacznie. Niech a' i a'' to elementy odwrotne elementu $a \in G$, wówczas $a' = e \cdot a' = (a'' \cdot a) \cdot a' = a'' \cdot (a \cdot a') = a'' \cdot e = a''$. $\square$

Definicja: Podzbiór $H \subseteq G$ jest podgrupą, gdy:

1. $a, b \in H \Rightarrow a \cdot b \in H$
2. $a \in H \Rightarrow a^{-1} \in H$

Definicja: Niech $X \subseteq G$ będzie dowolnym podzbiorem grupy G. Wtedy podgrupa w G generowana przez X to przecięcie wszystkich podgrup w G zawierających X. Jest to podgrupa w G. Oznaczenie $\langle X \rangle \leq G$. Innymi słowy, $\langle X \rangle$ jest to najmniejsza podgrupa, która zawiera podzbiór $X \subseteq G$.

Przykład: Dla $X = \{a\}$ piszemy $\langle \{a\} \rangle = \langle a \rangle \leq G$, wówczas $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, przy czym a^0 to element neutralny.

Definicja: Grupa G jest cykliczna, gdy istnieje element $g \in G$ taki, że $\langle g \rangle \in G$.

Fakt: Dowolna grupa cykliczna jest izomorficzna z $(\mathbb{Z}, +)$ lub $(\mathbb{Z}_n, +_{\bmod n})$

Przykład: Generatorem grupy $(\mathbb{Z}, +)$ oraz generatorem grupy $(\mathbb{Z}_n, +_{\bmod n})$ jest $\langle 1 \rangle$

Zadanie 3.
Wyznaczyć wszystkie podgrupy $(\mathbb{Z}, +)$.

Rozwiązanie:
Są to na pewno $(\{0\}, +)$ oraz $(\mathbb{Z}, +)$. Również $(n\mathbb{Z}, +)$, gdzie $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ dla $n \in \mathbb{Z}$ jest podgrupą, gdzie generatorem jest $\langle n \rangle = \langle -n \rangle$.

Pokażemy, że wszystkie podgrupy w $(\mathbb{Z}, +)$ są postaci $\langle n \rangle$ dla pewnego $n \in \mathbb{Z}$.

Niech $\{0\} \neq H \leq (\mathbb{Z}, +)$. Wybierzmy $k > 0$ najmniejsze takie, że $k \in H$. Chcemy pokazać, że $H = \langle k \rangle$. Z wyboru k wiemy, że $\langle k \rangle \subseteq H$. Przypuśćmy, że istnieje $l \in H \setminus \langle k \rangle$. Podzielmy l przez k z resztą, czyli $l = mk + r$, gdzie $0 \leq r < k$ oraz $l \in H$ i $mk \in H$. Wynika stąd, że $r \in H$. Z minimalności k otrzymujemy więc, że $r = 0$, skąd $l = m \cdot k \in \langle k \rangle$, co jest sprzeczne z założeniem. Stąd dowolna podgrupa $\mathbb{Z}$ jest generowana przez jeden element.

Zadanie 4.
Wyznaczyć wszystkie podgrupy $(\mathbb{Z}_n, +)$ dla dowolnego n.

Rozwiązanie:
Niech p będzie liczbą pierwszą. Pokażemy, że wszystkimi podgrupami grupy $(\mathbb{Z}_p, +)$ są $\langle 1\rangle = \mathbb{Z}_p$ oraz $\langle 0\rangle = \{0\}$. Przypuśćmy, że dla $k \neq 0$ oraz $k \in \mathbb{Z}_p$, zbiór $\langle k\rangle$ jest podgrupą $(\mathbb{Z}_p, +)$. Wówczas skoro $NWD(k, p) = 1$ (bo p jest liczbą pierwszą), to istnieje $\alpha, \beta \in \mathbb{Z}$ takie, że $k\alpha + p\beta = 1$. A stąd $1 \in \langle k\rangle$. Stąd $\mathbb{Z}_p = \langle 1\rangle \subseteq \langle k\rangle$, czyli $\langle k\rangle = \mathbb{Z}_p$. Dla nie pierwszej liczby n wszystkimi podgrupami będą $\langle 0\rangle, \langle 1\rangle = \mathbb{Z}_n$ oraz $\langle x_1\rangle, \ldots, \langle x_m\rangle$ dla $x_1, \ldots, x_m$ będącymi dzielnikami liczby n. Weźmy $\langle 0\rangle \neq H \leq \mathbb{Z}_n$ i niech $0 \neq k \in H$ będzie najmniejszym elementem H różnym od zera. Pokażemy, że $\langle k\rangle = H$. Przypuśćmy, przeciwnie że istnieje $l \in H \setminus \langle k\rangle$, czyli $l = mk + r$ dla pewnego $0 \leq r \leq k$, wówczas $r \in H$, czyli z minimalności k mamy $r = 0$ skąd $l = mk$, co jest sprzeczne. Czyli dowolna grupa w $(\mathbb{Z}_n, +)$ jest postaci $\langle k\rangle$, gdzie k jest dzielnikiem n.

Zadanie 5.
Znajdź wszystkie podgrupy grupy $\mathbb{Z}_{12}$ oraz rzędy wszystkich jej elementów, gdzie $\mathbb{Z}_{12}$ jest cykliczną grupą rzędu 12.

Rozwiązanie:
Podgrupami będą $\langle 0\rangle, \langle 1\rangle, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle, \langle 6\rangle$. Mamy również

k^1	k^2	k^3	k^4	k^5	k^6	k^7	k^8	k^9	k^{10}	k^{11}	k^{12}
0											
1	2	3	4	5	6	7	8	9	10	11	0
2	4	6	8	10	0						
3	6	9	0								
4	8	0									
5	10	3	8	1	6	11	4	9	2	7	0
6	0										
7	2	9	4	11	6	1	8	3	10	5	0
8	4	0									
9	6	3	0								
10	8	6	4	2	0						
11	10	9	8	7	6	5	4	3	2	1	0

Zatem

k	0	1	2	3	4	5	6	7	8	9	10	11
$o(k)$	1	12	6	4	3	12	2	12	3	4	6	12

Zadanie 6.
Rozstrzygnij, czy zbiór

$$S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$$

liczb zespolonych o module 1 z działaniem mnożenia liczb zespolonych tworzy grupę.

Rozwiązanie:
Musimy sprawdzić, że zbiór spełnia aksjomaty grupy

1. Weźmy $x = a_1 + b_1 i,\ y = a_2 + b_2 i,\ z = a_3 + b_3 i \in S^1$, wówczas

$$\begin{aligned} x \cdot (y \cdot z) &= (a_1 + b_1 i) \cdot ((a_2 + b_2 i) \cdot (a_3 + b_3 i)) = \\ &= (a_1 + b_1 i) \cdot (a_2 a_3 + a_2 b_3 i + a_3 b_2 i - b_2 b_3) = \\ &= a_1 a_2 a_3 + a_1 a_2 b_3 i + a_1 a_3 b_2 i - a_1 b_2 b_3 + a_2 a_3 b_1 i - a_2 b_1 b_3 - a_3 b_1 b_2 - b_1 b_2 b_3 i = \\ &= a_1 a_2 a_3 - a_1 b_2 b_3 - a_2 b_1 b_3 - a_3 b_1 b_2 + i(a_1 a_2 b_3 + a_1 a_3 b_2 + a_2 a_3 b_1 - b_1 b_2 b_3) \end{aligned}$$

$$\begin{aligned} (x \cdot y) \cdot z &= ((a_1 + b_1 i) \cdot (a_2 + b_2 i)) \cdot (a_3 + b_3 i) = \\ &= (a_1 a_2 + a_1 b_2 i + a_2 b_1 i - b_1 b_2) \cdot (a_3 + b_3 i) = \\ &= a_1 a_2 a_3 + a_1 a_2 b_3 i + a_1 a_3 b_2 i - a_1 b_2 b_3 + a_2 a_3 b_1 i - a_2 b_1 b_3 - a_3 b_1 b_2 - b_1 b_2 b_3 i = \\ &= a_1 a_2 a_3 - a_1 b_2 b_3 - a_2 b_1 b_3 - a_3 b_1 b_2 + i(a_1 a_2 b_3 + a_1 a_3 b_2 + a_2 a_3 b_1 - b_1 b_2 b_3) \end{aligned}$$

   Stąd $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

2. Elementem neutralnym jest 1, bo wówczas $|1| = 1$ oraz dla $z = (a, b) \in S^1$ zachodzi

$$z \cdot 1 = (a, b) \cdot (1, 0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a, b) = z$$

   Zatem istnieje element neutralny.

3. Sprawdźmy, czy dla $z = (a, b) \in S^1$ liczba $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ jest elementem odwrotnym do elementu z

$$(a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = \left(a \cdot \frac{a}{a^2 + b^2} - b \cdot \frac{-b}{a^2 + b^2}, a \cdot \frac{-b}{a^2 + b^2} + b \cdot \frac{a}{a^2 + b^2}\right) = (1, 0) = 1$$

   sprawdźmy czy $z^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) \in S^1$. Mamy

$$|z^{-1}| = \sqrt{\left(\frac{a}{a^2 + b^2}\right)^2 + \left(\frac{-b}{a^2 + b^2}\right)^2} = \frac{1}{\sqrt{a^2 + b^2}} = \frac{1}{1} = 1$$

   Korzystamy tu z faktu $\sqrt{a^2 + b^2} = 1$, bo $(a, b) \in S^1$.

Zatem zbiór S^1 jest grupą.

Ćwiczenia 2

Zadanie 1.

a) Pokaż, że $H \subseteq G$ jest podgrupą wtedy i tylko wtedy, gdy dla dowolnych $a, b \in G$ jeśli $a, b \in H$, to $ab^{-1} \in H$ oraz $1 \in H$.

b) Niech H będzie podzbiorem grupy G takim, że

- $1_G \in H$
- jeśli dwa z elementów x, y, xy należą do H, to również trzeci należy do H

Udowodnij, że H jest podgrupą w G.

Rozwiązanie:

a) $\Rightarrow$ Jeśli H jest podgrupą, to skoro $a \in H$, to również $a^{-1} \in H$, czyli $aa^{-1} = 1 \in H$. Jeśli $b \in H$, to również $b^{-1} \in H$, czyli $ab^{-1} \in H$.

$\Leftarrow$ Skoro dla $a, b \in H$ zachodzi $ab^{-1} \in H$ oraz $1 \in H$, to dla $a = 1$ mamy $1 \cdot b^{-1} \in H$, czyli $b^{-1} \in H$. Skoro $ab^{-1} \in H$ oraz $b^{-1} \in H$, to również $a(b^{-1})^{-1} \in H$. Wiemy, że $(b^{-1})^{-1} \in H$, czyli $ab \in H$. Zatem H jest podgrupą.

b) Jeśli $x, y \in H$ to również $xy \in H$ z drugiego warunku. Jeśli $x \in H$ oraz $xy = 1 \in H$, to również $y = x^{-1} \in H$.

Definicja: Rząd grupy G to liczba jej elementów. Rzędem elementu $a \in G$ nazywamy najmniejsze $n \geq 1$ takie, że $a^n = 1$ lub ∞, gdy takie n nie istnieje. Piszemy $o(a)$ lub $|a|$.

Fakt:

$$o(a) = |\langle a \rangle| = |\{a^m \mid m \in \mathbb{Z}\}|$$

Zadanie 2.

Sześcioelementowa grupa dihedralna D_6 to grupa izometrii trójkąta równobocznego.

a) Wykaż, że jest generowana przez dwa elementy: obrót - nazwijmy go ρ (zgodnie ze wskazówkami zegara) oraz symetrię osiową - nazwijmy ją σ. Wypisz każdy element jako iloczyn generatorów i napisz jaka to izometria płaszczyzny

b) Policz rząd każdego elementu

Rozwiązanie:

a) Dla trójkąta równobocznego o wierzchołkach A, B, C mamy

$$D_6 = \{id, o_{\frac{2\pi}{3}}, o_{\frac{4\pi}{3}}, S_A, S_B, S_C\}$$

Są to wszystkie izometrie, ponieważ permutacji wierzchołków trójkąta jest $3! = 6$. Działaniem w tej grupie jest składanie izometrii. Niech $o_{\frac{2\pi}{3}} = \rho$ oraz $S_A = \sigma$, wówczas $id = \rho^3 = \sigma^2$, $o_{\frac{4\pi}{3}} = \rho^2$, $S_B = \sigma \cdot \rho^2$, $S_C = \sigma \cdot \rho$. Zatem $\langle \rho, \sigma \rangle = D_6$.

b) Policzmy rząd każdego elementu.

k	id	$o_{\frac{2\pi}{3}}$	$o_{\frac{4\pi}{3}}$	S_A	S_B	S_C
$o(k)$	1	3	3	2	2	2

Mamy

- $\sigma^2 = id$
- $\rho^3 = id$
- $\sigma\rho\sigma = \rho^2$

Te trzy warunki wyznaczają nam działania w grupie.

Ogólnie dla $D_{2n} = \langle \rho, \sigma \rangle$ mamy działania $\sigma^2 = id$, $\rho^n = id$ oraz $\sigma\rho\sigma = \rho^{n-1}$.

Zadanie 3.
Niech $G = \mathbb{Z}_n$. Udowodnij, że wtedy dla dowolnego $r \in \mathbb{Z}_n$ zachodzi $o(r) = \frac{n}{NWD(n,r)}$.

Rozwiązanie:
Aby $\frac{n}{NWD(n,r)}$ było rzędem elementu r, to

1. liczba $r \cdot \frac{n}{NWD(n,r)}$ musi być podzielna przez n, bo wówczas $\frac{n}{NWD(n,r)} \cdot r$ to 0 w $\mathbb{Z}_n$
2. jeśli istnieje θ takie, że $\theta \cdot r = 0$ w $\mathbb{Z}_n$, to $\theta \geq \frac{n}{NWD(n,r)}$

Liczba $r \cdot \frac{n}{NWD(n,r)}$ jest podzielna przez n, ponieważ $\frac{r}{NWD(n,r)} \in \mathbb{Z}$, bo $NWD(n,r) \mid r$. Wiemy, że $n \mid \theta \cdot r$, gdzie $n = NWD(n,r) \cdot n'$ oraz $r = NWD(n,r) \cdot r'$ przy czym $NWD(n',r') = 1$. Mamy więc $NWD(n,r) \cdot n' \mid \theta \cdot NWD(n,r) \cdot r'$, czyli $n' \mid \theta \cdot r'$. Skoro $NWD(n',r') = 1$, to r' nie dzieli się przez n', czyli θ dzieli się przez n', skąd $\theta \geq n'$. Zatem $\theta \geq \frac{n}{NWD(n,r)}$.

Uwaga: W $\mathbb{Z}_n$ mamy $NWD(n,k_1) = NWD(n,k_2)$ wtedy i tylko wtedy, gdy $\langle k_1 \rangle = \langle k_2 \rangle$.

Zadanie 4.
Udowodnij, że w skończonej grupie rzędu parzystego istnieje element rzędu 2.

Rozwiązanie:
Niech G będzie parzystego rzędu, czyli $|G| = 2n$. Przypuśćmy, że taki element nie istnieje. Rozpatrzmy dla każdego elementu $a \in G \setminus \{e\}$ pary elementów $\{a, a^{-1}\}$. Wówczas $a \neq a^{-1}$, czyli $|\{a, a^{-1}\}| = 2$. Pokażemy teraz, że dla $a, b \in G \setminus \{e\}$ zachodzi albo $\{a, a^{-1}\} = \{b, b^{-1}\}$, albo $\{a, a^{-1}\} \cap \{b, b^{-1}\} = \emptyset$. Jeśli $a = b$, to wówczas $a^{-1} = b^{-1}$. Jeśli $a = b^{-1}$, to $a^{-1} = b$. Jeśli $a^{-1} = b$, to $a = b^{-1}$. Jeśli $a^{-1} = b^{-1}$, to $a = b$. Zatem mamy

$$G = \bigcup_{a \in G \setminus \{e\}} \{a, a^{-1}\} \cup \{e\}$$

czyli rząd grupy G jest nieparzysty. Mamy więc sprzeczność, skąd w G istnieje element rzędu 2.

Zadanie 5.
Niech $g \in G$ będzie elementem skończonego rzędu. Udowodnij, że $g^k = 1$ wtedy i tylko wtedy, gdy $o(g) \mid k$.

Rozwiązanie:
$\Rightarrow$ Załóżmy, że $g^k = 1$ oraz $k = o(g) \cdot m + r$ dla pewnego $0 \leq r < o(g)$. Wówczas

$$1 = g^k = g^{o(g)\cdot m + r} = \left(g^{o(g)}\right)^m \cdot g^r = 1 \cdot g^r$$

skąd otrzymujemy, że $r = 0$, zatem $o(g) \mid k$.
$\Leftarrow$ Jeśli $o(g) \mid k$, to wówczas $k = o(g) \cdot m$, czyli $g^k = g^{o(g)\cdot m} = \left(g^{o(g)}\right)^m = 1^m = 1$.

Definicja: Mówimy, że grupa G jest przemienna, jeśli dla każdych elementów $x, y \in G$ zachodzi $xy = yx$.

Przykłady:

- Grupa $\langle g \rangle$ jest przemienna, bo $g^k \cdot g^l = g^{k+l} = g^l \cdot g^k$.
- Grupa $GL(n, \mathbb{R})$ (macierzy odwracalnych z działaniem mnożenia) nie jest przemienna, bo $A \cdot B \neq B \cdot A$.

Zadanie 6.
Mówimy, że elementy $x, y \in G$ są przemienne, gdy $xy = yx$. Grupa G jest przemienna, gdy dowolne $x, y \in G$ są przemienne.

a) Pokaż, że jeśli $x, y \in G$ mają rząd 2 oraz xy ma rząd 2, to x oraz y są przemienne.

b) Grupa G jest taka, że dla dowolnego $g \in G$ zachodzi $g^2 = 1$. Pokaż, że G jest przemienna.

Rozwiązanie:

a) Mamy $x^2 = 1 \Leftrightarrow x = x^{-1}$, $y^2 = 1 \Leftrightarrow y = y^{-1}$ oraz $(xy)^2 = 1$, zatem skoro $x^{-1}y^{-1} = (xy)^{-1}$, to

$$xy = (x^{-1})(y^{-1}) = x^{-1}y^{-1} = (yx)^{-1} = yx$$

Zatem x oraz y są przemienne.

b) Dla dowolnych $x, y \in G$ mamy $xy \in G$, zatem skoro $x^2 = 1$, $y^2 = 1$ oraz $(xy)^2 = 1$, to x i y są przemienne, czyli cała grupa G jest przemienna.

Zadanie 7.
Niech $o(a) = m$, $o(b) = n$ oraz $ab = ba$. Udowodnij, że $o(ab) < \infty$. Czy wtedy $o(xy) = NWW(o(x), o(y))$?

Rozwiązanie:
Wiemy, że $a^m = 1$ oraz $b^n = 1$. Niech więc $M = NWW(m, n)$, wówczas $a^M = 1$ oraz $b^M = 1$, czyli $a^M b^M = 1$. Skoro a oraz b są przemienne, to mamy

$$a^M b^M = \underbrace{a \cdot \ldots \cdot a}_{M} \cdot \underbrace{b \cdot \ldots \cdot b}_{M} = \ldots = a \cdot b \cdot \underbrace{a \cdot \ldots \cdot a}_{M-1} \cdot \underbrace{b \cdot \ldots \cdot b}_{M-1} \overset{\text{indukcja}}{=} \underbrace{a \cdot b \cdot \ldots \cdot a \cdot b}_{M} = (ab)^M$$

Zatem $(ab)^M = 1$, czyli $o(ab) < \infty$.

Dla grupy $\mathbb{Z}_2$ mamy $o(1) = 2$ oraz $o(0) = 1$, zatem dla $x = y = 1$ mamy $o(xy) = o(0) = 1 \neq 2 = NWW(o(1), o(1)) = NWW(o(x), o(y))$.

Zadanie 8.
Niech $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ oraz $B = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \in GL(2, \mathbb{R})$. Oblicz $o(A), o(B)$ oraz $o(AB)$.

Rozwiązanie:
Mamy $o(A) = 2$ oraz $o(B) = 2$, ponieważ $A^2 = B^2 = I$. Wówczas dla $n \in \mathbb{N}_+$ mamy

$$(AB)^n = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \right)^n = I^n + \binom{n}{1} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot I^{n-1} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$

zatem $o(AB) = \infty$.

Zadanie 9.
Niech G będzie pewną grupą, zaś g, h jej elementami.

1. Udowodnij, że zachodzi $(gh)^{-1} = h^{-1}g^{-1}$ oraz $(g^n)^{-1} = (g^{-1})^n$ dla dowolnej liczby całkowitej dodatniej n.
2. Udowodnij, że $o(h^{-1}gh) = o(g)$, gdzie $o(g)$ oznacza rząd elementu g w grupie G
3. Udowodnij, że $o(g^{-1}) = o(g)$

Rozwiązanie:

1. Mamy
$$gh \cdot h^{-1}g^{-1} = g \cdot 1 \cdot g^{-1} = gg^{-1} = 1$$
skąd $h^{-1}g^{-1}$ jest elementem odwrotnym do gh, czyli $(gh)^{-1} = h^{-1}g^{-1}$. Mamy
$$g^n \cdot (g^{-1})^n = \underbrace{g \cdot \ldots \cdot g}_{n} \cdot \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{n} = \underbrace{g \cdot \ldots \cdot g}_{n-1} \cdot 1 \cdot \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{n-1} \overset{\text{indukcja}}{=} 1$$
stąd $(g^{-1})^n$ jest elementem odwrotnym do g^n, czyli $(g^n)^{-1} = (g^{-1})^n$.
2. Niech $o(g) = n$, wówczas skoro $h^{-1}h = e$, to mamy
$$\underbrace{h^{-1}gh \cdot \ldots \cdot h^{-1}gh}_{n} = h^{-1} \cdot \underbrace{g \cdot \ldots \cdot g}_{n} \cdot h = h^{-1} \cdot e \cdot h = h^{-1}h = e$$

Zatem $o(h^{-1}gh) \geq n = o(g)$. W drugą stronę, niech $n = o(h^{-1}gh)$, wówczas

$$\underbrace{h^{-1}gh \cdot \ldots \cdot h^{-1}gh}_{n} = e \Leftrightarrow h^{-1} \cdot \underbrace{g \cdot \ldots \cdot g}_{n} \cdot h = e \Leftrightarrow \underbrace{g \cdot \ldots \cdot g}_{n} = hh^{-1} = e$$

czyli $o(g) \geq n = o(h^{-1}gh)$. Stąd otrzymujemy $o(g) = o(h^{-1}gh)$.

3. Niech $o(g) = n$, wówczas mamy

$$\underbrace{g \cdot \ldots \cdot g}_{n} = e \Leftrightarrow g^{-1} \cdot g \cdot \underbrace{g \cdot \ldots \cdot g}_{n-1} = g^{-1} \Leftrightarrow e \cdot \underbrace{g \cdot \ldots \cdot g}_{n-1} = g^{-1} \overset{\text{indukcja}}{\Leftrightarrow} e = \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{n}$$

stąd $o(g^{-1}) \geq n = o(g)$. Analogicznie mamy $o(g) \geq o(g^{-1})$, czyli $o(g) = o(g^{-1})$.

Ćwiczenia 3

Zadanie 1.
Uzasadnić, że półgrupa G jest grupą wtedy i tylko wtedy, gdy dla dowolnych $a, b \in G$ równania $ax = b$ i $ya = b$ mają rozwiązania w G.

Rozwiązanie:
Półgrupa to zbiór G z działaniem, które jest łączne, czyli $\forall_{a,b,c \in G}\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

$\Rightarrow$ Jeśli G jest grupą, to dla $a, b \in G$ mamy $a \cdot (a^{-1}b) = b$ oraz $(ba^{-1})a = b$, czyli $x = a^{-1}b$ oraz $y = ba^{-1}$ są rozwiązaniami.

$\Leftarrow$ Chcemy pokazać, że istnieje element neutralny oraz że każdy element ma element odwrotny. Wiemy, że istnieje $e_a \in G$ takie, że $a \cdot e_a = a$ oraz istnieje $f_a \in G$ takie, że $f_a \cdot a = a$. Musimy pokazać, że $e_a = f_a$ oraz, że elementy te nie zależą od a. Weźmy dowolne $b \in G$ i pokażemy, że $b \cdot e_a = b$ oraz $f_a \cdot b = b$. Wiemy, że istnieje element $y_{ab} \in G$ taki, że $b = y_{ab}a$, wówczas $b \cdot e_a = (y_{ab} \cdot a) \cdot e_a = y_{ab} \cdot (a \cdot e_a) = y_{ab} \cdot a = b$, skąd $e = e_a$ jest takim elementem G, że dla dowolnego $b \in G$ zachodzi $b \cdot e = b$. Analogicznie pokazujemy, że element $f = f_a$ jest wyznaczony jednoznacznie. Teraz trzeba pokazać, że elementy e i f są równe. Mamy $e \cdot f$ równa się z jednej strony f, a z drugiej strony e, zatem $e = f$. Pokazaliśmy więc, że istnieje element neutralny. Wiemy, że istnieje element $x \in G$, że $a \cdot x = e$ oraz że istnieje $y \in G$ taki, że $y \cdot a = e$. Mamy $y = y \cdot e = y \cdot (a \cdot x) = (y \cdot a) \cdot x = e \cdot x = x$. Zatem dla dowolnego $a \in G$ istnieje element odwrotny i jest on wyznaczony jednoznacznie.

Zadanie 2.
Udowodnij, ze $o(ba) = o(ab)$.

Rozwiązanie:
Niech $n = o(ba) \leq \infty$, wówczas

$$\underbrace{ba \cdot \ldots \cdot ba}_{n} = e \Leftrightarrow b^{-1}a^{-1} = \underbrace{ab \cdot \ldots \cdot ab}_{n-1}$$

Wiemy, że $(ab)^{-1} = b^{-1}a^{-1}$, zatem

$$(ab)^{-1} = (ab)^{n-1} \Leftrightarrow 1 = (ab)^n$$

skąd otrzymujemy $o(ab) \leq n = o(ba)$. Analogicznie $o(ba) \leq o(ab)$.
Jeśli rzędy nie są równe, to co najmniej jeden z rzędów jest skończony. Wówczas niech $o(ba) < \infty$. Stąd otrzymujemy, że $o(ab) \leq o(ba) < \infty$.

Definicja: Homomorfizm grup to $f : (G, \cdot) \to (H, \star)$ taka, że dla dowolnych elementów grupy G zachodzi $f(g \cdot h) = f(g) \star f(h)$. Izomorfizm to homomorfizm z bijekcją.

Definicja: Niech H będzie podgrupą w grupie G. Wówczas $Ha = \{ha \mid h \in H\}$ nazywamy warstwą prawostronną względem podgrupy H wyznaczoną przez element a.

Dla dwóch różnych elementów zachodzi $Ha = Hb$ lub $Ha \cap Hb = \emptyset$.

Twierdzenie: (Lagrange'a) Niech $[G : H]$ oznacza liczbę warstw w grupie G względem podgrupy H. Wówczas dla dowolnej grupy skończonej G zachodzi $|G| = [G : H]|H|$.

Wnioski:

1. Jeśli H jest podgrupą w grupie skończonej G, to $|H| \mid |G|$.
2. Rząd elementu grupy skończonej dzieli rząd grupy.
3. Jeśli grupa ma rząd, który jest liczbą pierwszą, to nie posiada ona podgrup właściwych, czyli różnych od G i $\{e\}$.

Zadanie 3.
Znajdź wszystkie grupy rzędu co najwyżej 3.

Rozwiązanie:
Grupy rzędu 1 to grupy zawierające element neutralny, czyli jedyną grupą rzędu 1 to $\{e\}$. Grupą rzędu 2 jest $\mathbb{Z}_2$. Jest to jedyna grupa, ponieważ jeśli $G = \{e, a\}$, to $a^2 = e$, czyli $o(a) = 2$, skąd $\langle a \rangle = G$. Jedyną grupą cykliczną o dwóch elementach jest $\mathbb{Z}_2$. Grupą rzędu 3 jest $\mathbb{Z}_3$. Jest to jedyna grupa, ponieważ jeśli $a \in G$, to jego rząd może być równy 1 lub 3. Elementem o rzędzie 1 jest element neutralny. Jeśli a jest rzędu 3, to podgrupa generowana przez a, czyli $\langle a \rangle$ ma trzy elementy. Jako, że jest to podgrupa w G, która też ma trzy elementy, toteż $\langle a \rangle = G$.

Zadanie 4.
Pokaż, że grupy G oraz H są izomorficzne, gdzie

a) $G = \mathbb{Z}_n$, $H = C_n = \{\varepsilon^k \mid k = n - 1\}$, gdzie ε to pierwiastek pierwotny stopnia n z 1, a w C_n działanie grupowe to mnożenie.

b) $G = (\mathbb{Q}, +)$, $H = (\mathbb{Q}, \star)$, gdzie $a \star b = a + b - 2$

Rozwiązanie:

a) Pierwiastki z jedynki są postaci $\varepsilon = e^{\frac{2\pi i}{n}}$, wówczas $\varepsilon^k \cdot \varepsilon^l = \varepsilon^{(k+l) \mod n}$. Niech $f : C_n \to \mathbb{Z}_n$ zadane jest wzorem $f(\varepsilon^k) = k$. Chcemy sprawdzić, czy f jest homomorfizmem. Mamy

$$f(\varepsilon^k \cdot \varepsilon^l) = f(\varepsilon^{(k+l) \mod n}) = (k + l) \mod n = \big(f(\varepsilon^k) + f(\varepsilon^n)\big) \mod n$$

Niech $g : (\mathbb{Z}_n, +) \to C_n$, zadane będzie wzorem $g(k) = \varepsilon^k$, wówczas $g \circ f(\varepsilon^k) = g(k) = \varepsilon^k$, czyli $g \circ f = id_{C_n}$ oraz $f \circ g(k) = f(\varepsilon^k) = k$, czyli $f \circ g = id_{\mathbb{Z}_n}$, zatem f jest izomorfizmem.

b) Niech $\phi : G \to H$, chcemy zobaczyć jaki może być obraz elementu neutralnego. Mamy $\phi(e_G) \cdot e_H = \phi(e_G) = \phi(e_G \cdot e_G) = \phi(e_G) \cdot \phi(e_G)$, skąd $e_H = \phi(e_G)$. Zatem element neutralny przechodzi na element neutralny. Rozważmy więc funkcję $f : (\mathbb{Q}, +) \to (\mathbb{Q}, \star)$ zadaną wzorem $f(k) = k + 2$. Mamy

$$f(k + l) = k + l + 2 = k + 2 + l + 2 - 2 = f(k) + f(l) - 2 = f(k) \star f(l)$$

czyli f jest homomorfizmem. Niech $g : (\mathbb{Q}, \star) \to (\mathbb{Q}, +)$ zadane będzie wzorem $g(k) = k - 2$, wówczas g jest funkcją odwrotną do f, czyli f jest izomorfizmem.

Zadanie 5.
Udowodnij, że zbiór U macierzy postaci $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$, gdzie $x \in \mathbb{C}$ jest podgrupą grupy macierzy górnotrójkątych odwracalnych o współczynnikach zespolonych izomorficzną z grupą $(\mathbb{C}, +)$ zbioru liczb zespolonych z dodawaniem.

Rozwiązanie:
Musimy udowodnić, że zbiór U z działaniem mnożenia jest podgrupą macierzy górnotrójkątych odwracalnych o współczynnikach zespolonych oraz że podgrupa ta jest izomorficzna z grupą $(\mathbb{C}, +)$ zbioru liczb zespolonych z działaniem dodawania. Udowodnijmy najpierw, że zbiór U jest podgrupą.

1. Weźmy $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} \in U$, wówczas

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & y+x \\ 0 & 1 \end{bmatrix} \in U \text{ ponieważ } x + y \in \mathbb{C}$$

2. Elementem odwrotnym do $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ jest $\begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix}$, bo wówczas

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x-x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Oczywiście $\begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} \in U$ ponieważ $-x \in \mathbb{C}$.

Zatem zbiór U z działaniem mnożenia tworzy podgrupę $GL(2, \mathbb{C})$. Udowodnimy teraz, że podgrupa ta jest izomorficzna z grupą $(\mathbb{C}, +)$. Niech $f : U \to \mathbb{C}$ zadane będzie wzorem $f\left(\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\right) = x$. Chcemy sprawdzić, że f jest homomorfizmem. Mamy

$$f\left(\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix}\right) = f\left(\begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix}\right) = x + y = f\left(\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\right) + f\left(\begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix}\right)$$

Zatem f jest homomorfizmem. Pokażemy teraz, że f jest bijekcją, czyli że istnieje $g : \mathbb{C} \to U$ takie, że $g \circ f = id_U$ oraz $f \circ g = id_{\mathbb{C}}$. Niech $g(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$, wówczas

$$g \circ f\left(\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\right) = g(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$$

oraz

$$f \circ g(x) = f\left(\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\right) = x$$

Stąd f jest bijekcją, zatem grupy $(\mathbb{C}, +)$ i $(U, \cdot)$ są izomorficzne.

Definicja: Permutację $\sigma \in S_n$ nazywamy cyklem o długości k, gdy istnieje podzbiór $A = \{a_1, \ldots, a_k\} \subseteq \{1, \ldots, n\}$ taki, że $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_k) = a_1$ oraz $\sigma(i) = i$ dla $i \in \{1, \ldots, n\} \setminus A$. Taką permutację oznaczamy przez $\sigma = (a_1\ a_2\ \ldots\ a_{k-1}\ a_k)$.

Definicja: Nośnik permutacji σ jest zdefiniowany następująco

$$\operatorname{supp}(\sigma) = \{a \in \{1, \ldots, n\} \mid \sigma(a) \neq a\}$$

Mówimy, że permutacje σ i τ są rozłączne, gdy $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = \emptyset$.

Twierdzenie: (Rozkład permutacji na cykle) Każdą permutację można przestawić w postaci iloczynu cykli rozłącznych. Przedstawienie to jest jednoznaczne z dokładnością do kolejności cykli.

Przykład: Dla permutacji $\sigma = \begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 3\ 4\ 6\ 2\ 6\ 1\ 9\ 8\ 7 \end{pmatrix}$, $\sigma \in S_9$ mamy następujące przedstawienie $(1\ 3\ 6)(2\ 4)(5)(7\ 9)(8)$.

Zadanie 6.
Wyznacz wszystkie podgrupy S_3 permutacji zbioru 3-elementowego.

Rozwiązanie:
Permutacji zbioru n elementowego jest $n!$, czyli $|S_n| = n!$, skąd mamy

$$S_3 = \{id, (1\ 2\ 3), (1\ 2), (2\ 3), (1\ 3), (1\ 3\ 2)\}$$

Z twierdzenia Lagrange'a wszystkie podgrupy właściwe mogą mieć rzędy $1, 2, 3$ lub 6. Podgrupami rzędu 1 jest id, natomiast podgrupą rzędu 6 jest S_3. Pozostałe podgrupy mają rząd 2 lub 3, czyli są cykliczne, czyli są generowane przez jeden element. Permutacje o cyklu długości 3 są rzędu 3, ponieważ

$$(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2) \quad \text{oraz} \quad (1\ 3\ 2)(1\ 2\ 3) = (1\ 2\ 3)$$

Mamy więc $o((1\ 2\ 3)) = 3$ oraz $\langle(1\ 2\ 3)\rangle = \{id, (1\ 2\ 3), (1\ 3\ 2)\}$. Stąd $o((1\ 3\ 2)) = 3$. Mamy również $\langle(1\ 2)\rangle = \{id, (1\ 2)\}$, $\langle(2\ 3)\rangle = \{id, (2\ 3)\}$ oraz $\langle(1\ 3)\rangle = \{id, (1\ 3)\}$. Aby uzasadnić, że nie ma więcej podgrup, korzystamy z twierdzenia Lagrange'a. Przypuśćmy, że mamy podgrupę $H \leq S_3$, wówczas z twierdzenia Lagrange'a moc tej grupy wynosi $|H| = \{1, 2, 3, 6\}$, czyli $H = \{e\}$ lub $H = S_3$. Jeśli $|H| = 2$ lub $|H| = 3$, to $H = \langle a\rangle$ dla pewnego $a \in S_3$. Stąd wynika, że wypisaliśmy wszystkie podgrupy S_3.

Zadanie 7.
Pokaż, że istnieją dokładnie dwie grupy rzędu 4.

Rozwiązanie:
Niech $|G| = 4$, wówczas rzędy jej elementów to $1, 2$ lub 4. Tylko element neutralny ma rząd 1.

Mamy więc dwie możliwości

1. W G istnieje element rzędu 4, czyli $o(a) = 4$
2. W G dla każdego $a \in G$ oraz $a \neq e$ zachodzi $o(a) = 2$

Jeśli w a istnieje element rzędu 4, to podgrupa generowana przez element a ma cztery elementy, czyli $\langle a \rangle = G$, ponieważ jest to grupa cykliczna. Grupa ta jest izomorficzna z $\mathbb{Z}_4$. Jeśli każdy element poza elementem neutralnym ma rząd 2, to grupa jest przemienna. Mamy $G = \{e, a, b, ab\}$, ponieważ gdyby $ab = a$ (BSO), to b byłoby elementem neutralnym, gdyby $ab = e$, to $a = b^{-1}$, czyli $a = b$. Stwórzmy więc tabelkę działań w grupie

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Jest to grupa izomorficzna z $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(x, y) \mid x \in \mathbb{Z}_2,\ y \in \mathbb{Z}_2\}$ z działaniem po współrzędnych, ponieważ zachodzi izomorfizm $e \to (0, 0)$, $a \to (0, 1)$, $b \to (1, 0)$ oraz $ab \to (1, 1)$.

Zadanie 8.
Niech $x, y \in G$ będą elementami grupy takimi, że $NWD(o(x), o(y)) = 1$. Pokaż, że wówczas $\langle x \rangle \cap \langle y \rangle = \{1\}$.

Rozwiązanie:
Załóżmy, że mamy $NWD(o(x), o(y)) = 1$ oraz, że $k \in \langle x \rangle \cap \langle y \rangle$. Wówczas $k = x^i$ dla pewnego $i \in \{0, 1, \ldots, n-1\}$ oraz $k = y^j$ dla $j \in \{0, 1, \ldots, m-1\}$, gdzie $n = o(x)$ oraz $m = o(y)$. Wówczas mamy

$$k^n = (x^i)^n = 1 = (y^j)^m = k^m$$

czyli $o(k) \mid n$ oraz $o(k) \mid m$. Ale skoro $NWD(n, m) = 1$, to stąd $o(k) = 1$. Jedynym elementem rzędu 1 jest element neutralny, skąd $k = \{1\}$.

Ćwiczenia 4

Fakt: Jeśli σ i τ są permutacjami rozłącznymi, to są one przemienne, czyli $\sigma\tau = \tau\sigma$.

Zadanie 1.
Niech $\sigma, \rho \in S_n$ będą permutacjami. Uzasadnij, że w rozkładzie na cykle rozłączne permutacji $\sigma\rho\sigma^{-1}$ występuje tyle samo cykli określonej długości co w ρ. Co więcej, jeśli w rozkładzie na cykle rozłączne permutacji ρ występuje cykl $(a_1, \ldots, a_k)$, to w rozkładzie $\sigma\rho\sigma^{-1}$ występuje cykl $(\sigma(a_1), \ldots, \sigma(a_k))$ oraz, że innych cykli w tym rozkładzie nie ma.

Rozwiązanie:
Pokażemy najpierw, że dowolna permutacja jest złożeniem transpozycji. Każda permutacja rozkłada się na cykle rozłączne, zatem wystarczy, że pokażemy, że każdy cykl jest złożeniem transpozycji. Niech dany jest cykl $(a_1, \ldots, a_n)$. Chcemy aby element a_1 przeszedł na a_2, element a_2 przeszedł na a_3 itd. aż do elementu a_5 który przechodzi na a_1. Stosując permutację (a_1, a_2), element a_1 przechodzi na a_2, natomiast element a_2 przechodzi na a_1. Pozostałe elementy nie zmieniają pozycji.

$$\begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_k \\ a_2 & a_1 & a_3 & \ldots & a_k \end{pmatrix}$$

Stosując transpozycję (a_1, a_3), element a_1 przechodzi na a_3, natomiast element a_3 przechodzi na a_1, pozostałe elementy nie zmieniają pozycji.

$$\begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_k \\ a_2 & a_3 & a_1 & \ldots & a_k \end{pmatrix}$$

Postępując indukcyjnie, dochodzimy do sytuacji, gdzie mamy permutację $(a_2, a_3, \ldots, a_1, a_k)$. Stosując transpozycję (a_1, a_k), element a_1 przechodzi na a_k, natomiast element a_k przechodzi na a_1, czyli mamy permutację $(a_2, a_3, \ldots, a_k, a_1)$. Zatem cykl $(a_1, \ldots, a_k)$ jest złożeniem transpozycji $(a_1, a_k)(a_1, a_{k-1}) \ldots (a_1, a_3)(a_1, a_2)$.

Pokażemy teraz, że można się ograniczyć do przypadku, gdy permutacja σ jest transpozycją. Niech $\sigma = \sigma_m \cdot \ldots \cdot \sigma_1$. Załóżmy, że teza zachodzi dla transpozycji, czyli że $\sigma_1\rho\sigma_1^{-1}$ ma tyle samo cykli co ρ. Wówczas $\sigma_2(\sigma_1\rho\sigma_1^{-1})\sigma_2^{-1}$ ma tyle samo cykli co $\sigma_1\rho\sigma_1^{-1}$, czyli ma tyle samo cykli co ρ. Postępując indukcyjnie dochodzimy do konkluzji, że $\sigma_m \cdot \ldots \cdot \sigma_1\rho\sigma_1^{-1} \cdot \ldots \cdot \sigma_m^{-1}$ ma tyle samo cykli co ρ. Zatem wystarczy pokazać tezę dla σ będącego transpozycją.

Pokażemy, że wystarczy rozpatrzeć przypadek, gdy ρ jest jednym cyklem. ρ rozkłada się na rozłączne cykle, zatem niech $\rho = \rho_1 \cdot \ldots \cdot \rho_n$. Mamy

$$\sigma\rho\sigma^{-1} = \sigma\rho_1 \cdot \ldots \cdot \rho_n\sigma^{-1} = \sigma\rho_1\sigma^{-1} \cdot \ldots \cdot \sigma\rho_n\sigma^{-1}$$

Załóżmy, że teza zachodzi dla jednego cyklu, wówczas $\sigma\rho_1\sigma^{-1}$ ma tyle samo cykli co ρ_1, $\sigma\rho_2\sigma^{-1}$ ma tyle samo cykli co ρ_2 itd. aż do $\sigma\rho_n\sigma^{-1}$, które ma tyle samo cykli co ρ_n. Zatem $\sigma\rho\sigma^{-1}$ ma tyle samo cykli co $\rho_1 \cdot \ldots \cdot \rho_n = \rho$. Zatem wystarczy rozpatrzyć ρ jako pojedynczy cykl.

Pokażemy więc tezę z zadania jedynie dla σ będącego transpozycją oraz ρ będącego cyklem.

Jeśli σ i ρ są rozłączne, to wtedy są one przemienne, czyli mamy $\sigma\rho\sigma^{-1} = \rho\sigma\sigma^{-1} = \rho$, skąd teza jest oczywista. σ jest identycznością na ρ, zatem dla $\rho = (a_1, \ldots, a_k)$ mamy

$$\sigma\rho\sigma^{-1} = \rho = (a_1, \ldots, a_k) = (\sigma(a_1), \ldots, \sigma(a_k))$$

Czyli cykli określonej długości jest tyle samo w ρ co w $\sigma\rho\sigma^{-1}$.

Jeśli σ i ρ nie są do końca rozłączne, czyli dla $\rho = (a_1, \ldots, a_k)$ mamy $\sigma = (a_i, x)$ dla pewnego $x \neq a_i$, to wówczas jako, że $\sigma = \sigma^{-1}$ mamy

$$\sigma\rho\sigma(a_1) = \rho(a_1) = a_2 = \sigma(a_2)$$

$$\vdots$$

$$\sigma\rho\sigma(a_{i-1}) = \sigma\rho(a_{i-1}) = \sigma(a_i) = x = \sigma(a_i)$$

$$\sigma\rho\sigma(a_i) = \sigma\rho(x) = \sigma(x) = a_i \quad \text{(tu mamy identyczność)}$$

$$\vdots$$

$$\sigma\rho\sigma(x) = \sigma\rho(a_i) = \sigma(a_{i+1}) = a_{i+1}$$

Zatem otrzymujemy

$$\sigma\rho\sigma = (a_1, a_2, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_k) = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_{i-1}), \sigma(a_i), \ldots, \sigma(a_k))$$

Ten cykl jest takiej samej długości co ρ.

Jeśli σ i ρ nie są rozłączne, czyli dla $\rho = (a_1, \ldots, a_k)$ mamy $\sigma = (a_i, a_j)$, gdzie BSO $i < j$, to wtedy mamy

$$\sigma\rho\sigma(a_1) = \rho(a_1) = a_2 = \sigma(a_2)$$

$$\vdots$$

$$\sigma\rho\sigma(a_{i-1}) = \sigma\rho(a_{i-1}) = \sigma(a_i) = a_j$$

$$\sigma\rho\sigma(a_i) = \sigma\rho(a_j) = \sigma(a_{j+1}) = a_{j+1}$$

$$\vdots$$

$$\sigma\rho\sigma(a_{j-1} = \sigma\rho(a_{j-1}) = \sigma(a_j) = a_i$$

$$\sigma\rho\sigma(a_j = \sigma\rho(a_i) = \sigma(a_{i+1}) = a_{i+1}$$

$$\vdots$$

$$\sigma\rho\sigma(a_k = a_1 = \sigma(a_1)$$

Zatem otrzymujemy

$$\sigma\rho\sigma = (a_1, \ldots, a_{i-1}, a_j, a_{i+1}, \ldots, a_{j-1}, a_i, a_{j+1}, \ldots, a_k) = (\sigma(a_1), \ldots, \sigma(a_i), \ldots, \sigma(a_j), \ldots, \sigma(a_k))$$

Ten cykl jest tej samej długości co ρ.

W każdym z trzech przypadków nie ma innych cykli niż $(\sigma(a_1), \ldots, \sigma(a_k))$. $\square$

Zadanie 2.
Rozłóż na rozłączne cykle następujące permutacje

a) $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 5 & 1 & 4 & 2 & 6 & 9 & 8 & 10 \end{pmatrix}$

b) $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 1 & 10 & 2 & 4 & 3 & 5 & 8 & 9 & 6 \end{pmatrix}$

A następnie policz $\sigma_1 \cdot \sigma_2$, $\sigma_2 \cdot \sigma_1$ oraz $\sigma_1 \cdot \sigma_2 \cdot \sigma_1^{-1}$.

Rozwiązanie:

a) Mamy $\sigma_1 = (1\ 3\ 5\ 4)(2\ 7\ 6)(8\ 9)(10)$

b) Mamy $\sigma_2 = (1\ 7\ 5\ 4\ 2)(3\ 10\ 6)(8)(9)$

Dalej mamy

$$\sigma_1 \cdot \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 1 & 10 & 2 & 4 & 3 & 5 & 8 & 9 & 6 \\ 6 & 3 & 10 & 7 & 1 & 5 & 4 & 9 & 8 & 2 \end{pmatrix} = (1\ 6\ 5)(2\ 3\ 10)(4\ 7)(8\ 9)$$

$$\sigma_2 \cdot \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 5 & 1 & 4 & 2 & 6 & 9 & 8 & 10 \\ 10 & 5 & 4 & 7 & 2 & 1 & 3 & 9 & 8 & 6 \end{pmatrix} = (1\ 10\ 6)(2\ 5)(3\ 4\ 7)(8\ 9)$$

$$\sigma_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 6 & 1 & 5 & 3 & 7 & 2 & 9 & 8 & 10 \end{pmatrix}$$

$$\sigma_1 \cdot \sigma_2 \cdot \sigma_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 6 & 1 & 5 & 3 & 7 & 2 & 9 & 8 & 10 \\ 2 & 3 & 7 & 4 & 10 & 5 & 1 & 9 & 8 & 6 \\ 7 & 5 & 6 & 1 & 10 & 4 & 3 & 8 & 9 & 2 \end{pmatrix} = (1\ 7\ 3\ 6\ 4)(2\ 5\ 10)(8)(9)$$

Zadanie 3.
Udowodnij, że jeśli $|\sigma_{i_r}| = m_r$, gdzie σ_{i_r} to cykle parami rozłączne, to wtedy $o(\sigma_{i_1}, \ldots, \sigma_{i_k}) = NWW(m_{i_1}, \ldots, m_{i_k})$.

Rozwiązanie:
Niech $(a_1, \ldots, a_k) \in S_n$, wówczas $o((a_1, \ldots, a_k)) = k$, ponieważ trzeba k razy zastosować tę permutację, aby osiągnąć identyczność. Wiemy, że jeśli σ i τ to permutacje rozłączne, to są one przemienne, czyli $\sigma\tau = \tau\sigma$. Szukamy takiego najmniejszego M, że $(\sigma_{i_1}, \ldots, \sigma_{i_k})^M = 1$. Skoro σ_{i_r} są parami rozłączne, to jest to równoważne z tym, że $\sigma_{i_1}^M \ldots \sigma_{i_k}^M = 1$. Stąd z jednoznaczności rozkładu na cykle rozłączne mamy $\sigma_{i_1}^M = \ldots = \sigma_{i_k}^M = 1$. Wówczas skoro $\sigma_{i_j}^M = 1$, to $o(\sigma_{i_j}) \mid M$, czyli $M \geq NWW(m_{i_1}, \ldots, m_{i_k})$. Dalej mamy

$$(\sigma_{i_1}, \ldots, \sigma_{i_k})^{NWW(m_{i_1}, \ldots, m_{i_k})} = \sigma_{i_1}^{NWW(m_{i_1}, \ldots, m_{i_k})} \ldots \sigma_{i_k}^{NWW(m_{i_1}, \ldots, m_{i_k})} = 1$$

czyli $o(\sigma_{i_1}, \ldots, \sigma_{i_k}) \leq NWW(m_{i_1}, \ldots, m_{i_k})$. Skąd $o(\sigma_{i_1}, \ldots, \sigma_{i_k}) = NWW(m_{i_1}, \ldots, m_{i_k})$.

Zadanie 4.
Jakie są możliwe rzędy elementów w S_5?

Rozwiązanie:
Zapisujemy 5 w postaci różnych rozkładów, a następnie liczymy NWW rzędów każdego cyklu. Możliwe rozkłady to

$$5 = 1+1+1+1+1 \qquad 5 = 4+1 \qquad 5 = 3+1+1 \qquad 5 = 2+1+1+1+1$$

$$5 = 3+2 \qquad 5 = 2+2+1 \qquad 5 = 5$$

Zatem możliwe rzędy wynoszą kolejno $1,\ 4,\ 3,\ 2,\ 3\cdot 2 = 6,\ 2,\ 5$.

Zadanie 5.
Niech $f : G \to H$ będzie homomorfizmem grup.

a) Pokaż, że jeśli a jest elementem skończonego rzędu, to $o(f(a)) \mid o(a)$.

b) Uzasadnij, że jeśli grupa G jest generowana przez elementy $g_1, \ldots, g_k$ to istnieje co najwyżej jeden homomorfizm taki, że $f(g_i) = h_i$, gdzie $h_i \in H$ są ustalone.

c) Podaj przykład grupy G wraz z zestawem minimalnym generatorów $g_1, \ldots, g_k$ oraz grupy H wraz z elementami $h_1, \ldots, h_k$ tak, by założenia punktu a) były spełnione, ale żeby nie istniał żadem homomorfizm f taki, że $f(g_i) = h_i$.

Rozwiązanie:

a) Dla dowolnego homomorfizmu $f : G \to H$ zachodzi $f(1_G) = 1_H$, czyli element neutralny przechodzi na element neutralny. Weźmy dowolny element $a \in G$ oraz załóżmy, że $o(a) = n$, czyli $a^n = 1_G$. Wówczas
$$(f(a))^n = f(a^n) = f(1_G) = 1_H$$
czyli $o(f(a)) \mid n = o(a)$, bo jeśli $g^m = 1$, to $o(g) \mid m$.

b) Niech $G = \langle g_1, \ldots, g_k \rangle$. Chcemy pokazać, że istnieje co najwyżej jeden homomorfizm f, taki, że $f(g_i) = h_i$ dla pewnych $\{h_1, \ldots, h_k\} \in H$. Niech $g \in G$ oraz niech $g = g_{i_1}^{\alpha_1} \ldots g_{i_M}^{\alpha_M}$, czyli g jest przedstawione za pomocą generatorów. Wówczas mamy
$$f(g) = f(g_{i_1}^{\alpha_1} \ldots g_{i_M}^{\alpha_M}) = f(g_{i_1})^{\alpha_1} \ldots f(g_{i_M})^{\alpha_M} = h_{i_1}^{\alpha_1} \ldots h_{i_M}^{\alpha_M}$$
Zatem element $f(g)$ jest jednoznacznie wyznaczony przez wartości $h_i \in H$, zatem istnieje co najwyżej jeden homomorfizm.

c) Chcemy pokazać, że istnieją grypy G i H takie, że $f(g_i) = h_i$ oraz że $o(f(g_i)) \mid o(g_i)$. Niech $G = D_6 = \langle \sigma, \rho \rangle = \{\sigma, \rho \mid \sigma^2 = 1,\ \rho^3 = 1,\ \sigma\rho\sigma = \rho^2\}$ oraz $H = \mathbb{Z}_3 = \langle 1 \rangle$. Wiemy, że $o(\sigma) = 2$ oraz $o(\rho) = 3$, zatem jeśli istnieje homomorfizm $f : D_6 \to \mathbb{Z}_3$, to $o(f(\sigma)) = 1$ lub $o(f(\sigma)) = 2$ oraz $o(f(\rho)) = 1$ lub $o(f(\rho)) = 3$. W $\mathbb{Z}_3$ nie istnieje element rzędu 2, zatem $f(\sigma) = 0$. Niech więc $h_1 = 0$ oraz $h_2 = 2$, wówczas $f(\rho) = 2$, czyli
$$f(\sigma\rho\sigma) = f(\sigma) + f(\rho) + f(\sigma) = 0 + 2 + 0 = 2 \neq 1 = 2 + 2 = f(\rho) + f(\rho)$$
Zatem taki homomorfizm nie istnieje.

Zadanie 6.
Znajdź wszystkie homomorfizmy

a) $\mathbb{Z}_5 \to S_3$

b) $\mathbb{Z}_3 \to S_3$

c) $\mathbb{Z}_4 \to D_4$

d) $\mathbb{Z}_n \hookrightarrow G$ (tu pytanie jest tylko o monomorfizmy)

Rozwiązanie:

a) Mamy grupę cykliczną, zatem wystarczy zadać f na generatorze. Mamy $\mathbb{Z}_5 = \langle 1 \rangle$, zatem skoro $o(1) = 5$, to $o(f(1)) = 1$ lub $o(f(1)) = 5$. Możliwe rzędy elementów w S_3 to $1, 2, 3$ lub 6, zatem nie ma takiego elementu, który ma rząd 5. Zatem $o(f(1)) = 1$, czyli $f(1) = id$. Zatem dla dowolnego elementu $k \in \mathbb{Z}_5$ zachodzi $f(k) = id$. Czyli istnieje tylko jeden taki homomorfizm (nazywa się on trywialny homomorfizm).

b) Wiemy, że element neutralny zawsze przechodzi na element neutralny, czyli $f(0) = id$. $\mathbb{Z}_3$ jest grupą cykliczną, zatem wystarczy zadać f na generatorze. Mamy $o(1) = 3$, zatem jako że $o(f(a)) \mid o(a)$ dla dowolnego $a \in G$, to $o(f(1)) = 1$ lub $o(f(1)) = 3$. Elementem o rzędzie 1 w grupie S_3 jest identyczność, natomiast elementami o rzędzie 3 są permutacje o długości 3, czyli (1 2 3) lub (1 3 2). Zatem istnieją trzy homomorfizmy $f(1) = id$ lub $f(1) = (1\ 2\ 3)$ lub $f(1) = (1\ 3\ 2)$.

c) Grupa D_4 jest izomorficzna z grupą $\mathbb{Z}_2 \times \mathbb{Z}_2$, zatem wystarczy znaleźć homomorfizmy $\mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$. Generatorem grupy $\mathbb{Z}_4$ jest $\langle 1 \rangle$, zatem jako że $o(1) = 4$, to $o(f(1)) = 1$ lub $o(f(1)) = 2$ lub $o(f(1)) = 4$. W grupie $\mathbb{Z}_2 \times \mathbb{Z}_2$ elementy mają rząd 1 lub 2. Zatem mamy cztery możliwości $f_0(1) = (0, 0)$ (homomorfizm trywialny) lub $f_1(1) = (1, 0)$ lub $f_2(1) = (0, 1)$ lub $f_3(1) = (1, 1)$. Żaden z tych homomorfizmów nie jest różnowartościowy, ponieważ $f_1(k) = (k \mod 2, 0)$, $f_2(k) = (0, k \mod 2)$ oraz $f_3(k) = (k \mod 2, k \mod 2)$.

d) Chcemy znaleźć homomorfizmy, które są różnowartościowe. Chcemy pokazać, że szukanie monomorfizmu sprowadza się do szukania elementu rzędu n w grupie G. Niech $g \in G$ oraz $o(g) = n$. Chcemy pokazać, że f takie, że $f(1) = g$ jest monomorfizmem. Załóżmy nie wprost, że dla $k \neq l$ zachodzi $f(k) = f(l)$, czyli $f(k) = f(1^k) = g^k = g^l = f(1^l) = f(l)$. Wówczas (załóżmy BSO, że $k > l$) mamy $g^{k-l} = f(k - l) = f(k) - f(l) = 1_G$. Skoro $k < n$ oraz $l < n$, to $k - l < n$, czyli mamy sprzeczność, ponieważ element g był rzędu n. Niech f będzie takie, że $f(1) = h$ oraz niech $o(h) \mid n$ i $o(h) < n$, wówczas chcemy pokazać, że f nie jest monomorfizmem. Mamy $f(o(h)) = h^{o(h)} = 1_G$, zatem jako, że $f(0) = 1_G$, to f nie jest różnowartościowe.

Definicja: Jądro homomorfizmu $f : G \to H$ to $\ker f = \{g \in G \mid f(g) = 1_H\}$.

Twierdzenie: Jądro dowolnego homomorfizmu jest podgrupą (normalną) w G.

Zadanie 7.

a) Wskaż monomorfizm z grupy izometrii kwadratu D_8 w S_4.

b) W grupie $GL(n, \mathbb{R})$ wskaż podgrupę izomorficzną z S_n.

c) Wskaż homomorfizm z grupy S_4 w $\mathbb{Z}_2$ oraz podgrupę, która jest jego jądrem.

Rozwiązanie:

a) Mamy $D_8 = \langle \sigma, \rho \mid \sigma^2 = 1, \rho^4 = 1, \sigma\rho\sigma = \rho^3 \rangle$. Mamy więc na przykład $f(\rho) = (1\ 2\ 3\ 4)$ oraz $f(\sigma) = (1\ 2)(3\ 4)$. Weźmy przekształcenie $f : D_8 \to S_4$ takie, że $f(g) = \sigma_g$ dla $g \in D_8$ i $\sigma_g \in S_4$, gdzie $\sigma_g(i) = j$ wtedy i tylko wtedy, gdy wierzchołek i przechodzi na wierzchołek j w izometrii g. Chcemy sprawdzić czy tak zadana funkcja jest monomorfizmem. Pokażemy że jest to homomorfizm. Niech $\alpha, \beta \in D_8$, wówczas $f(\alpha, \beta) = \sigma_{\alpha\beta}$. Mamy $\sigma_{\alpha\beta}(i) = j$ wtedy i tylko wtedy, gdy izometria $\alpha\beta$ przeprowadza wierzchołek i na wierzchołek j, czyli β przeprowadza wierzchołek i na wierzchołek $\beta(i)$ oraz α przeprowadza wierzchołek $\beta(i)$ na wierzchołek j. Dalej mamy $f(\alpha)f(\beta) = \sigma_\alpha\sigma_\beta$. Mamy $\sigma_\alpha \circ \sigma_\beta(i) = k$ wtedy i tylko wtedy, gdy izometria β przeprowadza wierzchołek i na wierzchołek $\beta(i)$ oraz izometria α przeprowadza wierzchołek $\beta(i)$ na wierzchołek k. Stąd $\sigma_{\alpha\beta} = \sigma_\alpha \circ \sigma_\beta$, czyli $f(\alpha\beta) = f(\alpha)f(\beta)$, czyli f jest homomorfizmem. Oczywiście jest to przekształcenie różnowartościowe, ponieważ izometria ta jest jednoznacznie wyznaczona przez obrazy wierzchołków.

b) Chcemy znaleźć monomorfizm $S_n \hookrightarrow GL(n\mathbb{R})$. Niech $\sigma \in S_n$ oraz $\varepsilon_1, \ldots, \varepsilon_n$ to baza standardowa $\mathbb{R}^n$. Niech A_σ to macierz w bazie standardowej przekształcenia liniowego f takiego, że $f(\varepsilon_1) = \varepsilon_{\sigma(1)}, \ldots, f(\varepsilon_n) = \varepsilon_{\sigma(n)}$

$$A_\sigma = \begin{bmatrix} \varepsilon_{\sigma(1)} & \varepsilon_{\sigma(2)} & \ldots & \varepsilon_{\sigma(n)} \end{bmatrix}$$

Macierz A_σ powstaje przez przepermutowanie wierszy lub kolumn z macierzy jednostkowej, zatem jest to macierz odwracalna, czyli $A_\sigma \in GL(n, \mathbb{R})$. Znaleźliśmy więc przekształcenie różnowartościowe $f : S_n \to GL(n, \mathbb{R})$, ponieważ gdyby $f(\sigma) = f(\tau)$, to $A_\sigma = A_\tau$, czyli $\begin{bmatrix} \varepsilon_{\sigma(1)} & \ldots & \varepsilon_{\sigma(n)} \end{bmatrix} = \begin{bmatrix} \varepsilon_{\tau(1)} & \ldots & \varepsilon_{\tau(n)} \end{bmatrix}$, skąd $\sigma(1) = \tau(1), \ldots, \sigma(n) = \tau(n)$. Przekształcenie to jest homomorfizmem, ponieważ

$$f(\sigma)f(\tau) = A_\sigma \cdot A_\tau = A_{\sigma\tau} = f(\sigma \circ \tau)$$

Podgrupą w $GL(n, \mathbb{R})$ będzie obraz grupy S_n w przekształceniu f.

c) Wiemy, że złożenie homomorfizmu jest homomorfizmem, zatem znajdźmy najpierw przekształcenie $f : S_4 \to GL(4, \mathbb{R})$, a następnie przekształcenie $g : GL(4, \mathbb{R}) \to C_2 = \{1, -1\} = \mathbb{Z}_2$. Przekształcenie f zadane jest w podpunkcie b). Zatem wystarczy że znajdziemy przekształcenie g. Przekształcenie g zadane będzie wzorem $g(A) = \det(A)$. Jest to homomorfizm, ponieważ $\det(AB) = \det(A) \cdot \det(B)$ oraz $\det(A) = 1$ lub $\det(A) = -1$, ponieważ macierz A powstaje przez przepermutowanie wierszy lub kolumn macierzy standardowej, czyli macierzy o wyznaczniku równym jeden. A permutowanie wierszy lub kolumn nie zmienia wartości bezwzględnej z wyznacznika. Niech więc $h = g \circ f$. Jądro homomorfizmu h to $\ker h = \{\sigma \in S_n \mid h(\sigma) = 1\}$. Są to z definicji permutacje parzyste. Oznaczamy tę grupę jako A_n.

Twierdzenie: Złożenie homomorfizmu jest homomorfizmem.

Ćwiczenia 5

Zadanie 1.
Wyznacz rzędy grup $GL(n, \mathbb{F}_q)$, gdzie $\mathbb{F}_q$ jest ciałem o q elementach. Rozpoznaj grupę $SL(2, \mathbb{F}_2)$, czyli ustal, z którą z poznanych już grup jest ona izomorficzna.

Rozwiązanie:
Niech $v_i \in \mathbb{F}_q^n$ będzie wektorem. Wówczas $\begin{bmatrix} v_1 & \dots & v_n \end{bmatrix} \in GL(n\mathbb{F}_q)$ wtedy i tylko wtedy, gdy wektory $v_1, \dots, v_n$ są liniowo niezależne. Wektor v_1 może być dowolnym wektorem niezerowym. Możemy go wybrać na $q^n - 1$ sposobów. Wektor v_2 może być dowolnym liniowo niezależnym z v_1 niezerowym wektorem. Możemy go wybrać na $q^n - q$ sposobów. Zatem n wektorów $v_1, v_2, \dots, v_n$ możemy wybrać na $|GL(n, \mathbb{F}_q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdot \ldots \cdot (q^n - q^{n-1})$ sposobów.

Mamy $SL(2, \mathbb{F}_q) = \{A \in GL(2, \mathbb{F}_2) \mid \det A = 1\}$. Jako, że $\mathbb{F}_2 = \{0, 1\}$, czyli wyznacznik dowolnej macierzy $A \in GL(2, \mathbb{F}_2)$ jest równy 1, to $SL(2, \mathbb{F}_2) = GL(2, \mathbb{F}_2)$. Grupa ta ma 6 elementów

$$SL(2, \mathbb{F}_2) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

Elementem o rzędzie 1 jest $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, elementami o rzędzie 2 są $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ oraz $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, natomiast elementami o rzędzie 3 są $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ oraz $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. Pokażemy więc, że grupa ta jest izomorficzna z grupą permutacji S_3. W przestrzeni $\mathbb{F}_2^2$ weźmy wszystkie niezerowe wektory $p_1 = (1, 0)$, $p_2 = (0, 1)$ oraz $p_3 = (1, 1)$. Weźmy dowolną macierz $A \in SL(2, \mathbb{F}_2)$. Jest to macierz izomorfizmu, czyli $A \cdot p_i = p_{\sigma_A(i)}$. Izomorfizm $f : SL(2, \mathbb{F}_2) \to S_3$ zadamy więc wzorem $f(A) = \sigma_A$, gdzie $\sigma_A(i) = j$ wtedy i tylko wtedy, gdy $A \cdot p_i = p_j$. Pokażemy, że funkcja ta jest homomorfizmem i izomorfizmem. Funkcja jest różnowartościowa, ponieważ przekształcenie jest wyznaczone jednoznacznie przez obrazy na wszystkich trzech wektorach p_1, p_2, p_3. Niech $A, B \in SL(2, \mathbb{F}_2)$ będą takie, że $f(A) = f(B)$, wówczas dla każdego i mamy $Ap_i = p_{\sigma(i)} = Bp_i$, czyli skoro p_1, p_2, p_3 rozpinają przestrzeń $\mathbb{F}_2^2$, to $A = B$. Mamy $f(AB) = \sigma_{AB}$ oraz $\sigma_{AB}(i) = j$ wtedy i tylko wtedy gdy $(AB) \cdot p_i = p_j$. Mamy $f(A) \cdot f(B) = \sigma_A \circ \sigma_B$ oraz $\sigma_A\sigma_B(i) = j$ wtedy i tylko wtedy, gdy $A(B \cdot p_i) = p_j$. Zatem jako, że $A(B \cdot p_i) = (AB)p_i$, bo mnożenie macierzy jest łączne, to $f(AB) = f(A) \cdot f(B)$. Zatem f jest homomorfizmem. Stąd f jest izomorfizmem, bo $|S_3| = |SL(2, \mathbb{F}_2)|$.

Definicja: Centrum grupy to podgrupa której elementy są przemienne ze wszystkimi innymi elementami grupy

$$Z(G) = \{a \in G \mid \forall_g \; ag = ga\}$$

Jeśli $Z(G) = G$, to grupa G jest przemienna czyli abelowa. Centrum jest podgrupą normalną w G.

Zadanie 2.
Grupa kwaternionowa oznaczana Q_8 to z definicji podgrupa $GL(2, \mathbb{C})$ generowana przez macierze

$$j = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \qquad k = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

Oznaczmy przez i iloczyn $j \cdot k$.

a) Wyznacz wszystkie elementy Q_8 za pomocą i, j, k.

b) Policz rząd każdego elementu.

c) Znajdź centrum $Z(Q_8)$.

d) Wyznacz wszystkie możliwe podgrupy Q_8.

Rozwiązanie:

a) Mamy $i = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, zatem

$$Q_8 = \{1, j, k, i, -1, -j, -k, -i\} = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle$$

ponieważ mamy $i^2 = -1$, $j^2 = -1$. $k^2 = -1$ oraz $ijk = -1$.

b) Mamy $o(i) = o(j) = o(k) = 4$, $o(1) = 1$, $o(-1) = 2$ oraz $o(-i) = o(-j) = o(-k) = 4$.

c) Grupa kwaternionowa $\mathbb{Q}_8$ składa się z ośmiu elementów

$$\mathbb{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

gdzie

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad i = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \quad j = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \quad k = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

Szukamy więc takich elementów, które są przemienne, czyli $x \in Z(\mathbb{Q}_8)$ wtedy i tylko wtedy, gdy dla każdego $y \in \mathbb{Q}_8$ zachodzi $x \cdot y = y \cdot x$. Oczywiście $1 \in Z(\mathbb{Q}_8)$ oraz $-1 \in Z(\mathbb{Q}_8)$, ponieważ mnożenie przez macierz jednostkową jest przemienne. Dalej mamy

$$i \cdot j = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \cdot \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = k \quad j \cdot i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \cdot \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = -k$$

zatem $i \notin Z(\mathbb{Q}_8)$ oraz $j \notin Z(\mathbb{Q}_8)$. Stąd również $-i \notin Z(\mathbb{Q}_8)$ oraz $-j \notin Z(\mathbb{Q}_8)$.

$$k \cdot j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} = -i \quad j \cdot k = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = i$$

Zatem również $k \notin Z(\mathbb{Q}_8)$ oraz $-k \notin Z(\mathbb{Q}_8)$. Stąd $Z(\mathbb{Q}_8) = \{1, -1\}$.

d) Wyznaczmy teraz podgrupy Q_8. Są to na przykład podgrupy cykliczne: $\langle 1 \rangle = \{1\}$, $\langle -1 \rangle = \{-1, 1\}$, $\langle i \rangle = \{1, i, -1, -i\} = \langle -i \rangle$, $\langle j \rangle = \{1, j, -1, -j\} = \langle -j \rangle$ oraz $\langle k \rangle = \{1, k, -1, -k\} = \langle -k \rangle$. Weźmy teraz dowolną podgrupę $H \leq Q_8$, wówczas z twierdzenia Lagrange'a mamy $|H| \in \{1, 2, 4, 8\}$. Jeśli rząd grupy jest równy 2 to jest to grupa cykliczna. Rozważmy więc grupy rzędu 4. Załóżmy, że H jest generowane przez dwa elementy $H = \langle \alpha, \beta \rangle$. Jeśli $H = \langle -1, x \rangle$ to $H = \langle x \rangle$, gdzie $x = \pm i$, $x = \pm j$ lub $x = \pm k$. Jeśli $H = \langle x, y \rangle$, gdzie $x \neq \pm y$ oraz $x \in \{\pm i, \pm j, \pm k\}$ oraz $y \in \{\pm i, \pm j, \pm k\}$, to $H = Q_8$. Zatem grupa H musi być generowana przez jeden element.

Zadanie 3.
Znajdź centrum grupy dihedralnej D_{2n}, czyli grupy izometrii płaszczyzny zachowujących n-kąt foremny.

Rozwiązanie:

$$D_{2n} = \{\rho^i, \sigma\rho^i \mid \sigma^2 = 1, \rho^n = 1, \sigma\rho\sigma = \rho^{n-1} = \rho^{-1}\}$$

Mamy $D_{2n} = \langle \rho, \sigma \rangle$, zatem $x \in Z(D_{2n})$ wtedy i tylko wtedy, gdy $\rho x = x\rho$ oraz $\sigma x = x\sigma$, ponieważ wówczas dla $\alpha = \sigma^{i_1}\rho^{i_2}\dots\sigma^{i_k}$ mamy

$$\alpha x = \sigma^{i_1}\rho^{i_2}\dots\sigma^{i_k}x = \sigma^{i_1}\rho^{i_2}\dots\sigma^{i_k-1}\cdot\sigma x = \sigma^{i_1}\rho^{i_2}\dots\sigma^{i_k-1}\cdot x\sigma \overset{\text{indukcja}}{=} x\sigma^{i_1}\rho^{i_2}\dots\sigma^{i_k} = x\alpha$$

Sprawdźmy, czy ρ^i należy do centrum grupy. Mamy $\rho\cdot\rho^i = \rho^i\cdot\rho$ oraz mamy

$$\sigma\cdot\rho^i\cdot\sigma = (\sigma\rho\sigma)^i = \rho^{-i} = \rho^{n-i}$$

zatem $\sigma\rho^i = \rho^i\sigma$ dla $\rho^{n-i} = \rho^i$, czyli $\rho^{2i} = \rho^n$. Dla n nieparzystego $\forall_i\ \rho^i \notin Z(D_{2n})$. Dla n parzystego $\rho^{\frac{n}{2}} \in Z(D_{2n})$. Sprawdźmy, czy $\sigma\rho^i$ należy do centrum grupy. Mamy

$$\rho\cdot\sigma\rho^i = \sigma\rho^{n-1}\cdot\rho^i = \sigma\rho^{n-1+i} = \sigma\rho^{i-1}$$

oraz $\sigma\rho^i\cdot\rho = \sigma\rho^{i+1}$, zatem $\rho\cdot\sigma\rho^i = \sigma\rho^i\cdot\rho$ gdy $\rho^{i-1} = \rho^{i+1}$, czyli $\rho^2 = 1$, zatem dla $n \geq 3$, $\sigma\rho^i$ nie może należeć do centrum dla dowolnego i. Zatem ogólnie dla n nieparzystego $Z(D_{2n}) = \{id\}$, natomiast dla n parzystego $Z(D_{2n}) = \langle\rho^{\frac{n}{2}}\rangle = \{id, \rho^{\frac{n}{2}}\}$. Dla $n = 2$ mamy $D_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$, zatem $Z(D_4) = D_4$, ponieważ $\mathbb{Z}_2 \times \mathbb{Z}_2$ jest grupą przemienną.

Definicja: Permutacje $\sigma \in S_n$ jest parzysta wtedy i tylko wtedy, gdy σ należy do jądra homomorfizmu $\phi : S_n \to \mathbb{Z}_2$, czyli $\ker\phi = \{\det A_\sigma = 1\} = A_n$.

Zadanie 4.
Pokaż, że jeśli $\sigma = (a_1, \dots, a_k)$ jest cyklem długości k, to σ jest parzysta dokładnie wtedy, gdy k jest nieparzyste. Jak zachowuje się parzystość przy składaniu cykli?

Rozwiązanie:
Wiemy, że każdy cykl jest złożeniem transpozycji

$$(a_1\ \dots\ a_k) = (a_1\ a_k)\dots(a_1\ a_3)(a_1\ a_2)$$

Macierz transpozycji $(a_1\ a_2)$, to $A_{(a_1\ a_2)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, bo macierz ta powstaje z I przez zamianę dwóch kolumn. Stąd $\det A_{(a_1\ a_2)} = -1$, czyli transpozycja $(a_1\ a_2)$ jest nieparzysta. Niech teraz $\sigma, \tau \in S_n$, wówczas $\det A_{\sigma\tau} = \det A_\sigma \cdot \det A_\tau$, zatem złożenie dwóch permutacji parzystych jest parzyste, złożenie dwóch permutacji nieparzystych jest parzyste, natomiast złożenie permutacji parzystej i permutacji nieparzystej (lub nieparzystej i parzystej) jest nieparzyste. Zatem cykl długości k jest parzysty, wtedy i tylko wtedy, gdy k jest nieparzyste.

Zadanie 5.
Określ parzystość permutacji $\sigma \in S_8$, gdzie $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 5 & 1 & 4 & 2 & 6 & 8 \end{pmatrix}$

Rozwiązanie:
Rozłóżmy permutację na cykle rozłączne

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 5 & 1 & 4 & 2 & 6 & 8 \end{pmatrix} = (1\ 3\ 5\ 4)(2\ 7\ 6)(8)$$

Ta permutacja jest nieparzysta, ponieważ pierwszy cykl jest nieparzysty, natomiast dwa kolejne są parzyste.

Zadanie 6.
Niech G będzie grupą skończoną i $A, B < G$. Uzasadnij, że $|AB| = \frac{|A||B|}{|A \cap B|}$.

Rozwiązanie:
Mamy

$$AB = \{ab \mid a \in A, b \in B\}$$

Rozważmy element ab taki, że $a \in A$ oraz $b \in B$. Chcemy zobaczyć kiedy $ab = a'b'$, gdzie $a' \in A$ oraz $b' \in B$, bo wówczas element ab powstanie nam na kilka sposobów, a chcemy zliczyć go raz. Mamy

$$ab = a'b' \Leftrightarrow b \cdot b'^{-1} = a^{-1} \cdot a'$$

gdzie $b \cdot b'^{-1} \in B$ oraz $a^{-1} \cdot a' \in A$, czyli $b \cdot b'^{-1} = a^{-1} \cdot a' \in A \cap B$. Niech $a^{-1} \cdot a' = h$, wówczas $b = hb'$ oraz $a = a'h^{-1}$. Zatem mamy

$$a'b' = ab = (a'h^{-1}) \cdot (hb') \quad \text{dla każdego } h \in A \cap B$$

czyli każdy element $a'b'$ można przedstawić jako $a''b''$, gdzie $a'' \in A$ oraz $b'' \in B$, na co najwyżej $|A \cap B|$ sposobów. Chcemy teraz pokazać, że dla różnych $g, h \in A \cap B$ zachodzi związek $(a'h^{-1})(hb') \neq (a'g^{-1})(gb')$. Załóżmy przeciwnie, że $(a'h^{-1})(hb') = a'b' = (a'g^{-1})(gb')$, wówczas po przekształceniach mamy $h = g$, co jest sprzeczne z założeniem. Zatem każdy element $a'b'$ możemy przedstawić jako $a''b''$ na co najmniej $|A \cap B|$ sposobów. Stąd $|AB| = \frac{|A||B|}{|A \cap B|}$.

Definicja: Niech H będzie podgrupą w grupie G. Wówczas $Ha = \{ha \mid h \in H\}$ nazywamy warstwą prawostronną względem podgrupy H wyznaczoną przez element a.

Indeks podgrupy $[G : H]$ to liczba warstw w grupie G względem podgrupy H.

Przykłady:

1. Weźmy podgrupę $H = \langle \rho \rangle = \{id, \rho, \rho^2\}$ grupy D_6. Chcemy zobaczyć jak wyglądają warstwy w D_6 względem H. Z twierdzenia Lagrange'a wiemy, że warstw będzie $[G : H] = \frac{|G|}{|H|} = 2$. Jedna z nich to $H_e = \{id, \rho, \rho^2\}$, natomiast drugą będzie $H_\sigma = \{\sigma, \rho\sigma = \sigma\rho^2, \rho^2\sigma = \sigma\rho\}$.

2. Rozpatrzmy grupę macierzy odwracalnych $GL(n, \mathbb{R})$ i jej podgrupę macierzy o wyznaczniku równym jeden $SL(n, \mathbb{R})$. Chcemy opisać warstwy względem tej podgrupy. Wiemy, że $aH = bH$ wtedy i tylko wtedy, gdy $a^{-1}b \in H$ (lub równoważnie $b^{-1}a \in H$), zatem

   $$aSL(n, \mathbb{R}) = bSL(n, \mathbb{R}) \Leftrightarrow a^{-1}b \in SL(n, \mathbb{R}) \Leftrightarrow \det(a^{-1}b) = 1 \Leftrightarrow \det(a) = \det(b)$$

   Zatem każda warstwa to $H_\lambda = \{a \in GL(n, \mathbb{R}) \mid \det a = \lambda\}$ dla dowolnego $\lambda \in \mathbb{R} \setminus \{0\}$

Ćwiczenia 6

Zadanie 1.
Niech $F \leq H \leq G$ oraz $|G| < \infty$. Udowodnij, że wówczas

$$[G : F] = [G : H][H : F]$$

Rozwiązanie:
Z twierdzenia Lagrange'a mamy $[G : F] = \frac{|G|}{|F|}$, $[G : H] = \frac{|G|}{|H|}$ oraz $[H : F] = \frac{|H|}{|F|}$, skąd

$$[G : F] = \frac{|G|}{|F|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|F|} = [G : H][H : F]$$

Zadanie 2.
Niech H_1, H_2 będą podgrupami w G. Pokaż, że wówczas

$$[G : H_1 \cap H_2] \leq [G : H_1][G : H_2]$$

Rozwiązanie:
Mamy $H_1 \cap H_2 \leq H_1 \leq G$, czyli

$$[G : H_1 \cap H_2] = [G : H_1][H_1 : H_1 \cap H_2]$$

zatem wystarczy pokazać, że

$$[H_1 : H_1 \cap H_2] \leq [G : H_2]$$

Wystarczy, że znajdziemy funkcję f ze zbioru warstw $H_1 \cap H_2$ w H_1 w zbiór warstw H_2 w G, która jest różnowartościowa. Niech $h \in H_1$ oraz niech $f(h(H_1 \cap H_2)) = hH_2$. Chcemy pokazać, że f jest dobrze określone oraz że jest różnowartościowe. Weźmy $h, h' \in H_1$, takie że $h(H_1 \cap H_2) = h'(H_1 \cap H_2)$, wówczas $h^{-1}h' \in H_1 \cap H_2$. Stąd $h^{-1}h' \in H_2$, czyli $hH_2 = h'H_2$. Zatem funkcja jest dobrze określona. Niech $h, h' \in H_1$ będą takie, że $hH_2 = h'H_2$. Chcemy pokazać, że $h(H_1 \cap H_2) = h'(H_1 \cap H_2)$. Skoro $hH_2 = h'H_2$, to $h^{-1}h' \in H_2$. Skoro $h, h' \in H_1$ oraz H_1 jest podgrupą G, to $h^{-1}h' \in H_1$. Zatem mamy $h^{-1}h' \in H_1 \cap H_2$, czyli $h(H_1 \cap H_2) = h'(H_1 \cap H_2)$, czyli f jest różnowartościowe.

Definicja: Zbiór $\mathrm{Aut}(G)$ składający się z izomorfizmów $G \to G$ z działaniem składania tworzy grupę, zwaną grupą automorfizmów grupy G.

Zadanie 3.
Znaleźć grupę automorfizmów grupy

a) $\mathbb{Z}_6$

b) $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą

c) S_3

Rozwiązanie:

a) Chcemy zobaczyć jak wyglądają wszystkie izomorfizmy $f : \mathbb{Z}_6 \to \mathbb{Z}_6$. Chcemy zadać izomorfizm, czyli w szczególności monomorfizm, zatem $f(1) = a$, gdzie $o(a) = 6$. Elementami w $\mathbb{Z}_6$ rzędu 6 są 1 i 5, zatem $f(1) = \{1, 5\}$. Jeśli $f_1(1) = 1$, to $f_1(k) = k$. Jeśli $f_2(1) = 5$, to $f_2(k) = 5k = -k$. Funkcje f_1, f_2 są na, ponieważ moce zbiorów $\mathbb{Z}_6$ są równe. Stąd mamy $\mathrm{Aut}(\mathbb{Z}_6) = \{id, -id\} \simeq \mathbb{Z}_2$.

b) Niech $f : \mathbb{Z}_p \to \mathbb{Z}_p$. Mamy $f(1) = a \in \mathbb{Z}_p$ takie, że $o(a) = p$. Skoro p jest liczbą pierwszą, to $a \in \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. Wówczas $f(k) = a \cdot k$, skąd $|\mathrm{Aut}(\mathbb{Z}_p)| = p - 1$. Niech $f : \mathbb{Z}_p^* \to \mathrm{Aut}(\mathbb{Z}_p)$ będzie takie, że $f(a) = f_a$, gdzie $f_a(k) = a \cdot k$ oraz $f_a \in \mathrm{Aut}(\mathbb{Z}_p)$. Funkcja ta jest różnowartościowa, ponieważ jeśli $f_a = f_b$, to $a = b$, bo $a = f_a(1) = f_b(1) = b$. Grupy $\mathbb{Z}_p^*$ oraz $\mathrm{Aut}(\mathbb{Z}_p)$ mają te same moce, zatem funkcja f jest „na". Chcemy teraz pokazać, że f jest homomorfizmem, czyli że $f(ab) = f(a) \circ f(b) \Leftrightarrow f_{ab} = f_a \circ f_b$. Mamy $f_{ab}(k) = abk$ oraz $f_a \circ f_b(k) = f_a(bk) = a(bk) = abk$. Zatem f jest homomorfizmem. Stąd f jest izomorfizmem, czyli $\mathrm{Aut}(\mathbb{Z}_p) \simeq \mathbb{Z}_p^*$.

Dla dowolnego $n \in \mathbb{Z}$ mamy $|\mathrm{Aut}(\mathbb{Z}_n)| = \phi(n)$, gdzie ϕ to funkcje Eulera. Mamy $\mathrm{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \exists_{b \in \mathbb{Z}_n}\ ab = 1\}$.

c) Szukamy wszystkich izomorfizmów $f : S_3 \to S_3$. Wiemy, że dla każdego $g \in G$ funkcja $f_g(x) = gxg^{-1}$ jest automorfizmem, gdzie $f_g : G \to G$ (są to automorfizmy wewnętrzne). Jest to automorfizm, ponieważ jest to homomorfizm i izomorfizm. Jest to izomorfizm, ponieważ $f_{g^{-1}} \circ f_g = id = f_g \circ f_{g^{-1}}$. Niech $h : S_3 \to \mathrm{Aut}(S_3)$ zadane będzie wzorem $h(g) = f_g$. Wówczas h jest homomorfizmem, który dla dowolnego elementu $g \in S_3$ przyporządkowuje jakiś automorfizm f_g grupy S_3, gdzie $f_g(x) = gxg^{-1}$. Chcemy teraz zobaczyć jakie jest jądro tej funkcji $\ker h$. Mamy

$$\ker h = \{g \in S_3 \mid f_g = id\} = \{g \in S_3 \mid \forall_{x \in S_3}\ gx = xg\} = Z(S_3)$$

Wiemy, że $h : S_3 \to \mathrm{Aut}(S_3)$ jest różnowartościowe, ponieważ $\ker h = Z(S_3) = \{id\}$. Stąd mamy $|\mathrm{Aut}(S_3)| \geq 6$. Chcemy pokazać, że $|\mathrm{Aut}(S_3)| \leq 6$. Mamy

$$S_3 = D_6 = \{\sigma, \rho \mid \sigma\rho\sigma = \rho^2, \rho^3 = id, \sigma^2 = 1\}$$

zatem dowolny automorfizm $f : S_3 \to S_3$ zadany będzie na generatorach. Wówczas skoro f to automorfizm, to $o(f(\sigma)) = o(\sigma) = 2$ oraz $o(f(\rho)) = o(\rho) = 3$. Zatem $f(\sigma) \in \{\sigma, \sigma\rho, \sigma\rho^2\}$ oraz $f(\rho) = \{\rho, \rho^2\}$. Stąd $|\mathrm{Aut}(S_3)| \leq 3 \cdot 2 = 6$, bo $f(\sigma)$ możemy wybrać na 3 sposoby oraz $f(\rho)$ możemy wybrać na 2 sposoby. Zatem $|\mathrm{Aut}(S_3)| = 6$. Teraz skoro $|\mathrm{Aut}(S_3)| = 6$ oraz $f : S_3 \hookrightarrow \mathrm{Aut}(S_3)$, to f jest izomorfizmem, zatem $\mathrm{Aut}(S_3) \simeq S_3$.

Definicja: Mówimy, że podgrupa N grupy G jest normalna, gdy dla dowolnego $x \in G$ zachodzi $xNx^{-1} \subseteq N$. Równoważnie, gdy $xN = Nx$. Piszemy $N \triangleleft G$.

Zadanie 4.
Wyznacz wszystkie podgrupy oraz podgrupy normalne w grupie izometrii kwadratu D_8.

Rozwiązanie:
Grupa izometrii kwadratu to

$$D_8 = \{\sigma, \rho \mid \sigma^2 = 1, \rho^4 = 1 \text{ oraz } \sigma\rho\sigma = \rho^3\}$$

Wyznaczmy najpierw wszystkie podgrupy. Z twierdzenia Lagrange'a wiemy, że rząd podgrupy dzieli rząd grupy, zatem jako, że D_8 jest skończona (bo ma osiem elementów) oraz rząd D_8 jest równy 8, to jej podgrupy mogą mieć rzędy $1, 2, 4$ lub 8. Jedyną grupą rzędu 1 jest $\{id\}$, natomiast jedyną grupą rzędu 8 jest D_8.

$$D_8 = \{id, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$$

Znajdźmy najpierw podgrupy cykliczne, czyli generowane przez jeden element. Są to $\langle\rho\rangle = \langle\rho^3\rangle$, $\langle\rho^2\rangle$, $\langle\sigma\rangle$ - symetria względem boku AB, $\langle\sigma\rho\rangle$ - symetria względem przekątnej BD, $\langle\sigma\rho^2\rangle$ - symetria względem boku AD, $\langle\sigma\rho^3\rangle$ - symetria względem przekątnej AC. Podgrupy rzędu 2 muszą być cykliczne, zatem są to $\langle\rho^2\rangle, \langle\sigma\rangle, \langle\sigma\rho\rangle, \langle\sigma\rho^2\rangle, \langle\sigma\rho^3\rangle$. Pozostają nam więc do rozpatrzenia podgrupy rzędu 4. Rząd każdego elementu może być równy $1, 2$ lub 4. Jeśli w grupie istnieje element rzędu 4, to grupa ta jest izomorficzna z grupą $\mathbb{Z}_4$, czyli podgrupa ta to $\langle\rho\rangle$. Załóżmy więc, że w podgrupie nie ma elementu rzędu 4. Wówczas każdy jej element ma rząd 2 lub 1. Jedynym elementem o rzędzie 1 jest identyczność. Elementów o rzędzie 2 mamy pięć. Są to $\sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3$ oraz ρ^2. Skonstuujmy więc podgrupy rzędu 4. Są one generowane przez dwa elementy (ponieważ grupa D_8 jest generowana przez dwa elementy). Wiemy, że podzbiór $H \subseteq G$ jest podgrupą G, gdy:

1. $a, b \in H \Rightarrow a \cdot b \in H$
2. $a \in H \Rightarrow a^{-1} \in H$

Niech $\rho^2 \in H$ oraz $\sigma \in H$, wówczas $\sigma\rho^2 \in H$, zatem mamy podgrupę $\langle\sigma, \rho^2\rangle = \{id, \rho^2, \sigma, \sigma\rho^2\}$, bo $\sigma\rho^2\sigma = \rho^2$, $\rho^2\sigma = \sigma\rho^2$, $\rho^2\sigma\rho^2 = \sigma$. Niech $\rho^2 \in H$ oraz $\sigma\rho \in H$, wówczas $\sigma\rho^3 \in H$, zatem mamy podgrupę $\langle\sigma\rho, \rho^2\rangle = \{id, \rho^2, \sigma\rho, \sigma\rho^3\}$, bo $\rho^2\sigma\rho = \sigma\rho^3$, $\rho^2\sigma\rho^3 = \sigma\rho$, $\sigma\rho\sigma\rho^3 = \rho^2$, $\sigma\rho^3\sigma\rho = \rho^2$. Niech $\sigma \in H$ oraz $\sigma\rho \in H$, wówczas $\rho \in H$, zatem nie istnieje podgrupa rzędu cztery generowana przez elementy σ i $\sigma\rho$. Niech $\sigma \in H$ oraz $\sigma\rho^3 \in H$, wówczas $\rho^3 \in H$, zatem nie istnieje podgrupa rzędu cztery generowana przez elementy σ i $\sigma\rho^3$. Niech $\sigma\rho \in H$ oraz $\sigma\rho^2 \in H$, wówczas $\rho \in H$, zatem nie istnieje podgrupa rzędu cztery generowana przez elementy $\sigma\rho$ i $\sigma\rho^2$. Niech $\sigma\rho^2 \in H$ oraz $\sigma\rho^3 \in H$, wówczas $\rho \in H$, zatem nie istnieje podgrupa rzędu cztery generowana przez elementy $\sigma\rho^2$ i $\sigma\rho^3$. Rozważyliśmy wszystkie możliwe przypadki, ponieważ dwa elementy z pięciu mogliśmy wybrać na $\binom{5}{2} = 10$ sposobów. Zatem wszystkie możliwe podgrupy to

$$\{id\}, \langle\rho\rangle, \langle\rho^2\rangle, \langle\sigma\rangle, \langle\sigma\rho\rangle, \langle\sigma\rho^2\rangle, \langle\sigma\rho^3\rangle, \langle\sigma, \rho^2\rangle, \langle\rho^2, \sigma\rho\rangle, D_8$$

Znajdźmy teraz podgrupy normalne w grupie izometrii kwadratu. Podgrupa N grupy G będzie normalna, gdy wszystkie jej warstwy prawostronne będą równe odpowiadającym im warstwą lewostronnym, czyli

$$gN = Ng \Leftrightarrow \{gn \mid n \in N\} = \{ng \mid n \in N\}$$

dla każdego $g \in G$. Podgrupy $\{id\}$ oraz D_8 są normalne, to oczywiste. Sprawdźmy, czy każda z podgrup jest normalna. Sprawdźmy, czy $\langle\rho\rangle = \{id, \rho, \rho^2, \rho^3\}$ jest podgrupą normalną. Oczywiście dla $g \in \{id, \rho, \rho^2, \rho^3\}$ warunki są spełnione. Dalej mamy

$$\sigma\langle\rho\rangle = \{\sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\} \text{ oraz } \langle\rho\rangle\sigma = \{\sigma, \rho\sigma = \sigma\rho^3, \rho^2\sigma = \sigma\rho^2, \rho^3\sigma = \sigma\rho\}$$
$$\sigma\rho\langle\rho\rangle = \{\sigma\rho, \sigma\rho^2, \sigma\rho^3, \sigma\} \text{ oraz } \langle\rho\rangle\sigma\rho = \{\sigma\rho, \rho\sigma\rho = \sigma, \rho^2\sigma\rho = \sigma\rho^3, \rho^3\sigma\rho = \sigma\rho^2\}$$
$$\sigma\rho^2\langle\rho\rangle = \{\sigma\rho^2, \sigma\rho^3, \sigma, \sigma\rho\} \text{ oraz } \langle\rho\rangle\sigma\rho^2 = \{\sigma\rho^2, \rho\sigma\rho^2 = \sigma\rho, \rho^2\sigma\rho^2 = \sigma, \rho^3\sigma\rho^2 = \sigma\rho^3\}$$
$$\sigma\rho^3\langle\rho\rangle = \{\sigma\rho^3, \sigma, \sigma\rho, \sigma\rho^2\} \text{ oraz } \langle\rho\rangle\sigma\rho^2 = \{\sigma\rho^3, \rho\sigma\rho^3 = \sigma\rho^2, \rho^2\sigma\rho^3 = \sigma\rho, \rho^3\sigma\rho^3 = \sigma\}$$

Zatem grupa $\langle\rho\rangle$ jest normalna. Sprawdźmy czy $\langle\rho^2\rangle = \{id, \rho^2\}$ jest podgrupą normalną. Oczywiście dla $g \in \{id, \rho, \rho^2, \rho^3\}$ warunki są spełnione. Dalej mamy

$$\sigma\langle\rho^2\rangle = \{\sigma, \sigma\rho^2\} \text{ oraz } \langle\rho^2\rangle\sigma = \{\sigma, \rho^2\sigma = \sigma\rho^2\}$$
$$\sigma\rho\langle\rho^2\rangle = \{\sigma\rho, \sigma\rho^3\} \text{ oraz } \langle\rho^2\rangle\sigma\rho = \{\sigma\rho, \rho^2\sigma\rho = \sigma\rho^3\}$$
$$\sigma\rho^2\langle\rho^2\rangle = \{\sigma\rho^2, \sigma\} \text{ oraz } \langle\rho^2\rangle\sigma\rho^2 = \{\sigma\rho^2, \rho^2\sigma\rho^2 = \sigma\}$$
$$\sigma\rho^3\langle\rho^2\rangle = \{\sigma\rho^3, \sigma\rho\} \text{ oraz } \langle\rho^2\rangle\sigma\rho^3 = \{\sigma\rho^3, \rho^2\sigma\rho^3 = \sigma\rho\}$$

Zatem grupa $\langle\rho^2\rangle$ jest normalna. Sprawdźmy czy $\langle\sigma\rangle = \{id, \sigma\}$ jest podgrupą normalną. Mamy

$$\rho\langle\sigma\rangle = \{\rho, \rho\sigma = \sigma\rho^3\} \text{ oraz } \langle\sigma\rangle\rho = \{\rho, \sigma\rho\}$$

Zatem podgrupa $\langle\sigma\rangle$ nie jest normalna. Sprawdźmy czy $\langle\sigma\rho\rangle = \{id, \sigma\rho\}$ jest podgrupą normalną. Mamy

$$\rho\langle\sigma\rho\rangle = \{\rho, \rho\sigma\rho = \sigma\} \text{ oraz } \langle\sigma\rho\rangle\rho = \{\rho, \sigma\rho^2\}$$

Zatem podgrupa $\langle\sigma\rho\rangle$ nie jest normalna. Sprawdźmy czy $\langle\sigma\rho^2\rangle = \{id, \sigma\rho^2\}$ jest podgrupą normalną. Mamy

$$\rho\langle\sigma\rho^2\rangle = \{\rho, \rho\sigma\rho^2 = \sigma\rho\} \text{ oraz } \langle\sigma\rho^2\rangle\rho = \{\rho, \sigma\rho^3\}$$

Zatem podgrupa $\langle\sigma\rho^2\rangle$ nie jest normalna. Sprawdźmy czy $\langle\sigma\rho^3\rangle = \{id, \sigma\rho^3\}$ jest podgrupą normalną. Mamy

$$\rho\langle\sigma\rho^3\rangle = \{\rho, \rho\sigma\rho^3 = \sigma\rho^2\} \text{ oraz } \langle\sigma\rho^3\rangle\rho = \{\rho, \sigma\}$$

Zatem podgrupa $\langle\sigma\rho^3\rangle$ nie jest normalna. Sprawdźmy czy $\langle\rho^2, \sigma\rangle = \{id, \rho^2, \sigma\rho^2, \sigma\}$ jest podgrupą normalną. Mamy

$$\rho\langle\rho^2, \sigma\rangle = \{\rho, \rho^3, \rho\sigma\rho^2 = \sigma\rho, \rho\sigma = \sigma\rho^3\} \text{ oraz } \langle\rho^2, \sigma\rangle\rho = \{\rho, \rho^3, \sigma\rho^3, \sigma\rho\}$$
$$\rho^2\langle\rho^2, \sigma\rangle = \{\rho^2, id, \rho^2\sigma\rho^2 = \sigma, \rho^2\sigma = \sigma\rho^2\} \text{ oraz } \langle\rho^2, \sigma\rangle\rho^2 = \{\rho^2, id, \sigma, \sigma\rho^2\}$$
$$\rho^3\langle\rho^2, \sigma\rangle = \{\rho^3, \rho, \rho^3\sigma\rho^2 = \sigma\rho^3, \rho^3\sigma = \sigma\rho\} \text{ oraz } \langle\rho^2, \sigma\rangle\rho^3 = \{\rho^3, \rho, \sigma\rho, \sigma\rho^3\}$$
$$\sigma\langle\rho^2, \sigma\rangle = \{\sigma, \sigma\rho^2, \rho^2, id\} \text{ oraz } \langle\rho^2, \sigma\rangle\sigma = \{\sigma, \sigma\rho^2, \sigma\rho^2\sigma = \rho^2, id\}$$
$$\sigma\rho\langle\rho^2, \sigma\rangle = \{\sigma\rho, \sigma\rho^3, \sigma\rho\sigma\rho^2 = \rho, \sigma\rho\sigma = \rho^3\} \text{ oraz } \langle\rho^2, \sigma\rangle\sigma\rho = \{\sigma\rho, \rho^2\sigma\rho = \sigma\rho^3, \sigma\rho^2\sigma\rho = \rho^3, \rho\}$$
$$\sigma\rho^2\langle\rho^2, \sigma\rangle = \{\sigma\rho^2, \sigma, \sigma\rho^2\sigma\rho^2 = id, \sigma\rho^2\sigma = \rho^2\} \text{ oraz } \langle\rho^2, \sigma\rangle\sigma\rho^2 = \{\sigma\rho^2, \rho^2\sigma\rho^2 = \sigma, \sigma\rho^2\sigma\rho^2 = id, \rho^2\}$$
$$\sigma\rho^3\langle\rho^2, \sigma\rangle = \{\sigma\rho^3, \sigma\rho, \sigma\rho^3\sigma\rho^2 = \rho^3, \sigma\rho^3\sigma = \rho\} \text{ oraz } \langle\rho^2, \sigma\rangle\sigma\rho^3 = \{\sigma\rho^3, \rho^2\sigma\rho^3 = \sigma\rho, \sigma\rho^2\sigma\rho^3 = \rho, \rho^3\}$$

Zatem grupa $\langle \rho^2, \sigma \rangle$ jest normalna. Sprawdźmy czy $\langle \rho^2, \sigma\rho \rangle = \{id, \rho^2, \sigma\rho, \sigma\rho^3\}$ jest podgrupą normalną. Mamy

$$\rho\langle \rho^2, \sigma\rho \rangle = \{\rho, \rho^3, \rho\sigma\rho = \sigma, \sigma\rho^2\} \text{ oraz } \langle \rho^2, \sigma\rho \rangle\rho = \{\rho, \rho^3, \sigma\rho^2, \sigma\}$$
$$\rho^2\langle \rho^2, \sigma\rho \rangle = \{\rho^2, id, \rho^2\sigma\rho = \sigma\rho^3, \rho^2\sigma\rho^3 = \sigma\rho\} \text{ oraz } \langle \rho^2, \sigma\rho \rangle\rho^2 = \{\rho^2, id, \sigma\rho^3, \sigma\rho\}$$
$$\rho^3\langle \rho^2, \sigma\rho \rangle = \{\rho^3, \rho, \rho^3\sigma\rho = \sigma\rho^2, \sigma\} \text{ oraz } \langle \rho^2, \sigma\rho \rangle\rho^3 = \{\rho^3, \rho, \sigma, \sigma\rho^2\}$$
$$\sigma\langle \rho^2, \sigma\rho \rangle = \{\sigma, \sigma\rho^2, \rho, \rho^3\} \text{ oraz } \langle \rho^2, \sigma\rho \rangle\sigma = \{\sigma, \rho^2\sigma = \sigma\rho^2, \sigma\rho\sigma = \rho^3, \sigma\rho^3\sigma = \rho\}$$
$$\sigma\rho\langle \rho^2, \sigma\rho \rangle = \{\sigma\rho, \sigma\rho^3, \sigma\rho\sigma\rho = id, \sigma\rho\sigma\rho^3 = \rho^2\}$$

oraz

$$\langle \rho^2, \sigma\rho \rangle\sigma\rho = \{\sigma\rho, \rho^2\sigma\rho = \sigma\rho^3, \sigma\rho\sigma\rho = id, \sigma\rho^3\sigma\rho = \rho^2\}$$
$$\sigma\rho^2\langle \rho^2, \sigma\rho \rangle = \{\sigma\rho^2, \sigma, \sigma\rho^2\sigma\rho = \rho^3, \sigma\rho^2\sigma\rho^3 = \rho\}$$

oraz

$$\langle \rho^2, \sigma\rho \rangle\sigma\rho^2 = \{\sigma\rho^2, \rho^2\sigma\rho^2 = \sigma, \sigma\rho\sigma\rho^2 = \rho, \sigma\rho^3\sigma\rho^2 = \rho^3\}$$
$$\sigma\rho^3\langle \rho^2, \sigma\rho \rangle = \{\sigma\rho^3, \sigma\rho, \sigma\rho^3\sigma\rho = \rho^2, \sigma\rho^3\sigma\rho^3 = id\}$$

oraz

$$\langle \rho^2, \sigma\rho \rangle\sigma\rho^3 = \{\sigma\rho^3, \rho^2\sigma\rho^3 = \sigma\rho, \sigma\rho\sigma\rho^3 = \rho^2, \sigma\rho^3\sigma\rho^3 = id\}$$

Zatem grupa $\langle \rho^2, \sigma\rho \rangle$ jest normalna. Zatem podgrupy normalne w grupie izometrii D_8 to

$$\{id\}, D_8, \langle \rho \rangle, \langle \rho^2 \rangle, \langle \rho^2, \sigma \rangle, \langle \rho^2, \sigma\rho \rangle$$

Zadanie 5.
Pokaż, że jeśli $H \leq G$ jest taka, że $[G : H] = 2$, to $H \triangleleft G$.

Rozwiązanie:
Indeks $[G : H]$ jest równy 2 oznacza, że grupa G jest sumą rozłączną dwóch warstw, czyli że $G = He \cup Ha$ lub $G = aH \cup eH$, gdzie $a \notin H$. Chcemy pokazać, że $Hb = bH$ dla dowolnego $b \in G$. Jeśli $b \in H$, to $Hb = H = bH$. Jeśli $b \notin H$, to $Hb \neq H$, czyli $G = H \cup Hb$ oraz $bH \neq H$, czyli $G = bH \cup H$. Stąd mamy $H \cup Hb = bH \cup H$. Skoro mamy tu sumy rozłączne, to $Hb = G \setminus H = bH$, czyli $H \triangleleft G$.

Zadanie 6.
Znaleźć wszystkie podgrupy oraz podgrupy normalne w grupie

a) $\mathbb{Z}_2 \times \mathbb{Z}_4$

b) D_6

c) $\mathbb{Q}_8$

Rozwiązanie:

a) Grupa $\mathbb{Z}_2 \times \mathbb{Z}_4$ jest abelowa, zatem dla dowolnej podgrupy $H \leq \mathbb{Z}_2 \times \mathbb{Z}_4$, podgrupa H jest normalna. Wyznaczmy więc wszystkie podgrupy w $\mathbb{Z}_2 \times \mathbb{Z}_4$. Wiemy, że jeśli $H_1 < G$ i $H_2 < H$, to $H_1 \times H_2 < G \times H$. Podgrupy w $\mathbb{Z}_2$ to $\{0\}$ i $\mathbb{Z}_2$, natomiast podgrupy w $\mathbb{Z}_4$ to $\{0\}$, $\langle 2\rangle$ i $\mathbb{Z}_4$, zatem podgrupy w $\mathbb{Z}_2 \times \mathbb{Z}_4$ to m.in. $\{(0,0)\}$, $\langle(0,2)\rangle$, $\langle(0,1)\rangle = 0 \times \mathbb{Z}_4$, $\langle(1,0)\rangle = \mathbb{Z}_2 \times 0$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ oraz $\langle(1,2)\rangle = \mathbb{Z}_2 \times \langle 2\rangle$. Są to wszystkie podgrupy cykliczne. Wiemy, że jeśli $H < \mathbb{Z}_2 \times \mathbb{Z}_4$, to $|H| \in \{1,2,4,8\}$, ponieważ grupa $\mathbb{Z}_2 \times \mathbb{Z}_4$ ma osiem elementów. Podgrupa rzędu jeden to element neutralny, podgrupa rzędu osiem to cała grupa, natomiast podgrupy rzędu dwa to podgrupy cykliczne. Pozostają nam więc do rozpatrzenia podgrupy rzędu cztery niecykliczne, czyli generowane przez co najmniej dwa elementy. Elementy te muszą być rzędu dwa, bo w przeciwnym przypadku rząd tej grupy byłby większy niż cztery. Elementami rzędu dwa w $\mathbb{Z}_2 \times \mathbb{Z}_4$ są $(0,2)$, $(1,2)$ i $(1,0)$, zatem rozpatrzmy na przykład grupę

$$\langle(0,2),(1,0)\rangle = \{(0,0),(0,2),(1,0),(1,2)\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

Widać, że każde dwa inne elementy rzędu dwa generują tę samą podgrupę. Stąd wszystkimi możliwymi podgrupami są

$$\{(0,0)\}, \langle(0,2)\rangle, \langle(0,1)\rangle, \langle(1,0)\rangle, \langle(1,2)\rangle, \langle(0,2),(1,0)\rangle, \mathbb{Z}_2 \times \mathbb{Z}_4$$

b) Podgrupami grupy D_6 są

$$\langle\sigma\rangle = \{1,\sigma\}, \langle\sigma\rho^i\rangle = \{1,\sigma\rho^i\}, \langle\rho\rangle = \{1,\rho,\rho^2\}, \{id\}, D_6$$

Mamy $|D_6| = 6$, zatem jeśli $H \leq D_6$, to $|H| = \{1,2,3,6\}$. Wiemy, że jeśli $|H| \in \{2,3\}$, to H jest cykliczna czyli generowana przez jeden element. Zatem nie istnieją inne podgrupy D_6. Podgrupami normalnymi będą na pewno $\{id\}$, D_6 oraz $\langle\rho\rangle$, ponieważ jej indeks jest równy 2. Sprawdźmy teraz, czy $\langle\sigma\rho^i\rangle$ jest normalna w D_6. Dla $i = 0$ mamy

$$\rho\langle\sigma\rangle = \{\rho, \rho\sigma = \sigma\rho^2\} \quad \text{oraz} \quad \langle\sigma\rangle\rho = \{\rho, \sigma\rho\}$$

zatem nie jest to podgrupa normalna. Dla $i = 1$ mamy

$$\rho\langle\sigma\rho\rangle = \{\rho, \rho\sigma\rho = \sigma\} \quad \text{oraz} \quad \langle\sigma\rho\rangle\rho = \{\rho, \sigma\rho^2\}$$

zatem nie jest to podgrupa normalna. Analogicznie $\langle\sigma\rho^2\rangle$ nie jest podgrupą normalną w D_6.

c) Na pewno grupami normalnymi będą $\{1\}$ oraz $\mathbb{Q}_8$. Podgrupami grupy $\mathbb{Q}_8$ są

$$\{1\}, \{1,-1\}, \langle i\rangle = \{i,-i,1,-1\}, \langle j\rangle = \{j,-j,1,-1\}, \langle k\rangle = \{k,-k,1,-1\}, \mathbb{Q}_8$$

Wiemy, że podgrupa jest normalna, jeśli jej indeks w grupie $\mathbb{Q}_8$ jest równy 2. Podgrupy $\langle i\rangle, \langle j\rangle, \langle k\rangle$ mają po 4 elementy, zatem indeks tych grup jest równy 2. Stąd grupy $\langle i\rangle, \langle j\rangle, \langle k\rangle$ będą normalne. Pozostaje zobaczyć, czy $\{1,-1\}$ jest podgrupą normalną. Zachodzi równość $(-1)\cdot x = -x = x\cdot(-1)$, zatem oczywiście podgrupa $\langle 1\rangle = \{1,-1\}$ jest normalna.

Zadanie 7.
Czy grupy $\mathrm{Aut}(\mathbb{Z}_8)$ oraz $\mathrm{Aut}(\mathbb{Z}_{10})$ są izomorficzne? Wskaż, o ile istnieją, dwie właściwe podgrupy F, H w grupie $\mathrm{Aut}(\mathbb{Z}_8)$ takie, że $\mathrm{Aut}(\mathbb{Z}_8) = F \times H$.

Rozwiązanie:
Elementami rzędu 8 w grupie $\mathbb{Z}_8$ są $1, 3, 5, 7$, zatem $\mathrm{Aut}(\mathbb{Z}_8)$ ma 4 elementy $\phi_1(1) = 1$, $\phi_2(1) = 3$, $\phi_3(1) = 5$ oraz $\phi_4(1) = 7$, przy czym $o(\phi_1) = 1$ oraz $o(\phi_2) = o(\phi_3) = o(\phi_4) = 2$. Elementami rzędu 10 w grupie $\mathbb{Z}_{10}$ są $1, 3, 7, 9$, zatem $\mathrm{Aut}(\mathbb{Z}_8)$ ma 4 elementy $\psi_1(1) = 1$, $\psi_2(1) = 3$, $\psi_3(1) = 7$ oraz $\psi_4(1) = 9$, przy czym $o(\psi_1) = 1$, $o(\psi_2) = o(\psi_3) = 4$ oraz $o(\psi_4) = 2$. Wiemy, że automorfizm zachowuje rzędy elementów, zatem jako, że rzędy elementów obu grup są różne, to $\mathrm{Aut}(\mathbb{Z}_8)$ i $\mathrm{Aut}(Z_{10})$ nie są izomorficzne.

Zauważmy, że $\phi_2 \circ \phi_3 = \phi_3 \circ \phi_2 = \phi_4$, bo $\phi_2(\phi_3(1)) = \phi_2(5) = 7$ oraz $\phi_3(\phi_2(1)) = \phi_3(3) = 7$. Zatem generatory $\mathrm{Aut}(\mathbb{Z}_8)$ to ϕ_2 oraz ϕ_3. Zauważmy też, że $\mathrm{Aut}(\mathbb{Z}_8) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, ponieważ $\mathrm{Aut}(\mathbb{Z}_8)$ ma trzy elementy rzędu 2. Weźmy więc $F = \{\phi_1, \phi_2\}$ oraz $H = \{\phi_1, \phi_3\}$, wówczas

$$F \times H = \{\phi_1, \phi_2, \phi_3, \phi_2 \circ \phi_3 = \phi_4\} = \mathrm{Aut}(\mathbb{Z}_8)$$

Ćwiczenia 7

Definicja: Klasa sprzężoności elementu x grupy G, to zbiór $[x] = \{gxg^{-1} \mid g \in G\}$.

Fakt: Permutacje $\sigma, \tau \in S_n$ są sprzężone, czyli istnieje $\rho \in S_n$, że $\sigma = \rho\tau\rho^{-1}$, wtedy i tylko wtedy, gdy σ i τ mają taki sam rozkład na cykle rozłączne.

Zadanie 1.
Niech $g \in S_7$ będzie permutacją, która w rozkładzie na cykle rozłączne ma jeden 3-cykl oraz cztery cykle długości 1. Ile jest elementów sprzężonych z g w S_7?

Rozwiązanie:
Szukamy więc ile jest permutacji, które mają taki sam rozkład na cykle co permutacja g. Na $\binom{7}{3} = 35$ wybieramy elementy do cyklu długości 3 i ustawiamy je na $\frac{3!}{3} = 2$ sposoby. Pozostałe elementy ustawiamy na 1 sposób. Daje nam to łącznie $35 \cdot 2 = 70$ elementów sprzężonych z g w S_7.

Zadanie 2.
Wyznacz klasy sprzężoności w grupie S_4 oraz wszystkie dzielniki normalne grupy S_4.

Rozwiązanie:
Wyznaczmy najpierw klasy sprzężoności

$K_1 : (\cdot)(\cdot)(\cdot)(\cdot)$	$K_{22} : (\cdot\ \cdot)(\cdot\ \cdot)$	$K_2 : (\cdot\ \cdot)(\cdot)(\cdot)$	$K_3 : (\cdot\ \cdot\ \cdot)(\cdot)$	$K_4 : (\cdot\ \cdot\ \cdot\ \cdot)$
1	3	6	8	6

Wyznaczmy teraz wszystkie dzielniki normalne w grupie S_4. Wiemy, że jeśli $H \triangleleft G$ oraz $g \in G$ i $h \in H$, to klasa sprzężoności elementu h to $\{ghg^{-1} \mid g \in G\} \subseteq H$, bo skoro H jest podgrupą normalną, to $ghg^{-1} \in H$. Zatem jeśli $H \triangleleft G$, to H jest sumą pewnych klas sprzężnoności w G. Zatem dla dowolnego elementu z H jego klasa sprzężoności jest zawarta w H.

Mamy $|S_4| = 24$, zatem jeśli $H \leq S_4$, to $|H| \in \{1, 2, 3, 4, 6, 8, 12, 24\}$. Grupy $\{id\}$ oraz S_4 to oczywiście podgrupy normalne S_4. Będziemy więc brali klasy sprzężoności grupy S_4 i patrzyli czy ich sumy tworzą podgrupy. Jeśli będą to podgrupy, to wiemy że będą to podgrupy normalne. Suma rzędów klas sprzężoności musi być dzielnikiem 24. Ponadto wiemy, że $\{id\} \in H \leq S_4$, zatem szukamy takich $k_1, \ldots, k_l$, że $(1 + k_1 + \ldots + k_l) \mid 24$, gdzie k_i jest możliwym rzędem klasy sprzężoności grupy S_4. Oczywiście jednym z k_i musi być 3, ponieważ w przeciwny, przypadku suma nie będzie podzielna przez 24.

Rozważmy przypadek $1 + 3$. Sprawdźmy, czy

$$V_4 = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

to podgrupa. Jest to podgrupa, bo dla dowolnego $a \in V_4$ i $a \neq id$ mamy $o(a) = 2$, czyli $a^{-1} = a \in V$ oraz jeśli $a, b \in V_4$, to również $ab \in V_4$.

Rozważmy przypadek $1 + 3 + 8$. Sprawdźmy czy

$$A_4 = \{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3)\}$$

to podgrupa. Jest to podgrupa, bo jest to grupa permutacji parzystych (grupa alternująca).

Trzeci przypadek to gdy mamy $1 + 3 + 6 + 6 + 8$, ale wówczas otrzymujemy całą grupę S_4.

Zatem podgrupy normalne S_4 to

$$\{id\}, V_4, A_4, S_4$$

Fakt: Jeśli $H \triangleleft G$, to H jest sumą pewnych klas sprzężoności w G.

Zadanie 3.
Uzasadnić, że istnieje bijekcja

$$\{ \text{ homomorfizmy } G \to H_1 \times H_2\} \longrightarrow \{ \text{ homomorfizmy } G \to H_1\} \times \{ \text{ homomorfizmy } G \to H_2\}$$

Rozwiązanie:
Chcemy przyporządkować wzajemnie jednoznacznie homomorfizmowi $\phi : G \to H_1 \times H_2$ parę $(\phi_1 : G \to H_1, \phi_2 : G \to H_2)$.

$\to$ Niech $\phi : G \to H_1 \times H_2$ oraz niech $\phi(g) = (g_1, g_2)$, wówczas niech $\phi_1(g) = g_1$ oraz $\phi_2(g) = g_2$. Innymi słowy niech $p_1 : H_1 \times H_2 \to H_1$ oraz $p_2 : H_1 \times H_2 \to H_2$ będą rzutami na współrzędne. Wówczas p_1 i p_2 to homomorfizmy. Stąd $\phi_1 = p_1 \circ \phi$ oraz $\phi_2 = p_2 \circ \phi$. Zatem ϕ_1 i ϕ_2 to homomorfizmy jako złożenie dwóch homomorfizmów.

$\leftarrow$ Jeśli $\phi_1 : G \to H_1$ oraz $\phi_2 : G \to H_2$, to $\phi : G \to H_1 \times H_2$ zadane będzie dla każdego $g \in G$ wzorem $\phi(g) = (\phi_1(g), \phi_2(g))$. Chcemy sprawdzić czy to jest dobrze określony homomorfizm. Mamy

$$\begin{aligned} \phi(gh) &= (\phi_1(gh), \phi_2(gh)) = (\phi_1(g) \cdot \phi_1(h), \phi_2(g) \cdot \phi_2(h)) = \\ &= (\phi_1((g), \phi_2(g)) \cdot (\phi_1(h), \phi_2(h)) = \phi(g) \cdot \phi(h) \end{aligned}$$

Fakt: Jeśli $f : G \to H$ to homomorfizm, to $\ker(f) \triangleleft G$.

Zadanie 4.
Wyznaczyć homomorfizmy z grupy D_6 w grupę $\mathbb{Z}_6$

Rozwiązanie:
Wiemy, że jeśli $f : G \to H$ to homomorfizm, to $\ker f \triangleleft G$. Musimy więc patrzeć na podgrupy normalne w G jako na jądra homomorfizmów. Podgrupy normalne w D_6 to $\{id\}, D_6, \langle\rho\rangle$

- Jeśli $\ker f = \{id\}$, to $f : D_6 \hookrightarrow \mathbb{Z}_6$, czyli $|D_6| = |\mathbb{Z}_6| = 6$, czyli f jest izomorfizmem. Wówczas zachodziłoby $D_6 \simeq \mathbb{Z}_6$, ale to jest sprzeczne, bo $D_6 \not\simeq \mathbb{Z}_6$.
- Jeśli $\ker f = D_6$, to f jest homomorfizmem trywialnym, ponieważ $\ker f = \{x \in D_6 \mid f(x) = 0\}$, czyli $f(x) = 0$ dla każdego $x \in D_6$.
- Jeśli $\ker f = \langle\rho\rangle$, to $f : D_6 \to \mathbb{Z}_6$ będzie takie, że $f(\rho) = 0$. Wówczas $o(f(\sigma)) \mid o(\sigma) = 2$, czyli $f(\sigma)$ musi być rzędu 2, ponieważ $f(\sigma)$ nie może być elementem neutralnym, bo nie należy do jądra f. Stąd $f(\sigma) = 3$. Mamy więc homomorfizm zadany na generatorach $f(\rho) = 0$ oraz $f(\sigma) = 3$.

Zatem istnieją dwa homomorfizmy.

Definicja: Zbiór ilorazowy grupy G względem N to zbiór $G/N = \{gN \mid g \in G\}$. Jeśli $N \triangleleft G$, to $G/N = \{gN \mid g \in G\}$ jest grupą, gdzie $xN \cdot yN = xyN$ oraz $(xN)^{-1} = x^{-1}N$.

Twierdzenie: (Pierwsze twierdzenie o izomorfizmie) Niech $f : G \to H$ będzie homomorfizmem grup. Wówczas

1. istnieje dokładnie jeden homomorfizm $g : G/\ker(f) \to H$ taki, że $f = g \circ \pi$
2. grupa $G/\ker(f)$ jest izomorficzna z $\mathrm{im}(f)$
3. jeśli homomorfizm f jest epimorfizmem, to $G/\ker(f) \simeq H$

Homomorfizm $\pi : G \to G/N$, gdzie $\pi(g) = gN$ to epimorfizm naturalny (naturalne rzutowanie dla $N = \ker(f)$)

Zadanie 5.
Rozważmy odwzorowanie $f : \mathbb{R} \to \mathbb{C}^*$ dane wzorem $f(t) = e^{2\pi i \cdot t}$. Czy jest to homomorfizm grup? Znajdź obraz i jądro.

Rozwiązanie:
Pokażemy, że $f(t + s) = f(t) \cdot f(s)$. Mamy

$$f(t + s) = e^{2\pi i(t+s)} = e^{2\pi it} \cdot e^{2\pi is} = f(t) \cdot f(s)$$

zatem f jest homomorfizmem. Mamy $|e^{2\pi it}| = 1$, zatem $f : (\mathbb{R}, t) \to S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$, skąd $\mathrm{im} f = S^1$. Mamy $\ker f = \{t \in \mathbb{R} \mid e^{2\pi it} = 1\} = \mathbb{Z}$

Zadanie 6.
Niech G będzie grupą A_4 parzystych permutacji czterech elementów

a) Wypisać wszystkie klasy sprzężoności

b) Znaleźć wszystkie podgrupy normalne

c) Znaleźć wszystkie obrazy homomorficzne

Rozwiązanie:
Wiemy, że

$$A_4 = \{id, (\cdot\ \cdot\ \cdot) \times 8, (\cdot\ \cdot)(\cdot\ \cdot) \times 3\}$$

a) Jeśli $A_4 \triangleleft S_4$, to dla każdego $x \in A_4$ zachodzi $\{gxg^{-1} \mid g \in A_4\} \subseteq \{gxg^{-1} \mid g \in S_4\}$, czyli jeśli $x, y \in A_4$ są w tej samej klasie sprzężoności, to mają taki sam rozkład na cykle, bo są w tej samej klasie sprzężoności S_4. Mamy $[(id)] = \{id\}$. Wyznaczmy klasę sprzeżoności cyklu długości trzy (1 2 3). Zauważmy, że jeśli $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a_1 & a_2 & a_3 & a_4 \end{pmatrix} \in A_4$, to wówczas $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a_2 & a_3 & a_1 & a_4 \end{pmatrix} \in A_4$ oraz $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a_3 & a_1 & a_2 & a_4 \end{pmatrix} \in A_4$, ponieważ każdy z dwóch ostatnich cykli (σ_2, σ_3) to pierwszy (σ_1) pomnożony przez 3-cykl $\tau = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_1 & a_4 \end{pmatrix} = (a_1\ a_2\ a_3) \in A_4$. Dalej mamy

$$\sigma_1 \cdot (1\ 2\ 3) \cdot \sigma_1^{-1} = (a_1\ a_2\ a_3)$$

$$\sigma_2 \cdot (1\ 2\ 3) \cdot \sigma_2^{-1} = (a_2\ a_3\ a_1) = (a_1\ a_2\ a_3)$$

$$\sigma_3 \cdot (1\ 2\ 3) \cdot \sigma_3^{-1} = (a_3\ a_1\ a_2) = (a_1\ a_2\ a_3)$$

Czyli sprzęgając przez trzy elementy w A_4, dostajemy ten sam element w klasie sprzężoności $[(1\ 2\ 3)]$. Stąd w klasie sprzężoności elementu (1 2 3) w A_4 mogą być co najwyżej $\frac{12}{3} = 4$ elementy. Wyznaczmy wiec te elementy. Mamy

$$(1\ 2)(3\ 4) \cdot (1\ 2\ 3) \cdot ((1\ 2)(3\ 4))^{-1} = (2\ 1\ 4)$$

$$(1\ 3)(2\ 4) \cdot (1\ 2\ 3) \cdot ((1\ 3)(2\ 4))^{-1} = (3\ 4\ 1)$$

$$(1\ 4)(2\ 3) \cdot (1\ 2\ 3) \cdot ((1\ 4)(2\ 3))^{-1} = (4\ 3\ 2)$$

Stąd

$$[(1\ 2\ 3)] = \{(1\ 2\ 3), (2\ 1\ 4), (1\ 3\ 4), (2\ 4\ 3)\}$$

Analogicznie

$$[(1\ 3\ 2)] = \{(1\ 3\ 2), (2\ 4\ 1), (1\ 4\ 3), (2\ 3\ 4)\}$$

Wyznaczmy klasę sprzężoności elementu (1 2)(3 4). Jeśli $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a_1 & a_2 & a_3 & a_4 \end{pmatrix} \notin A_4$, to $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a_2 & a_1 & a_3 & a_4 \end{pmatrix} \in A_4$, ponieważ $\sigma_2 = (a_1\ a_2) \circ \sigma_1$, czyli złożenie dwóch permutacji nieparzystych jest parzyste. Mamy

$$\sigma_1 \cdot (1\ 2)(3\ 4) \cdot \sigma_1^{-1} = (a_1\ a_2)(a_3\ a_4)$$

$$\sigma_2 \cdot (1\ 2)(3\ 4) \cdot \sigma_2^{-1} = (a_2\ a_1)(a_3\ a_4) = (a_1\ a_2)(a_3\ a_4)$$

Wiemy, że klasa sprzężoności w S_4 dwóch transpozycji to $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Ponadto biorąc dowolną $\sigma \in S_4$, wiemy że istnieje $\sigma' \in A_4$ taka, że sprzężenie z danym cyklem to to samo. Zatem

$$[(1\ 2)(3\ 4)] = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Stąd

$$A_4 = [id] \cup [(1\ 2)(3\ 4)] \cup [(1\ 2\ 3)] \cup [(1\ 3\ 2)] = K_1 \cup K_{22} \cup K_{(1\ 2\ 3)} \cup K_{(1\ 3\ 2)}$$

b) Wyznaczmy podgrupy normalne w A_4. Wiemy, że $|A_4| = 12$, zatem jeśli $H \leq A_4$, to $|H| \in \{1, 2, 3, 4, 6, 12\}$. Wiemy też, że jeśli $N \triangleleft A_4$, to N jest sumą klas sprzężoności. Klasy sprzężoności mają rzędy odpowiednio równe $1, 3, 4, 4$. Niech więc $N \triangleleft A_4$. Oczywiście $id \in N$.

Sprawdźmy, czy $K_1 \cup K_{22} \leq A_4$, czyli czy

$$V_4 = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

jest grupą. To oczywiście jest podgrupa. Jest ona izomorficzna z $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Więcej możliwości nie mamy do sprawdzenia, ponieważ aby rząd podgrupy był podzielny przez 12, to musimy wziąć K_1, bo id jest elementem każdej podgrupy oraz K_{22}, bo jako jedyne ma rząd nieparzysty. Branie większej liczby klas sprzężoności da nam całą grupę A_4. Stąd wszystkie podgrupy normalne to

$$\{id\}, V_4, A_4$$

c) Szukanie obrazów homomorficznych grupy G, to jest tak naprawdę patrzenie na podgrupy ilorazowe G/N, gdzie $N \triangleleft G$.

- Jeśli $N = \{id\}$, to $A_4/N = A_4$, czyli A_4 jest obrazem homomorficznym A_4.
- Jeśli $N = A_4$, to $A_4/N = \{id\}$, czyli $\{id\}$ jest obrazem homomorficznym A_4.
- Jeśli $N = V_4$, to mamy $|A_4/N| = \frac{|A_4|}{|N|} = \frac{12}{4} = 3$, skąd $A_4/N \simeq \mathbb{Z}_3$, bo istnieje tylko jedna grupa rzędu 3.

Stąd obrazy homomorficzne to

$$A_4, \{id\}, \mathbb{Z}_3$$

Zadanie 7.
Znajdź wszystkie grupy, które mogą być obrazem homomorfizmu $f : G \to H$ gdzie G jest

a) grupą S_3 permutacji trzech elementów

b) grupą D_8 izometrii kwadratu

Rozwiązanie:

a) Wiemy, że $S_3 \simeq D_6$, zatem jako, że znamy już podgrupy normalne D_6, to rozpatrzmy $G = D_6$. Z twierdzenia o izomorfizmie wiemy, że możliwe jądra to podgrupy normalne, czyli

$$\{id\}, \langle\rho\rangle, D_6$$

Wiemy też, że grupa $\frac{G}{\ker(f)}$ jest izomorficzna z $\mathrm{im}(f)$.

- Jeśli $\ker(f) = \{id\}$, to $\left|\frac{G}{\ker(f)}\right| = \frac{6}{1} = 6$, czyli obrazem są grupy izomorficzne z D_6.
- Jeśli $\ker(f) = D_6$, to $\left|\frac{G}{\ker(f)}\right| = \frac{1}{1} = 1$, zatem obrazem jest $\{id\}$.
- Jeśli $\ker(f) = \langle\rho\rangle$, to $\left|\frac{D_6}{\ker(f)}\right| = \frac{6}{3} = 2$, czyli obrazem będzie grupa o rzędzie 2, czyli $\mathbb{Z}_2$.

Zatem możliwe obrazy homomorfizmu to $\{id\}, \mathbb{Z}_2, D_6$ oraz wszystkie grupy z nimi izomorficzne.

b) Podgrupy normalne D_8 to

$$\{id\}, \langle\rho\rangle, \langle\rho^2\rangle, \langle\sigma, \rho^2\rangle, \langle\rho^2, \sigma\rho\rangle, D_8$$

- Jeśli $\ker(f) = \{id\}$, to $\left|\frac{G}{\ker(f)}\right| = \frac{8}{1} = 8$, zatem obrazem będą grupy izomorficzne z D_8.
- Jeśli $\ker(f) = D_8$, to $\left|\frac{G}{\ker(f)}\right| = \frac{8}{8} = 1$, czyli obrazem będą grupy izomorficzne z $\{id\}$.
- Jeśli $\ker(f) = \langle\rho\rangle$, to $\left|\frac{G}{\ker(f)}\right| = \frac{8}{4} = 2$, czyli obrazem będą grupy izomorficzne z $\mathbb{Z}_2$.
- Jeśli $\ker(f) = \langle\rho^2\rangle$, to $\left|\frac{G}{\ker(f)}\right| = \frac{8}{2} = 4$. Dalej mamy

  $$D_8/\ker(f) = \{\langle\rho^2\rangle, \rho\langle\rho^2\rangle, \sigma\langle\rho^2\rangle, \sigma\rho\langle\rho^2\rangle\}$$

  przy czym $o(\langle\rho^2\rangle) = 1$, $o(\rho\langle\rho^2\rangle) = 2$ (bo najmniejsze k takie, że $\rho^k \in \langle\rho^2\rangle$ to 2), $o(\sigma\langle\rho^2\rangle) = 2$ oraz $o(\sigma\rho\langle\rho^2\rangle) = 2$. Zatem obrazem będą grupy izomorficzne z $\mathbb{Z}_2 \times \mathbb{Z}_2$.
- Jeśli $\ker(f) = \langle\rho^2, \sigma\rangle$, to $\left|\frac{G}{\ker(f)}\right| = \frac{8}{4} = 2$, czyli obrazem będą grupy izomorficzne z $\mathbb{Z}_2$.
- Jeśli $\ker(f) = \langle\rho^2, \sigma\rho\rangle$, to $\left|\frac{G}{\ker(f)}\right| = \frac{8}{4} = 2$, czyli obrazem będą grupy izomorficzne z $\mathbb{Z}_2$.

Zatem możliwe obrazy homomorfizmu to $\{id\}, \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2, D_8$ oraz wszystkie grupy z nimi izomorficzne.

Zadanie 8.
Znajdź wszystkie homomorfizmy $D_8 \to \mathbb{Z}_4 \times \mathbb{Z}_4$.

Rozwiązanie:
Grupy H, które mogą być obrazem homomorfizmu $f : D_8 \to H$ to $\{id\}, \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2$ oraz D_8. Szukamy więc podgrup $\mathbb{Z}_4 \times \mathbb{Z}_4$ izomorficznych z $\{id\}, \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2$ lub D_8.

1. Jeśli $\mathrm{im}(f) = \{id\}$, to mamy homomorfizm trywialny, czyli $f(\sigma) = f(\rho) = (0, 0)$, zatem mamy 1 homomorfizm.

2. Jeśli $\mathrm{im}(f) = \mathbb{Z}_2$, to mamy trzy przypadki

   - Gdy $\ker(f) = \langle\rho\rangle$, to $f(\rho) = 0$ oraz $f(\sigma) \in \{(2,0),(0,2),(2,2)\}$, zatem mamy 3 homomorfizmy.
   - Gdy $\ker(f) = \langle\sigma,\rho^2\rangle$, to $f(\sigma) = (0,0)$ oraz $f(\rho) \in \{(2,0),(0,2),(2,2)\}$, zatem mamy 3 homomorfizmy.
   - Gdy $\ker(f) = \langle\rho^2,\sigma\rho\rangle$, to $f(\sigma) = f(\rho) \in \{(2,0),(0,2),(2,2)\}$, zatem mamy 3 homomorfizmy.

   Mamy więc 9 homomorfizmów.

3. Jeśli $\mathrm{im}(f) = \mathbb{Z}_2 \times \mathbb{Z}_2$, to jądro f jest izomorficzne z $\mathbb{Z}_2$, czyli $f(\rho)$ oraz $f(\sigma)$ są generatorami rzędu 2, zatem mamy

$$f(\rho) = (2,0) \text{ oraz } f(\sigma) \in \{(0,2),(2,2)\}$$

$$f(\rho) = (0,2) \text{ oraz } f(\sigma) \in \{(2,0),(2,2)\}$$

$$f(\rho) = (2,2) \text{ oraz } f(\sigma) \in \{(0,2),(2,0)\}$$

   czyli dostajemy 6 homomorfizmów.

4. Dla $\mathrm{im}(f) = D_8$ nie mamy żadnych homomorfizmów, ponieważ $\mathbb{Z}_4 \times \mathbb{Z}_4$ nie ma podgrup izomorficznych z D_8, bo D_8 ma pięć elementów rzędu 2, natomiast $\mathbb{Z}_4 \times \mathbb{Z}_4$ ma trzy elementy rzędu 2.

Dostajemy więc 16 homomorfizmów, które są opisane wyżej.

Zadanie 9.
Pokaż, że grupa $\mathbb{Q}/\mathbb{Z}$ (grupy te są rozpatrywane jako grupy względem działania dodawania) jest izomorficzna z grupą wszystkich pierwiastków zespolonych z 1 wszystkich możliwych stopni, względem działania mnożenia.

Rozwiązanie:
Niech G to grupa wszystkich pierwiastków zespolonych z 1 wszystkich możliwych stopni. Dowolny element $\in \mathbb{Q}/\mathbb{Z}$ możemy napisać w postaci $q + \mathbb{Z}$, gdzie $q \in [0,1) \cap \mathbb{Q}$.

Elementy grupy G są postaci

$$\cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$$

gdzie n to stopień pierwiastka, a $k \in \{0,1,\ldots,n-1\}$ to k-ty pierwiastek danego stopnia. Zauważmy teraz, że dla każdej liczby $q \in [0,1) \cap \mathbb{Q}$ możemy przedstawić ją w postaci $\frac{k}{n}$, gdzie n to liczba naturalna oraz $k \in \{0,1,\ldots,n-1\}$.

Rozważmy więc funkcję $f : \mathbb{Q}/\mathbb{Z} \to G$ zadaną wzorem $f(q+\mathbb{Z}) = \cos(2q\pi) + i\sin(2q\pi)$ dla $q \in [0,1) \cap \mathbb{Q}$. Pokażemy, że funkcja ta jest izomorfizmem.

- Funkcja ta jest homomorfizmem, ponieważ

$$\begin{aligned} f((q_1+\mathbb{Z})+(q_2+\mathbb{Z})) &= f((q_1+q_2)+\mathbb{Z}) = \cos(2(q_1+q_2)\pi)+i\sin(2(q_1+q_2)\pi) = \\ &= (\cos(2q_1\pi)\cos(2q_2\pi)-\sin(2q_1\pi)\sin(2q_2\pi))+ \\ &\quad +(i\sin(2q_1\pi)\cos(2q_2\pi)+i\cos(2q_1\pi)\sin(2q_2\pi)) = \\ &= (\cos(2q_1\pi)+i\sin(2q_1\pi))\cdot(\cos(2q_2\pi)+i\sin(2q_2\pi) = \\ &= f(q_1+\mathbb{Z})\cdot f(q_2+\mathbb{Z}) \end{aligned}$$

- Funkcja ta jest różnowartościowa, ponieważ

$$f(q_1+\mathbb{Z}) = f(q_2+\mathbb{Z}) \Leftrightarrow \cos(2q_1\pi)+i\sin(2q_1\pi) = \cos(2q_2\pi)+i\sin(2q_2\pi) \Leftrightarrow$$

$$\Leftrightarrow \cos(2q_1\pi) = \cos(2q_2\pi) \ \wedge \ \sin(2q_1\pi) = \sin(2q_2\pi) \Leftrightarrow q_1 = q_2 \quad (\text{bo } q_1, q_2 \in [0,1)\cap\mathbb{Q})$$

- Pokażemy, że $g(\cos(2q\pi)+i\sin(2q\pi)) = q+\mathbb{Z}$ jest funkcją odwrotną do f

$$g\circ f(q+\mathbb{Z}) = g(\cos(2q\pi)+i\sin(2q\pi)) = q+\mathbb{Z}$$

$$f\circ g(\cos(2q\pi)+i\sin(2q\pi)) = f(q+\mathbb{Z}) = \cos(2q\pi)+i\sin(2q\pi)$$

Zatem f jest izomorfizmem, czyli grupy $\mathbb{Q}/\mathbb{Z}$ oraz G są izomorficzne.

Ćwiczenia 8

Zadanie 1.
Niech $H \leq G$ będzie podgrupą taką, że $|H| = 2$. Pokaż, że wtedy $H \triangleleft G$ wtedy i tylko wtedy, gdy $H \subseteq Z(G)$.

Rozwiązanie:
Mamy $Z(G) = \{a \in G \mid \forall_{g \in G}\ ga = ag\}$. Weźmy więc $H \leq G$ taką, że $|H| = 2$.

$\Rightarrow$ Jeśli $|H| = 2$, to $H = \{1, a\}$, gdzie $a^2 = 1$. Wówczas dla każdego $x \in G$ mamy $x \cdot 1 = 1 \cdot x$, skąd $1 \in Z(G)$. Dalej chcemy pokazać, że $ax = xa$, czyli równoważnie, że $xax^{-1} = a$. Wiemy, że $xax^{-1} \in H$ z definicji podgrupy normalnej. Stąd $xax^{-1} = 1 \Leftrightarrow a = 1$ lub $xax^{-1} = a$. Pierwsze równanie jest sprzeczne z tym, że $a \neq 1$, zatem $xax^{-1} = a$. Stąd $H \subset Z(G)$.

$\Leftarrow$ Niech $H \subseteq Z(G)$, wówczas dla $h \in H$ dla każdego $x \in G$ mamy $xh = hx$, skąd $xH = Hx$.

Zadanie 2.
Niech $f : G \to H$ będzie homomorfizmem grup, zaś $N \triangleleft G$ i $K \triangleleft H$ podgrupami normalnymi. Udowodnij, że

a) $f(N) \triangleleft f(G)$

b) $f^{-1}(K) \triangleleft G$

Rozwiązanie:

a) Sprawdźmy najpierw, czy $f(N) \leq f(G)$. Dla dowolnego $a \in N$ mamy $a^{-1} \in N$, czyli

$$f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(1) = 1$$

skąd $f(a^{-1}) = (f(a))^{-1}$, zatem jeśli $f(a) \in f(N)$, to $(f(a))^{-1} \in f(N)$. Weźmy $x, y \in f(N)$, wówczas istnieją $a, b \in N$ takie, że $f(a) = x$ i $f(b) = y$. Chcemy pokazać, że $xy \in f(N)$. Mamy

$$xy = f(a)f(b) = f(ab)$$

skoro $a \in N$ i $b \in N$, to $ab \in N$, zatem $xy = f(ab) \in N$. Zatem $f(N)$ jest podgrupą $f(G)$. Pokażemy teraz, że jest to podgrupa normalna. Chcemy pokazać, że dla dowolnego $x \in f(G)$ zachodzi $xf(N) = f(N)x$. Skoro $x \in f(G)$, to istnieje $y \in G$ taki, że $f(y) = x$. Wówczas

$$xf(N) = f(y)f(N) = f(yN) \overset{N \triangleleft G}{=} f(Ny) = f(N)f(y) = f(N)x$$

przy czym $f(yN) = \{f(yn) \mid n \in \mathbb{N}\}$.

b) Weźmy $x \in G$. Chcemy pokazać, że $xf^{-1}(K)x^{-1} \subseteq f^{-1}(K)$, czyli że dla dowolnego $y \in f^{-1}(K)$ zachodzi $xyx^{-1} \in f^{-1}(K)$ lub równoważnie, że $f(xyx^{-1}) \in K$. Mamy

$$f(xyx^{-1}) = f(x)f(y)f(x^{-1}) = f(x)f(y)f(x)^{-1}$$

Skoro $f(y) \in K$ oraz $K \triangleleft H$, to również $f(x)f(y)f(x)^{-1} \in K$, zatem $f^{-1}(K)$ jest podgrupą normalną w G.

Definicja: Komutantem grupy G nazywamy podgrupę

$$[G,G] = \{ghg^{-1}h^{-1} \mid g \in G,\ h \in G\} \overset{ozn.}{=} \{[g,h] \mid g \in G, h \in G\}$$

Element $[g,h] = ghg^{-1}h^{-1}$ nazywamy komutatorem.

Zadanie 3.
Uzasadnij, że

a) komutant jest podgrupą normalną

b) jeśli podgrupa zawiera komutant to jest normalna

Rozwiązanie:

a) Komutant z definicji jest podgrupą, pozostaje nam więc do sprawdzenia, że jest to podgrupa normalna, czyli że dla każdego $x \in G$ zachodzi $x[G,G]x^{-1} \subseteq [G,G]$. Mamy

$$xghg^{-1}h^{-1}x^{-1} = xgx^{-1} \cdot xhx^{-1} \cdot xg^{-1}x^{-1} \cdot xh^{-1}x^{-1}$$

Ponadto $(xgx^{-1})^{-1} = xg^{-1}x^{-1}$, zatem

$$xgx^{-1} \cdot xhx^{-1} \cdot xg^{-1}x^{-1} \cdot xh^{-1}x^{-1} = [xgx^{-1}, xhx^{-1}]$$

oczywiście $xgx^{-1} \in G$ oraz $xhx^{-1} \in G$, zatem $[xgx^{-1}, xhx^{-1}] \in [G,G]$, czyli $[G,G]$ jest podgrupą normalną w G.

b) Chcemy pokazać, że jeśli $[G,G] \subseteq H$, to $H \triangleleft G$. Weźmy dowolny element $g \in G$ oraz dowolny element $h \in H$. Chcemy pokazać, że $ghg^{-1} \in H$. Mamy

$$ghg^{-1} = ghg^{-1}h^{-1} \cdot h$$

Skoro $ghg^{-1}h^{-1} \in [G,G] \subseteq H$, to $ghg^{-1}h^{-1} \in H$. Mamy więc $ghg^{-1} \in H$, bo H jest podgrupą. Zatem H jest podgrupą normalną.

Definicja: Podgrupę $H \leq G$ nazywamy podgrupą charakterystyczną, jeśli dla dowolnego automorfizmu $\varphi \in \mathrm{Aut}(G)$ zachodzi $\varphi(H) = H$, czyli H jest zachowywane przez każdy automorfizm.

Twierdzenie: Niech G będzie dowolną grupą i a jej ustalonym elementem. Funkcja φ_a określona wzorem $\varphi_a(x) = axa^{-1}$ jest automorfizmem grupy G. Automorfizm tej postaci nazywamy automorfizmem wewnętrznym. Zbiór automorfizmów wewnętrznych oznaczamy jako $\mathrm{In}(G)$.

Zadanie 4.

a) Uzasadnij, że komutant $[G,G]$ jest podgrupą charakterystyczną

b) Uzasadnij, że centrum $Z(G)$ jest podgrupą charakterystyczną

c) Uzasadnij, że jeśli H jest podgrupą charakterystyczną, $N \triangleleft G$ podgrupą normalną oraz $H \leq N$, to $H \triangleleft G$ jest podgrupą normalną w G

d) Wyznacz wszystkie podgrupy charakterystyczne grup S_3, Q_8, D_8

e) Podaj przykład grupy i jej dzielnika normalnego, który nie jest podgrupą charakterystyczną

Rozwiązanie:

a) Chcemy pokazać, że dla każdego $\varphi \in \mathrm{Aut}(G)$ mamy $\varphi([G,G]) = [G,G]$. Niech $[g,h] \in [G,G]$, wówczas

$$\varphi([g,h]) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = [\varphi(g), \varphi(h)]$$

Stąd $\varphi([G,G]) \subseteq [G,G]$. Wiemy, że $\varphi \in \mathrm{Aut}(G)$, czyli dla każdych $x, y \in G$ istnieją g, h takie, że $\varphi(g) = x$ oraz $\varphi(h) = y$, skąd $[x,y] = [\varphi(g), \varphi(h)] = \varphi([g,h])$ czyli $\varphi([G,G]) \supseteq [G,G]$. Stąd $\varphi([G,G]) = [G,G]$.

b) Niech $\varphi \in \mathrm{Aut}(G)$ oraz $x \in Z(G)$. Chcemy pokazać, że $\varphi(x) \in Z(G)$, czyli czy dla dowolnego $g \in G$ zachodzi $\varphi(x) \cdot g = g \cdot \varphi(x)$. Wiemy, że istnieje $q \in G$ takie, że $\varphi(q) = g$, czyli

$$\varphi(x) \cdot g = \varphi(x) \cdot \varphi(q) = \varphi(xq) \overset{x \in Z(G)}{=} \varphi(qx) = \varphi(q) \cdot \varphi(x) = g \cdot \varphi(x)$$

Stąd $\varphi(Z(G)) \subseteq Z(G)$. Chcemy pokazać teraz, że $Z(G) \subseteq \varphi(Z(G))$, czyli że z tego że $x \in Z(G)$ wynika, że $x \in \varphi(Z(G))$, czyli że $\varphi^{-1}(x) \in Z(G)$. Skoro φ jest automorfizmem to również φ^{-1} jest automorfizmem (czyli $\varphi^{-1} = \psi$), zatem powtarzając rozumowanie mamy $\varphi^{-1}(x) \in Z(G)$, skąd $Z(G) \subseteq \varphi(Z(G))$.

c) Wiemy, że skoro $N \triangleleft G$, to dla każdego $g \in G$ zachodzi $gNg^{-1} = N$. Rozważmy dla każdego $g \in G$ automorfizm wewnętrzny $\varphi_g \in \mathrm{Aut}(G)$, czyli taki automorfizm, że dla każdego $h \in G$ zachodzi $\varphi_g(h) = ghg^{-1}$. Wiemy, że skoro $N \triangleleft G$, to dla każdego $g \in G$ automorfizm φ_g jest również automorfizmem w $\mathrm{Aut}(N)$, czyli $\varphi_g : N \to N$. Skoro H jest podgrupą charakterystyczną, to dla każdego $\varphi \in \mathrm{Aut}(N)$ mamy $\varphi(H) = H$. Chcemy pokazać, że dla dowolnego $g \in G$ mamy $gHg^{-1} = H$. Biorąc $\varphi_g \in \mathrm{Aut}(N)$ dla dowolnego elementu $g \in G$ mamy $\varphi_g(H) = H$, czyli również $gHg^{-1} = H$, skąd $H \triangleleft G$.

d) Jeśli $H \leq G$ i H to podgrupa charakterystyczna, to dla dowolnego automorfizmu, czyli w szczególności dla φ_g mamy $\varphi_g(H) = H$, czyli $gHg^{-1} = H$, czyli $H \triangleleft G$. Zatem jeśli podgrupa H jest charakterystyczna, to jest również normalna.

Wyznaczmy podgrupy charakterystyczne S_3. Podgrupy normalne w S_3 to $\{id\}, A_3, S_3$. Wiemy, że $\mathrm{Aut}(S_3) \simeq S_3$ oraz $\mathrm{Aut}(S_3) = \mathrm{In}(S_3)$, zatem dla każdego $\varphi \in \mathrm{Aut}(S_3)$ istnieje $g \in S_3$ takie, że $\varphi = \varphi_g$. Dla dowolnego $g \in S_3$ i dowolnej podgrupy normalnej H grupy S_3 mamy więc $\phi_g(H) = gHg^{-1} = H$, skąd wszystkie podgrupy normalne w S_3 to podgrupy charakterystyczne w S_3.

Wyznaczmy podgrupy charakterystyczne Q_8. Podgrupy normalne w Q_8 to $\{1\}$, $\{1,-1\}$, $\langle i \rangle$, $\langle j \rangle$, $\langle k \rangle$, Q_8. Wiemy, że centrum jest podgrupą charakterystyczną, czyli $Z(Q_8) = \{1,-1\}$

jest podgrupą charakterystyczną Q_8. Podgrupa trywialna $\{1\}$ i podgrupa będąca całą grupą Q_8 również są charakterystyczne. Pozostaje więc sprawdzić, czy $\langle i\rangle$ lub $\langle j\rangle$ lub $\langle k\rangle$ są charakterystyczne. Weźmy automorfizm φ taki, że $\varphi(i) = j$, $\varphi(j) = k$ oraz $\varphi(k) = i$, wówczas $\varphi(\langle i\rangle) = \langle j\rangle$, $\varphi(\langle j\rangle) = \langle k\rangle$ oraz $\varphi(\langle k\rangle) = \langle i\rangle$. Stąd $\langle i\rangle, \langle j\rangle, \langle k\rangle$ to nie są podgrupy charakterystyczne Q_8.

Wyznaczmy podgrupy charakterystyczne w D_8. Podgrupy normalne w D_8 to $\{id\}$, $\langle\rho\rangle$, $\langle\rho^2\rangle$, $\langle\rho^2, \sigma\rho\rangle$ oraz $\langle\rho^2, \sigma\rho^2\rangle$. Na pewno podgrupami charakterystycznymi będą $\{id\}$ oraz D_8. Również $\langle\rho^2\rangle$ jest podgrupą charakterystyczną, bo jest centrum grupy D_8. Dalej mamy $\langle\rho\rangle \simeq \mathbb{Z}_4$ oraz $\langle\rho^2, \sigma\rho\rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq \langle\rho^2, \sigma\rho^2\rangle$. Weźmy więc dowolny automorfizm $\varphi \in \mathrm{Aut}(D_8)$, wówczas $\varphi(\langle\rho\rangle) \simeq \langle\rho\rangle$, ale jedyną podgrupą w D_8 izomorficzną z $\langle\rho\rangle$ jest $\langle\rho\rangle$, skąd $\varphi(\langle\rho\rangle) = \langle\rho\rangle$, czyli również $\langle\rho\rangle$ jest podgrupą charakterystyczną. Podgrupy $\langle\rho^2, \sigma\rho\rangle$ oraz $\langle\rho^2, \sigma\rho^2\rangle$ są z dokładnością do izomorfizmu nierozróżnialne, więc pewnie nie będą charakterystyczne. Wskażemy więc taki automorfizm, który jedną przeprowadza na drugą. Niech więc $\varphi : D_8 \to D_8$ zadany będzie wzorem $\varphi(\rho) = \rho$ (bo $\varphi(\rho)$ to może być ρ albo ρ^3, bo to są jedyne elementy rzędu 4 w D_8) oraz $\varphi(\sigma) = \sigma\rho$ (bo $\varphi(\sigma)$ musi być rzędu 2 oraz musi być spełniony warunek $\varphi(\sigma\rho) = \sigma\rho^2$). Stąd $\langle\rho^2, \sigma\rho\rangle$ nie jest podgrupą charakterystyczną. Analogicznie automorfizm φ^{-1} przeprowadza drugą grupę na pierwszą, skąd $\langle\rho^2, \sigma\rho^2\rangle$ nie jest podgrupą charakterystyczną w D_8.

e) Jest to na przykład Q_8 i na przykład podgrupa $\langle i\rangle$ jest normalna ale nie jest charakterystyczna.

Zadanie 5.
Niech $G_1, \ldots, G_n$ będą dowolnymi grupami skończonymi, zaś $g_i \in G_i$ dowolnym zestawem elementów tych grup, po jednym elemencie z każdej grupy. Oznaczmy przez $m_i = o(g_i)$ rząd elementu g_i w grupie G_i. Wyznacz rząd elementu $(g_1, \ldots, g_n) \in G_1 \times \ldots \times G_n$ w produkcie w zależności od m_i.

Rozwiązanie:
Oznaczmy grupę $G_1 \times \ldots \times G_n$ jako H. Chcemy znaleźć rząd elementu $(g_1, \ldots, g_n)$, czyli szukamy najmniejsze M takie, że $(g_1, \ldots, g_n)^M = 1_H = (1_{G_1}, \ldots, 1_{G_n})$. Jest to element neutralny, ponieważ

$$(x_1, \ldots, x_n) \cdot (1_{G_1}, \ldots, 1_{G_n}) = (x_1 \cdot 1_{G_1}, \ldots, x_n \cdot 1_{G_n}) = (x_1, \ldots, x_n)$$

Dalej mamy $(g_1, \ldots, g_n)^M = (g_1^M, \ldots, g_n^M)$, zatem

$$(g_1, \ldots, g_n)^M = 1_H \Leftrightarrow (g_1^M, \ldots, g_n^M) = 1_H \Leftrightarrow g_1^M = 1_{G_1},\ \ldots\ , g_n^M = 1_{G_n}$$

czyli $o(g_i) \mid M$ dla każdego $i \in \{1, \ldots, n\}$. Stąd $M \geq NWW(m_1, \ldots, m_n)$. Mamy

$$(g_1, \ldots, g_n)^{NWW(m_1,\ldots,m_n)} = (g_1^{NWW(m_1,\ldots,m_n)}, \ldots, g_n^{NWW(m_1,\ldots,m_n)}) = (1_{G_1}, \ldots, 1_{G_n}) = 1_H$$

skąd $M \leq NWW(m_1, \ldots, m_n)$, czyli rząd elementu $(g_1, \ldots, g_n)$ wynosi $M = NWW(m_1, \ldots, m_n)$.

Ćwiczenia 9

Zadanie 1.
Przypuśćmy, że iloraz grupy G przez jej centrum jest grupą cykliczną. Udowodnij, że G jest przemienna.

Rozwiązanie:
Wiemy, że $G/Z(G)$ jest cykliczna. Chcemy pokazać, że G jest przemienna. Skoro $G/Z(G)$ jest cykliczna, to istnieje $g \in G$ takie, że $G/Z(G) = \langle gZ(G)\rangle$, zatem dla $x, y \in G/Z(G)$ mamy $x = g^k Z(G)$ oraz $y = g^l Z(G)$. Czyli dla każdego $x', y' \in G$ mamy $x' = g^k \cdot z_1$ i $y' = g^l \cdot x_2$, gdzie $z_1, z_2 \in Z(G)$. Mamy $z_1 \cdot z_2 \in Z(G)$, bo $Z(G)$ jest podgrupą. Ponadto skoro $z_1, z_2 \in Z(G)$ to są przemienne z dowolnym elementem z G, czyli

$$x'y' = g^k \cdot z_1 \cdot g^l \cdot z_2 = g^k \cdot g^l \cdot z_1 \cdot z_2 = g^{k+l} \cdot z_1 \cdot z_2$$

analogicznie

$$y'x' = g^l \cdot z_2 \cdot g^k \cdot z_1 = g^l \cdot g^k \cdot z_2 \cdot z_1 = g^{k+l} \cdot z_1 \cdot z_2$$

czyli $x'y' = y'x'$, czyli G jest przemienna.

Uwaga: $o(gN)$ to najmniejsze k takie, że

$$(gN)^k = N \Leftrightarrow g^k N = N \Leftrightarrow g^k \in N$$

lub nieskończoność w przeciwnym przypadku.

Zadanie 2.
Z czym izomorficzna jest grupa $Q_8/Z(Q_8)$?

Rozwiązanie:
Wiemy, że $Z(Q_8) = \{1, -1\}$, zatem $\left|\frac{Q_8}{Z(Q_8)}\right| = 4$, czyli $Q_8/Z(Q_8)$ jest izomorficzna z $\mathbb{Z}_4$ lub z $\mathbb{Z}_2 \times \mathbb{Z}_2$. Mamy $Q_8/Z(Q_8) = \{Z(Q_8), iZ(Q_8), kZ(Q_8), jZ(Q_8)\}$, ponieważ $iZ(Q_8) \neq jZ(Q_8)$, bo gdyby te warstwy były równe to $i^{-1}j = -k \in Z(Q_8)$, co jest sprzecznością. Dalej $o(Z(Q_8)) = 1$, $o(iZ(Q_8)) = 2$, bo $iZ(Q_8) \cdot iZ(Q_8) = i^2 Z(Q_8) = -1Z(Q_8) = Z(Q_8)$, analogicznie $o(jZ(Q_8)) = 2$ oraz $o(kZ(Q_8)) = 2$. Zatem $Q_8/Z(Q_8) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Zadanie 3.
Czy istnieje grupa, w której jest dokładnie 11 elementów rzędu 7?

Rozwiązanie:
Załóżmy, że taka grupa istnieje. Niech $a \in G$ będzie rzędu 7. Wówczas każdy element zbioru $\langle a\rangle \setminus \{1\}$ jest rzędu 7. Mamy więc już 6 elementów rzędu 7. Niech $b \notin \langle a\rangle$, wówczas w $\langle b\rangle$ mamy 6 elementów rzędu 7. Pokażemy teraz, że $\langle a\rangle \cap \langle b\rangle = \{1\}$. Z twierdzenia Lagrange'a mamy $|\langle a\rangle \cap \langle b\rangle| \in \{1, 7\}$. Jeśli rząd jest równy 1, to mamy po prostu podgrupę trywialną. Załóżmy więc, że rząd tej grupy jest równy 7, wówczas $\langle a\rangle \cap \langle b\rangle = \langle a\rangle = \langle b\rangle$, co z kolei prowadzi do sprzeczności z tym, że $a \neq b$. Stąd $\langle a\rangle \cap \langle b\rangle = \{1\}$. Stąd grupa ma wówczas co najmniej 12 elementów.

Definicja: (Działanie grupy na zbiorze) Niech G będzie grupą, a X niech będzie zbiorem. Powiemy, że grupa G działa na X, gdy jest zdefiniowane $\varphi : G \times X \to X$ takie, że dla dowolnych $g, h \in G$ oraz $x \in X$ zachodzi

1. $\varphi(g, \varphi(h, x)) = \varphi(gh, x)$
2. $\varphi(1, x) = x$

Często piszemy zamiast $\varphi(g, x)$ po prostu $\varphi_g(x)$

Przykłady:

- Niech G, X będą dowolne i niech $\varphi : G \times X \to X$ będzie zadane wzorem $\varphi(g, x) = x$. Jest to działanie stałe (trywialne)
- Niech $G = GL(n, \mathbb{R})$ i $X = \mathbb{R}^n$, wówczas $\varphi : G \times X \to X$ zadane wzorem $\varphi(A, v) = Av$ definiuje nam działanie na zbiorze, bo $\varphi(I, v) = v$ oraz $\varphi(B, \varphi(A, v)) = B(Av) = (BA)v = \varphi(BA, v)$.
- Niech G będzie dowolne oraz $X = G$, wówczas $\varphi : G \times X \to X$ zadane wzorem $\varphi(g, x) = gxg^{-1}$ definiuje działanie na zbiorze. Nazywamy to działaniem przez sprzężenie.
- Niech G będzie dowolną grupą i niech dla $H \leq G$ zbiór X to zbiór warstw lewostronnych względem H w G, wówczas $\varphi : G \times X \to X$ zadane wzorem $\varphi(g, fH) = gfH$ definiuje działanie na zbiorze.

Działanie grupy na zbiorze $\varphi : G \times X \to X$ to jest to samo co homomorfizm $\psi : G \to S_X$, gdzie S_X to permutacje zbioru X. Zadany jest on wzorem $\psi(g)(x) = \varphi(g, x)$, przy czym $\psi(g) \in S_X$. Sprawdźmy czy rzeczywiście tak zadana funkcja zadaje homomorfizm. Chcemy sprawdzić, czy $\psi(gh) = \psi(g) \cdot \psi(h)$. Weźmy dowolne $x \in X$, wówczas

$$\psi(gh)(x) = \varphi(gh, x)$$

oraz

$$\psi(g) \cdot \psi(h)(x) = \psi(g)(\varphi(h, x)) = \varphi(g, \varphi(h, x)) = \varphi(gh, x)$$

czyli ψ to homomorfizm. Zobaczymy czy w obrazie tego homomorfizmu dostajemy wszystkie bijekcje zbioru X, czyli czy $\psi(g)$ jest bijekcją. Sprawdźmy czy $\psi(g^{-1})$ jest funkcją odwrotną do $\psi(g)$. Mamy

$$\psi(g) \circ \psi(g^{-1})(x) = \psi(g, \varphi(g^{-1}, x) = \varphi(gg^{-1}, x) = \varphi(1, x) = x$$

Zatem rzeczywiście mamy homomorfizm w bijekcje.

Twierdzenie Działanie G na X indukuje homomorfizm $\psi : G \to S_X$ oraz każdy homomorfizm $\Phi : G \to S_X$ indukuje działanie grupy G na zbiorze X.

Zadanie 4.
Niech H będzie podgrupą w G taką, że $[G : H] < \infty$. Udowodnij, że wówczas istnieje $\widetilde{H} \subseteq H$ takie, że $\widetilde{H} \triangleleft G$ oraz $[G : \widetilde{H}] < \infty$.

Ćwiczenia 10

Definicja Niech grupa G działa na zbiorze X oraz $x \in X$. Wtedy zbiór

$$G(x) = \{\varphi(g, x) \mid g \in G\}$$

nazywamy orbitą elementu $x \in X$ przy działaniu G.

Definicja: Niech grupa G działa na zbiorze X oraz $x \in X$. Wtedy

$$G_x = \{g \in G \mid \varphi(g, x) = x\}$$

jest podgrupą w G nazywaną stabilizatorem elementu $x \in X$ (lub grupą izotropii).

Fakt: Dla dowolnego $x \in X$ zachodzi $[G : G_x] = |G(x)|$.

Wniosek: Dla każdego $x \in X$ zachodzi $|G(x)| \mid |G|$.

Zadanie 1.

a) Pokaż, że każde działanie grupy $\mathbb{Z}_5$ na zbiorze 4-elementowym jest trywialne.

b) Niech $G = \mathbb{Z}_6$. Czy każde działanie G na zbiorze 5-elementowym jest trywialne?

Rozwiązanie:

a) Chcemy pokazać, że działanie jest trywialne, czyli że dla każdego $x \in X$ i dla każdego $g \in \mathbb{Z}_5$ zachodzi $\varphi(g, x) = x$. Wiemy, że $|G(x)| \mid |G|$, czyli skoro $|G| = 5$, to $|G(x)| \in \{1, 5\}$. Dalej wiemy, że zbiór X jest sumą orbit, czyli $|G(x)| \leq 4$. Stąd mamy $|G(x)| = 1$. Zatem dla każdego $x \in X$ mamy $|G(x)| = 1$, czyli dla każdego $g \in \mathbb{Z}_5$ mamy $\varphi(g, x) = x$.

Pokazaliśmy w szczególności, że każdy homomorfizm $\varphi : \mathbb{Z}_5 \to S_4$ jest trywialny.

b) Oznaczmy elementy zbioru X jako $X = \{x_1, x_2, x_3, x_4, x_5\}$. Działanie G na zbiorze 5-elementowym indukuje nam jakiś homomorfizm $\varphi : \mathbb{Z}_6 \to S_5$. Niech $\varphi(1) = (x_1\ x_2)$, bo $o(\varphi(1)) \in \{1, 2, 3, 6\}$. Działanie $\Phi : \mathbb{Z}_6 \times X \to X$ zdefiniujemy następująco $\Phi(1, x_1) = x_2$, $\Phi(1, x_2) = x_1$ oraz $\Phi(1, x_i) = x_i$ dla $i \in \{3, 4, 5\}$. Działanie to nie jest trywialne, zatem nie każde działanie $G = \mathbb{Z}_6$ na zbiorze 5-elementowym jest trywialne.

Zadanie 2.
Niech G będzie taką grupą, że $|G| = 33$, X zbiorem o 16 elementach oraz G działa na X. Pokaż, że istnieje punkt stały tego działania.

Rozwiązanie:
Punkt stały działania G na X to $x \in X$ taki, że dla każdego $g \in G$ zachodzi $\varphi(g, x) = x$. Wiemy, że rząd orbity dzieli rząd grupy, czyli $|G(x)| \mid |G| = 33$, zatem $|G(x)| \in \{1, 3, 11, 33\}$. Ponad to wiemy, że zbiór X jest sumą swoich orbit, zatem jako, że $|X| = 16$, to $|G(x)| \in \{1, 3, 11\}$. Jeśli działanie nie ma punktu stałego, to dla każdego $x \in X$ mamy $|G(x)| \in \{3, 11\}$. Jako, że $3 \nmid 16$, to działanie musi mieć 11-elementową orbitę, ale wówczas skoro $3 \nmid 5$, to mamy sprzeczność. Stąd $|G(x)| = 1$, więc element x jest punktem stałym tego działania.

Twierdzenie: (Cauchy'ego) Jeśli p jest liczbą pierwszą dzielącą rząd skończonej grupy G, to G zawiera element rzędu p.

Zadanie 3.
Udowodnij, że istnieją dwie grupy rzędu 6.

Rozwiązanie:
Jeśli $|G| = 6$, to istnieją $a, b \in G$ takie, że $o(a) = 2$ oraz $o(b) = 3$. Wówczas mamy $\langle a, b\rangle = G$, bo $|\langle a, b\rangle| > 3$ oraz $|\langle a, b\rangle| \mid |G| = 6$, czyli $|\langle a, b\rangle| = 6$. Jeśli w G istnieje element rzędu 6, to $G \simeq \mathbb{Z}_6$. Załóżmy więc, że w G nie istnieje element rzędu 6. Wiemy, że $\langle b\rangle$ jest normalna w G, bo $[G : \langle b\rangle] = 2$. Niech grupa G działa na zbiorze $X = G$ przez sprzęganie, czyli działanie $\varphi : G \times X \to X$ zadane jest wzorem $\varphi_g(h) = ghg^{-1}$. Działanie to indukuje inne działanie, bo sprzęganie przez elementy grupy $\langle b\rangle$ sprawia, że nie wychodzimy poza grupę $\langle b\rangle$, bo $\langle b\rangle$ jest normalna. Stąd mamy działanie $\psi : G \times \langle b\rangle \to \langle b\rangle$. W szczególności $\langle a\rangle$ działa przez sprzęganie na $\langle b\rangle$, czyli $\psi_a(b) = aba^{-1} \in \langle b\rangle$. To działanie wyznacza nam homomorfizm $\xi : \langle a\rangle \to \mathrm{Aut}(\langle b\rangle)$. Mamy $\psi_a \in \mathrm{Aut}(\langle b\rangle)$, ponieważ $\psi_a \circ \psi_a(b) = a(aba^{-1})a^{-1} \overset{o(a)=2}{=} b$, czyli $\psi_a = (\psi_a)^{-1}$. Jeśli $\psi_a \in \mathrm{Aut}(\langle b\rangle)$ to mamy dwie możliwości. Albo $\psi_a(b) = b$, albo $\psi_a(b) = b^2$. Jeśli $\psi_a(b) = b$, to $aba^{-1} = b$, czyli $ab = ba$. Jako, że $|\langle a\rangle| = 2$ oraz $|\langle b\rangle| = 3$, to $\langle a\rangle \cap \langle b\rangle = \{1\}$. Wiemy, że $ab \in G$ oraz, że $ab = ba$, zatem $o(ab) = 6$, bo $(ab)^k = 1 \Leftrightarrow a^k b^k = 1$, czyli $a^k = b^{-k}$, ale jako że $a^k \in \langle a\rangle$ oraz $b^{-k} \in \langle b\rangle$ oraz $\langle a\rangle \cap \langle b\rangle = \{1\}$, to $a^k = 1$ oraz $b^{-k} = 1$, a stąd $2|k$ i $3|k$, skąd $k = 6$. Stąd mamy sprzeczność z tym, że w G nie istnieje element rzędu 6. Jeśli $\psi_a(b) = b^2$, to $G = \langle a, b\rangle$, przy czym $aba^{-1} = b^2$, $a^2 = 1$ oraz $b^3 = 1$. Skonstruujmy izomorfizm $f : D_6 \to G$ na generatorach, czyli $f(\sigma) = a$ oraz $f(\rho) = b$. Jest to dobrze określony homomorfizm, bo $f(\sigma\rho\sigma) = aba = b^2 = f(\sigma^2)$, $f(a^2) = a^2 = 1 = f(1)$ oraz $f(\rho^3) = b^3 = 1 = f(1)$. Dalej, skoro $a, b \in f(D_6)$, to $G = \langle a, b\rangle \subseteq f(D_6)$, skąd f jest epimorfizmem. Jako, że $|D_6| = 6 = |G|$, to f jest izomorfizmem, czyli $G \simeq D_6$.

Fakt: Jeśli $NWD(n, m) = 1$, to $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{mn}$.

Zadanie 4.
Niech G będzie grupą skończoną. Grupa G działa na zbiorze $X = G$ przez sprzęganie, to znaczy $\phi : G \times X \to X$ jest zadane przez $\phi(g, x) = gxg^{-1}$.

a) Pokaż, że orbita $x \in X$ jest jednoelementowa wtedy i tylko wtedy, gdy $x \in Z(G)$.

b) Załóżmy dodatkowo, że $|G| = p^a$ dla pewnej liczby naturalnej p. Wywnioskuj, że wówczas

$Z(G) \neq \{1_G\}$.

Rozwiązanie:

a) Jeśli orbita $x \in X$ jest jednoelementowa, to $|G(x)| = 1$, czyli równoważnie dla każdego $g \in G$ mamy $gxg^{-1} = x$ lub równoważnie $gx = xg$, czyli $x \in Z(G)$.

b) G jest sumą pewnych orbit, to znaczy że istnieją $x_1, \ldots, x_k \in G$ takie, że $G = \bigcup G(x_i)$. Czyli $p^a = 1 + \sum_{x \in G \setminus \{1\}} |G(x)|$, bo oczywiście mamy $1 \in Z(G)$. Wiemy, że $|G(x)| \mid |G| = p^a$, czyli $|G(x)| = p^b$ dla $0 \leq b \leq a$. Stąd istnieje jeszcze co najmniej $p-1$ jednoelementowych orbit. Stąd istnieje $x \neq 1_G$ takie, że $|G(x)| = 1$, czyli $x \in Z(G)$.

Zadanie 5.
Pokaż, że jeśli grupa ma p^2 elementów dla pewnej liczby pierwszej p, to jest przemienna.

Rozwiązanie:
Wiemy, że $|Z(G)| \neq 1$, zatem skoro rząd podgrupy dzieli rząd grupy, to $|Z(G)| \in \{p, p^2\}$. Jeśli $|Z(G)| = p^2$, to $Z(G) = G$, czyli G jest przemienna. Załóżmy więc, że $|Z(G)| = p$, wówczas $|G/Z(G)| = \frac{p^2}{p} = p$, czyli $G/Z(G) \simeq \mathbb{Z}_p$. Wiemy teraz, że jeśli grupa podzielona przez centrum jest cykliczna, to grupa jest abelowa, zatem stąd otrzymujemy, że G jest abelowa.

Zadanie 6.
Wyznacz wszystkie grupy rzędu 15.

Rozwiązanie:
Z twierdzenia Cauchy'ego wiemy, że istnieją elementy a i b takie, że $o(a) = 5$ oraz $o(b) = 3$ oraz $\langle a \rangle \cap \langle b \rangle = \{1\}$. Przypuśćmy, że $bab^{-1} \notin \langle a \rangle$, czyli $\langle a \rangle$ nie jest w szczególności normalna. Mamy $o(bab^{-1}) = o(a) = 5$, zatem $\langle bab^{-1} \rangle$ jest drugą podgrupą rzędu 5 taką, że $\langle bab^{-1} \rangle \cap \langle a \rangle = \{1\}$. Niech więc $H_1 = \langle a \rangle$ oraz $H_2 = \langle bab^{-1} \rangle$. Rozpatrzmy zbiór $H_1 \cdot H_2 = \{h_1 h_2 \mid h_1 \in H_1, h_2 \in H_2\}$. Mamy $|H_1 \cdot H_2| = \frac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|} = 25$. Mamy więc grupę G o 15 elementach i jej podzbiór o 25 elementach, co jest niemożliwe. Zatem $bab^{-1} \in \langle a \rangle$. Mamy więc homomorfizm $\varphi : \langle b \rangle \to \mathrm{Aut}(\langle a \rangle)$ zadany wzorem $\varphi_b(a) = bab^{-1}$. Ponadto $\mathrm{Aut}(\langle a \rangle) = \mathrm{Aut}(\mathbb{Z}_5) \simeq N$, gdzie $|N| = 5 - 1 = 4$. Skoro rząd elementu dzieli rząd grupy, to homomorfizm φ będzie trywialny. Zatem $\varphi_b(a) = a$, czyli $bab^{-1} = a$ skąd $ab = ba$. Skoro $o(a) = 5$ i $o(b) = 3$ oraz a i b są przemienne, to $o(ab) = NWW(o(a), o(b)) = 15$. Stąd $G \simeq \mathbb{Z}_{15} = \mathbb{Z}_3 \times \mathbb{Z}_5$.

Ćwiczenia 11

Zadanie 1.
Załóżmy, że G jest grupą rzędu 34, w której istnieje dokładnie jeden element rzędu 2. Pokaż, że grupa G jest cykliczna.

Rozwiązanie:
Niech $a \in G$ będzie takie, że $o(a) = 2$. Dla każdego elementu $g \in G$ mamy $o(gag^{-1}) = o(a) = 2$, stąd jako, że a jest jedynym elementem rzędu 2, mamy $gag^{-1} = a$, czyli $\langle a \rangle \subseteq \mathbb{Z}(G)$ a stąd $\langle a \rangle \triangleleft G$. Z twierdzenia Cauchy'ego wiemy też, że istnieje $b \in G$ takie, że $o(b) = 17$. Wystarczy, że pokażemy że b jest przemienne z a, bo $|\langle a, b \rangle| = \frac{|\langle a \rangle| \cdot |\langle b \rangle|}{|\langle a \rangle \cap \langle b \rangle|} = \frac{2 \cdot 17}{1} = 34$, czyli $\langle a, b \rangle = G$.

I sposób: Wiemy, że dla każdego $g \in G$ mamy $gag^{-1} = a$, zatem w szczególności $bab^{-1} = a \Leftrightarrow ab = ba$, skąd a i b są przemienne, czyli G jest abelowa.

II sposób: Rozpatrzmy działanie $\langle b \rangle$ na zbiorze $X = \langle a \rangle$ przez sprzęganie. Działanie to indukuje nam homomorfizm $\varphi : \langle b \rangle \to \mathrm{Aut}(\langle a \rangle)$ zadany wzorem $\varphi_b(a) = bab^{-1}$. Mamy $|\langle b \rangle| = 17$ oraz $|\mathrm{Aut}(\langle a \rangle)| = |\mathrm{Aut}(\mathbb{Z}_2)| = 2 - 1 = 1$, skąd φ jest homomorfizmem trywialnym. Stąd $\varphi_b(a) = a$, czyli $bab^{-1} = a \Leftrightarrow ab = ba$, czyli G jest przemienna.

Dalej mamy $o(ab) = NWW(o(a), o(b)) = NWW(2, 17) = 34$, skąd $\mathbb{Z}_{34} \simeq \langle ab \rangle \leq G$, czyli $G \simeq \mathbb{Z}_{34}$.

Zadanie 2.
Niech G będzie grupą i niech $|G| = 2p$. Udowodnij, że

a) jeśli G jest przemienna to $G \simeq \mathbb{Z}_{2p}$

b) w przeciwnym przypadku G ma podgrupę normalną indeksu 2 i jest izomorficzna z grupą dihedralną D_{2p}

Rozwiązanie:

a) Z twierdzenia Cauchy'ego wiemy, że istnieje w tej grupie element rzędu 2 oraz element rzędu p. Skoro G jest przemienna to $ab = ba$ i wówczas $o(ab) = 2p$, czyli $G = \langle ab \rangle = \mathbb{Z}_{2p}$.

b) Załóżmy, że G nie jest przemienna, wówczas skoro $o(b) = 17$, to $\langle b \rangle \leq G$ ma indeks równy 2, czyli $[G : \langle b \rangle] = 2$, czyli $\langle b \rangle \triangleleft G$. Niech teraz $\langle a \rangle \leq G$ działa przez sprzęganie na $\langle b \rangle \triangleleft G$. To sprzęganie zadaje homomorfizm $\varphi : \langle a \rangle \to \mathrm{Aut}(\langle b \rangle)$ wzorem $\varphi_a(b) = aba^{-1}$. Skoro $\langle b \rangle \triangleleft G$, to $aba^{-1} \in \langle b \rangle$, czyli $\varphi_a(b) = b^i$ dla pewnego $i \in \{0, 1, \ldots, p-1\}$. Dalej mamy

$$\varphi_{a^2}(b) = \varphi_1(b) = b$$

oraz z drugiej strony

$$\varphi_{a^2}(b) = \varphi_a \circ (\varphi_a(b)) = \varphi_a(b^i) = ab^i a^{-1} = \underbrace{aba^{-1} \cdot \ldots \cdot aba^{-1}}_{i \text{ razy}} = b^{i^2}$$

Stąd $b^{i^2} = b$, czyli $b^{i^2-1} = 1$, skąd $p \mid i^2 - 1$. Zatem $p \mid (i-1)$ lub $p \mid (p+1)$, czyli skoro $i \in \{0, \ldots, p-1\}$, to $i = 1$ lub $i = p - 1 = -1$. Jeśli $i = 1$, to $aba^{-1} = b$, czyli

a i b są przemienne, co jest sprzeczne z założeniem. Jeśli $i = -1$, to $aba^{-1} = b^{-1} = b^{p-1}$ i wówczas $G = \langle a, b\rangle$, gdzie $a^2 = 1$, $b^p = 1$ oraz $aba^{-1} = b^{p-1}$. Pokażemy teraz, że $G \simeq D_{2p}$. Niech $f : D_{2p} \to G$ to homomorfizm zadany na generatorach tak, że $f(\sigma) = a$ oraz $f(\rho) = b$. Homomorfizm ten jest dobrze określony, bo $f(\sigma^2) = a^2 = 1$, $f(\rho^p) = b^p = 1$ oraz $f(\sigma\rho\sigma^{-1}) = aba^{-1} = b^{p-1} = f(\rho^{p-1})$. I stąd f jest epimorfizmem, bo $a, b \in \mathrm{im}(f)$. Stąd skoro $|D_{2p}| = 2p = |G|$, to f jest izomorfizmem, czyli $G \simeq D_{2p}$.

Zadanie 3.
Niech X będzie zbiorem złożonym z wszystkich podgrup grupy S_4. Grupa S_4 działa na X przez automorfizmy wewnętrzne. Niech $x = \langle(1\ 2\ 3)\rangle \in X$. Wyznacz orbitę $G(x)$ oraz stabilizator.

Rozwiązanie:
Działanie $\varphi : G \times X \to X$ zdefiniowane jest następująco $\varphi(g, H) = gHg^{-1}$. Mamy więc

$$G(x) = \{\varphi(g, x) \mid g \in S_4\} = \{g\langle(1\ 2\ 3)\rangle g^{-1} \mid g \in S_4\}$$

Dla $\sigma \in S_4$ mamy $\sigma(1\ 2\ 3)\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \sigma(3))$, zatem w orbicie będą wszystkie grupy generowane przez 3-cykle, czyli

$$G(x) = \{\langle(1\ 2\ 3)\rangle, \langle(1\ 2\ 4)\rangle, \langle(2\ 3\ 4)\rangle, \langle(1\ 3\ 4)\rangle\}$$

Dalej mamy $[G : G_x] = |G(x)| = 4$. Z twierdzenia Lagrange'a mamy więc $4 = [S_4 : G_x] = \frac{|S_4|}{|G_x|}$, skąd $|G_x| = \frac{4!}{4} = 6$. Wiemy, że

$$G_x = \{g \in S_4 \mid \langle g(1\ 2\ 3)g^{-1}\rangle = \langle(1\ 2\ 3)\rangle\}$$

Skoro $\langle(1\ 2\ 3)\rangle \simeq \mathbb{Z}_3$, to $\langle(1\ 2\ 3)\rangle \subseteq G_x$, bo mamy wówczas grupę przemienną. Dalej mamy

$$(1\ 2)(1\ 2\ 3)(1\ 2)^{-1} = (2\ 1\ 3) \in \langle(1\ 2\ 3)\rangle$$

zatem $(1\ 2) \in G_x$. Analogicznie $(2\ 3), (1\ 3) \in G_x$. Skąd ostatecznie mamy

$$G_x = \{\{id\}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\} \simeq S_3$$

Definicja: Centralizatorem elementu x w grupie G nazywamy zbiór wszystkich elementów tej grupy, które są z nim przemienne

$$C_G(x) = \{g \in G \mid gx = xg\} = \{g \in G \mid gxg^{-1} = x\}$$

Jest to szczególny przypadek stabilizatora dla grupy G działającej na zbiorze $X = G$ działaniem $\varphi_g(x) = gxg^{-1}$.

Zadanie 4.
Niech $\sigma = (1\ 2\ 3\ 4\ 5) \in A_5$. Wyznacz centralizator elementu σ w grupie S_5 oraz A_5. Policz moce klasy sprzężoności w każdej grupie.

Rozwiązanie:
Wiemy, że $[S_5 : C_{S_5}(\sigma)] = |S_5(\sigma)| = 4! = 24$. Stąd z twierdzenia Lagrange'a mamy $4! = \frac{|S_5|}{|C_{S_5}(\sigma)|}$, czyli $|C_{S_5}(\sigma)| = 5$. Mamy

$$C_{S_5}(\sigma) = \{g \in S_5 \mid g\sigma g^{-1} \in \sigma\}$$

Oczywiście σ^i jest przemienne z σ, czyli $\sigma^i \cdot \sigma \cdot \sigma^{-i} = \sigma$, zatem $\langle\sigma\rangle \subset C_{S_5}(\sigma)$. Skoro $|\langle\sigma\rangle| = 5$, to mamy $C_{S_5}(\sigma) = \langle\sigma\rangle$.

Wyznaczmy teraz centralizator σ w grupie A_5. W tym celu zobaczmy jak się mają do siebie $C_{A_5}(\sigma) = \{g \in A_5 \mid g\sigma = \sigma g\}$ oraz $C_{S_5}(\sigma) = \{g \in S_5 \mid g\sigma = \sigma g\}$. Mamy oczywiście zawieranie $C_{A_5}(\sigma) \subseteq C_{S_5}(\sigma)$. Skoro $C_{S_5}(\sigma) = \langle\sigma\rangle \subseteq A_5$, to $C_{S_5}(\sigma) \subseteq C_{A_5}(\sigma)$. Czyli $C_{A_5}(\sigma) = \langle\sigma\rangle$.

Dalej mamy $|A_5(\sigma)| = [A_5 : C_{A_5}(\sigma)] = \frac{|A_5|}{|C_{A_5}(\sigma)|} = \frac{60}{5} = 12$. Stąd w klasie sprzężoności $\sigma = (1\,2\,3\,4\,5)$ w A_5 jest 12 permutacji.

Ćwiczenia 12

Zadanie 1.
Niech G będzie grupą. Pokaż, że liczba elementów rzędu 7 w G nie może być równa 12.

Rozwiązanie:
Przypuśćmy, że istnieje grupa G, która ma 12 elementów rzędu 7. Wówczas istnieje element a taki, że $o(a) = 7$, czyli w $\langle a\rangle$ każdy z sześciu elementów ma rząd 7. Dalej, skoro w G jest 12 elementów rzędu 7, to istnieje element $b \notin \langle a\rangle$ taki, że $o(b) = 7$ oraz w $\langle b\rangle$ jest sześć elementów rzędu 7 takich że $\langle a\rangle \cap \langle b\rangle = \{1\}$. Stąd w grupie G istnieją dokładnie dwie podgrupy rzędu 7.

I sposób: Rozpatrzmy więc działanie grupy G na zbiorze $X = \{\langle a\rangle, \langle b\rangle\}$ przez sprzęganie. Pokażemy, że a i b są przemienne. Działanie jest zdefiniowane następująco $\varphi : G \times X \to X$ wzorem $\varphi(g, H) = gHg^{-1}$. Działanie to (po obcięciu do grupy $\langle a\rangle$) indukuje nam działanie $\overline{\varphi} : \langle a\rangle \times X \to X$. Z kolei działanie $\overline{\varphi}$ indukuje nam homomorfizm $f : \langle a\rangle \to S_X = f : \langle a\rangle \to S_2$. Wiemy, że $|\langle a\rangle| = 7$ oraz $|S_2| = 2$, czyli $NWD(|\langle a\rangle|, |S_2|) = 1$, czyli f musi być homomorfizmem trywialnym. Stąd mamy $a \cdot \langle b\rangle \cdot a^{-1} = \langle b\rangle$ oraz $a \cdot \langle a\rangle \cdot a^{-1} = \langle a\rangle$. Stąd w G mamy podgrupę $\langle a, b\rangle \triangleright \langle b\rangle$. Działanie $G = \langle a\rangle$ na $X = \langle b\rangle$ przez sprzęganie zadaje nam więc homomorfizm $\psi : \langle a\rangle \to \mathrm{Aut}(\langle b\rangle)$. Mamy $|\langle a\rangle| = 7$ oraz $|\mathrm{Aut}(\langle b\rangle)| = |\mathrm{Aut}(\mathbb{Z}_7)| = 6$, skąd (jako, że $NWD(7, 6) = 1$) ψ jest homomorfizmem trywialnym, czyli $\varphi_a(b) = aba^{-1}$ jest identycznością ($\varphi_a = id$), zatem $aba^{-1} = b$, skąd $ab = ba$. Mamy więc, że a i b są przemienne oraz $\langle a\rangle \cap \langle b\rangle = \{1\}$. Pokażemy, że $\langle a, b\rangle \simeq \langle a\rangle \times \langle b\rangle$. Elementy w $\langle a\rangle \times \langle b\rangle$ są postaci (a^k, b^l), natomiast elementy w $\langle a, b\rangle$ są postaci $a^{\alpha_1}b^{\beta_1}a^{\alpha_2}\ldots$, ale skoro a i b są przemienne, to elementy te są postaci $a^\alpha b^\beta$. Zadajmy więc izomorfizm między tymi grupami $\varphi : \langle a\rangle \times \langle b\rangle \to \langle a, b\rangle$ wzorem $\varphi(a^k, b^l) = a^k b^l$. φ jest „na" co jest oczywiste oraz homomorfizmem co również jest oczywiste (bo $ab = ba$). Dalej mamy $\ker(\varphi) = \{(a^k, b^l) \in \langle a\rangle \times \langle b\rangle \mid a^k b^l = 1_G\} = \{(a^k, b^l) \in \langle a\rangle \times \langle b\rangle \mid a^k = b^{-l}\}$ czyli jako, że $\langle a\rangle \ni a^k = b^{-l} \in \langle b\rangle$, to $a^k = b^{-l} = 1_G$, czyli $\ker(\varphi) = \{(1, 1)\}$. Skoro jądro jest trywialne, to φ jest izomorfizmem, więc z twierdzenia o izomorfizmie mamy $\langle a, b\rangle \simeq \langle a\rangle \times \langle b\rangle \simeq \mathbb{Z}_7 \times \mathbb{Z}_7$. Dalej elementami rzędu 7 w grupie $\mathbb{Z}_7 \times \mathbb{Z}_7$ to wszystkie elementy oprócz elementu neutralnego. Czyli w G musi być co najmniej $49 - 1 = 48$ elementów rzędu 7, co jest sprzeczne z tym, że elementów jest 12.

II sposób: Wiemy, że $(ab)^7 = 1$, bo a i b są przemienne, zatem $o(ab) \leq 7$. Dalej $(ab)^k = 1 \Leftrightarrow a^k b^k = 1$, czyli $b^k = a^{-k} \in \langle a\rangle \cap \langle b\rangle = \{1\}$, skąd $a^k = 1$ oraz $b^k = 1$. Skąd $k = 7$ jest najmniejszym takim k. Zatem mamy $o(ab) = 7$ i $ab \notin \langle a\rangle$ i $ab \notin \langle b\rangle$, czyli w G istnieje co najmniej 13 elementów rzędu 7.

Problem: Dana jest grupa G oraz zbiór X taki, że $|X| = n$. Mamy skonstruować działanie G na X o pewnych własnościach

Obserwacja 1: Niech X_1, X_2 to pewne zbiory. Rozpatrzmy sumę rozłączną tych elementów $X_1 \cup X_2$. Niech $\varphi : G \times X_1 \to X_1$ i $\psi : G \times X_2 \to X_2$ to działania G na tych zbiorach. Wówczas istnieje działanie $\sigma : G \times (X_1 \cup X_2) \to X_1 \cup X_2$ zadane wzorem

$$\sigma(g, x) = \begin{cases} \varphi(g, x) & \text{dla } x \in X_1 \\ \psi(g, x) & \text{dla } x \in X_2 \end{cases}$$

Obserwacja 2: Jeśli mamy grupę G i jej podgrupę $H \leq G$, to możemy rozpatrywać działanie G na zbiorze warstw względem H, czyli na zbiorze $X = G/H$. Działanie $\varphi : G \times (G/H) \to G/H$

zdefiniowane jest wzorem $\varphi(g, hH) = ghH$. Działanie to jest tranzytywne, czyli ma jedną orbitę, czyli dla każdych $gH, hH \in G/H$ istnieje element $p \in G$ taki, że $\varphi(p, hH) = gH$ (wynosi on $p = gh^{-1}$). Stabilizatorem H będzie $G_H = \{g \in G \mid \varphi(g, H) = H\} = H$ (stabilizatorem gH będzie gHg^{-1}).

Zadanie 2.
Niech grupa S_3 działa na zbiorze 8-elementowym. Czy istnieje działanie, które ma 2 punkty stałe oraz

a) 4 orbity

b) 3 orbity

Rozwiązanie:
Niech $X = \{x_1, \ldots, x_8\}$. Bez straty ogólności możemy założyć, że punkty stałe to x_7 i x_8, czyli dla każdego $g \in S_3$ mamy $\varphi(g, x_7) = x_7$ oraz $\varphi(g, x_8) = x_8$. Zatem orbity tego działania to m.in. $G(x_7) = \{x_7\}$ oraz $G(x_8) = \{x_8\}$.

a) Chcemy, aby nasze działanie miało 4 orbity. Niech więc $G(x_1)$ i $G(x_4)$ to pozostałe dwie orbity. Wiemy, że suma mocy orbit jest równa mocy zbioru, zatem

$$1 + 1 + |G(x_1)| + |G(x_4)| = 8$$

oraz że moc orbity dzieli moc zbioru, czyli $|G(x_i)| \mid |S_3| = 6$, skąd $|G(x_i)| \in \{1, 2, 3, 6\}$. Z tych dwóch faktów otrzymujemy, że $|G(x_1)| = |G(x_4)| = 3$. Niech więc $G(x_1) = \{x_1, x_2, x_3\}$ oraz $G(x_4) = \{x_4, x_5, x_6\}$. Chcemy teraz skonstruować działanie o takich orbitach. Skonstruujmy więc najpierw działanie tranzytywne G na zbiorze $\{x_1, x_2, x_3\}$ a następnie na zbiorze $\{x_4, x_5, x_6\}$, a następnie skonstruujmy działanie na ich sumie rozłącznej.

Konstruujemy działanie na zbiorze $X_1 = \{x_1, x_2, x_3\}$. Wiemy, że $[G : G_{x_1}] = |G(x_1)| = 3$, skąd mamy $|G_{x_1}| = 2$. Szukamy podgrupy w S_3, która ma dwa elementy. Jest to na przykład $\langle(1\ 2)\rangle$. Chcemy aby ta podgrupa była stabilizatorem. Zdefiniujmy działanie $\sigma : S_3 \times (S_3/\langle(1\ 2)\rangle) \to S_3/\langle(1\ 2)\rangle$ wzorem $\sigma(g, h\langle(1\ 2)\rangle) = gh\langle(1\ 2)\rangle$. Wiemy, że $|S_3/\langle(1\ 2)\rangle| = 3$, zatem istnieje bijekcja $f_1 : X_1 \to S_3/\langle(1\ 2)\rangle$. Zdefiniujmy działanie $\psi_1 : G \times X_1 \to X_1$ wzorem

$$\psi_1(g, x_i) = f_1^{-1}(\sigma(g, f_1(x_i)) \in X_1$$

ψ_1 jest działaniem tranzytywnym S_3 na X_1.

Analogicznie konstruujemy działanie na zbiorze $X_2 = \{x_4, x_5, x_6\}$. Mamy $\psi_2 : G \times X_2 \to Y$

$$\psi_2(g, x_i) = f_2^{-1}(\sigma(g, f_2(x_i)) \in X_2$$

gdzie f_2 to bijekcja między zbiorami X_2 i $S_3/\langle(1\ 2)\rangle$. ψ_2 to działanie tranzytywne S_3 na X_2.

Dalej określamy $\psi_3 : G \times \{x_7\} \to \{x_7\}$ określone wzorem $\psi_3(g, x_7) = x_7$ oraz $\psi_4 : G \times \{x_8\} \to \{x_8\}$ określone wzorem $\psi_4(g, x_8) = x_8$. Na koniec $\psi : S_3 \times X \to X$ określamy wzorem

$$\psi(g, x) = \begin{cases} \psi_1(g, x) & \text{dla } x \in \{x_1, x_2, x_3\} \\ \psi_2(g, x) & \text{dla } x \in \{x_4, x_5, x_6\} \\ \psi_3(g, x) & \text{dla } x = x_7 \\ \psi_4(g, x) & \text{dla } x = x_8 \end{cases}$$

b) Trzecią orbitą będzie $G(x_1) = \{x_1, x_2, x_3, x_4, x_5, x_6\}$. Skonstruujmy więc działanie na zbiorze $X_1\{x_1, x_2, x_3, x_4, x_5, x_6\}$. Wiemy, że $[G : G_{x_1}] = |G(x_1)| = 6$, zatem $|G_{x_1}| = 1$, skąd $G_{x_1} = id$. Istnieje bijekcja $f_1 : X_1 \to S_3/\{id\}$, ponieważ $|X_1| = |S_3/\{id\}| = |S_3| = 6$. Ponadto działanie $\sigma : G \times (S_3/\{id\}) \to S_3/\{id\}$ określone wzorem $\sigma(g, h\{id\}) = \sigma(g, h) = gh\{id\} = gh$ jest tranzytywne. Zdefiniujmy więc działanie $\varphi : G \times X_1 \to X_1$ wzorem

$$\varphi(g, x) = f_1^{-1}(\sigma(g, f_1(x)))$$

Niech teraz $\psi : G \times X \to X$ zadane będzie wzorem

$$\psi(g, x) = \begin{cases} x & \text{dla } x \in \{x_7, x_8\} \\ \varphi(g, x) & \text{dla } x \in \{x_1, x_2, x_3, x_4, x_5, x_6\} \end{cases}$$

Twierdzenie: (Drugie twierdzenie o izomorfizmie) Niech $H, N \leq G$. Wówczas jeśli $N \triangleleft G$, to $H/(H \cap N) \simeq (HN)/N$.

Zadanie 3.
Niech $H \leq S_n$. Pokaż, że jeśli $H \not\leq A_n$, to $H \cdot A_n = S_n$ oraz $|H| = 2|H \cap A_n|$.

Rozwiązanie:
Wystarczy, że pokażemy że $H \cdot A_n$ zawiera wszystkie permutacje parzyste i wszystkie permutacje nieparzyste. Skoro $1 \in H$, to $\{1\sigma \mid \sigma \in A_n\} = A_n \subseteq H \cdot A_n$, zatem musimy pokazać, że $H \cdot A_n$ zawiera wszystkie permutacje nieparzyste. Skoro $H \not\leq A_n$, to istnieje $h \in H \setminus A_n$ czyli permutacja nieparzysta. Wówczas w $H \cdot A_n$ zawiera się zbiór $\{h \cdot \sigma \mid \sigma \in A_n\}$. Pokażemy, że dowolną permutację nieparzystą możemy napisać w tej postaci. Niech $\tau \notin A_n$, wówczas $\tau = h \cdot (h^{-1} \cdot \tau)$. Wystarczy więc pokazać, że $h^{-1} \cdot \tau$ to permutacja parzysta. Ale skoro h jest nieparzyste to h^{-1} też jest nieparzyste i skoro τ jest nieparzyste to $h^{-1} \cdot \tau$ jest parzyste jako złożenie permutacji nieparzystej. Stąd wszystkie permutacje nieparzyste należą do $H \cdot A_n$. A stąd $H \cdot A_n = S_n$.

Z twierdzenia o izomorfizmie mamy

$$|H/(H \cap A_n)| = |(H \cdot A_n)/A_n| = |S_n/A_n| = \frac{n!}{\frac{n!}{2}} = 2$$

Zadanie 4.
Niech $\sigma \in A_n$. Pokaż, że

a) jeśli $C_{S_n}(\sigma) \not\leq A_n$, to klasa sprzężoności elementu σ w S_n jest równa klasie sprzężoności w A_n

b) jeśli $C_{S_n}(\sigma) \leq A_n$, to klasa sprzężoności elementu σ w S_n jest sumą dwóch różnych równolicznych klas sprzężoności w A_n.

Rozwiązanie:

a) Chcemy pokazać, że jeśli $C_{S_n}(\sigma) \not\leq A_n$, czyli $\{g \in S_n \mid g\sigma = \sigma g\} \not\leq A_n$ to wówczas klasa sprzężoności σ w S_n równa jest klasie sprzężoności σ w A_n, czyli $S_n(\sigma) = A_n(\sigma)$. Mamy $S_n(\sigma) = \{g\sigma g^{-1} \mid g \in S_n\}$ oraz $A_n(\sigma) = \{g\sigma g^{-1} \mid g \in A_n\}$, zatem $A_n(\sigma) \subseteq S_n(\sigma)$. Wiemy, że $|S_n(\sigma)| = [S_n : C_{S_n}(\sigma)] = \frac{|S_n|}{|C_{S_n}(\sigma)|}$ oraz $|A_n(\sigma)| = \frac{|A_n|}{|C_{A_n}(\sigma)|} = \frac{\frac{1}{2}|S_n|}{|C_{A_n}(\sigma)|}$. Skoro $C_{S_n}(\sigma) \not\leq A_n$, to $|C_{S_n}(\sigma)| = 2|C_{S_n}(\sigma) \cap A_n|$. Mamy $A_n \cap \{\tau \in S_n \mid \sigma\tau = \tau\sigma\} = \{\tau \in A_n \mid \sigma\tau = \tau\sigma\} = C_{A_n}(\sigma)$, zatem $|C_{S_n}(\sigma)| = 2|C_{A_n}(\sigma)|$. Stąd $|A_n(\sigma)| = \frac{\frac{1}{2}|S_n|}{\frac{1}{2}|C_{S_n}(\sigma)|} = \frac{|S_n|}{|C_{S_n}(\sigma)|} = |S_n(\sigma)|$. A stąd $A_n(\sigma) = S_n(\sigma)$.

b) Załóżmy, że $\sigma \in A_n$ oraz $C_{S_n}(\sigma) \leq A_n$. Wówczas $C_{S_n}(\sigma) = C_{A_n}(\sigma)$. Stąd $\frac{|A_n|}{|C_{A_n}(\sigma)|} = \frac{1}{2} \cdot \frac{|S_n|}{|C_{S_n}(\sigma)|}$. Zatem $S_n(\sigma) = A_n(\sigma) \cup X$, gdzie X to zbiór pozostałych elementów, przy czym $|A_n(\sigma)| = |X| = \frac{1}{2}|S_n(\sigma)|$. Pokażemy, że X tworzy klasę pewnego elementu w A_n. Weźmy dowolny element $\rho \in X$, wówczas $S_n(\rho) = S_n(\sigma)$, bo $\sigma \in S_n(\sigma)$ oraz $\rho \in S_n(\sigma)$. Pokażemy, że $C_{S_n}(\rho) \leq A_n$. Mamy $C_{S_n}(\rho) = \{\tau \in S_n \mid \tau\rho\tau^{-1} = \rho\}$. Skoro ρ i σ są ze sobą sprzężone w S_n, to istnieje $\alpha \in S_n$, że $\rho = \alpha\sigma\alpha^{-1}$ i skoro $\sigma \in A_n$, to $\rho \in A_n$. Dalej α nie może być parzyste, bo wówczas $\rho \in \{g\sigma g^{-1} \mid g \in A_n\} = A_n(\sigma)$. Zatem α jest nieparzyste. Dalej mamy $C_{S_n}(\rho) = \{\tau \in S_n \mid \tau\rho\tau^{-1} = \rho\} = \{\tau \in S_n \mid (\tau\alpha)\sigma(\tau\alpha)^{-1} = \rho\}$, czyli znów jeśli $\tau\alpha$ jest parzyste, to $\rho \in A_n(\sigma)$. Skąd $\tau\alpha$ jest nieparzyste, a skoro α jest nieparzyste, to τ musi być parzyste. Stąd $C_{S_n}(\tau) = \{\tau \in A_n \mid \tau\rho = \rho\tau\} \leq A_n$. Teraz skoro $C_{S_n}(\rho) \leq A_n$, to postępując analogicznie mamy $S_n(\rho) = A_n(\rho) \cup Y$, skąd jako, że $A_n(\sigma) \cap A_n(\rho) = \emptyset$ (bo klasy sprzężoności albo są sobie równe albo są rozłączne) mamy $S_n(\rho) = S_n(\sigma) = A_n(\sigma) \cup A_n(\rho)$.

Fakt: Jeśli grupa G działa na zbiorze X, to jeśli $y \in G(x)$, to $G_x = gG_yg^{-1}$ dla pewnego $g \in G$, gdzie $G_y = \{h \in G \mid \varphi(h, y) = y\}$ dla działania φ.

Twierdzenie: Jeśli G jest grupą abelową to

$$G \simeq \mathbb{Z}_{p_1^{\alpha_1}} \times \ldots \times \mathbb{Z}_{p_i^{\alpha_i}}$$

gdzie $\alpha_j \geq 1$ oraz p_j to liczby pierwsze niekoniecznie różne.

Zadanie 5.
Opisać wszystkie grupy abelowe rządu 100.

Rozwiązanie:
Mamy $|G| = 100 = 2^2 \cdot 5^2$, zatem jedną z grup będzie

$$G_1 = \mathbb{Z}_{100} = \mathbb{Z}_4 \times \mathbb{Z}_{25}$$

(bo wiemy, że jeśli $NWD(m, n) = 1$, to $\mathbb{Z}_{mn} = \mathbb{Z}_n \times \mathbb{Z}_m$). Innymi grupami są

$$G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times Z_5 \times \mathbb{Z}_5 \quad (= \mathbb{Z}_{10} \times \mathbb{Z}_{10} \text{ bo } \mathbb{Z}_2 \times \mathbb{Z}_5 = \mathbb{Z}_{10})$$

$$G_3 = \mathbb{Z}_4 \times Z_5 \times \mathbb{Z}_5$$

$$G_4 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times Z_{25}$$

Pokażemy, że grupy te nie są parami izomorficzne. W G_1 istnieje element rzędu 100, natomiast w pozostałych grupach taki element nie istnieje, ponieważ NWW elementów każdej z podgrup $\mathbb{Z}_2$ i $\mathbb{Z}_5$ jest mniejsze niż 100. W G_2 maksymalny rząd elementu wynosi 10, w G_3 maksymalny rząd elementu wynosi 20, natomiast w G_4 maksymalny rząd elementu to 50. Stąd grupy G_2, G_3 oraz G_4 są parami nieizomorficzne. Stąd wszystkie grupy abelowe rzędu 100 to G_1, G_2, G_3 i G_4.

Ćwiczenia 13

Definicja: Niech G to skończona grupa i p to liczba pierwsza dzieląca $|G|$. p-podgrupą Sylowa nazwiemy dowolną podgrupę rzędu p^m, gdzie p^{m+1} nie dzieli $|G|$.

Twierdzenie: (Sylowa) Jeśli G grupa skończona i p to liczba pierwsza, to

1. jeśli p^m dzieli $|G|$, to G zawiera podgrupę rzędu p^m. W szczególności, gdy p dzieli $|G|$, to G zawiera p-podgrupę Sylowa
2. jeśli P, Q są p-podgrupami Sylowa, to istnieje $x \in G$ takie, że $Q = xPx^{-1}$
3. niech n_p oznacza liczbę p-podgrup Sylowa w G. Wówczas n_p dzieli $|G|$ oraz $n_p \equiv 1 \mod p$

Zadanie 1.
Wyznacz postać i liczbę podgrup Sylowa w grupie

a) S_4

b) D_{2n}

Rozwiązanie:

a) Mamy $|S_4| = 4! = 2^3 \cdot 3$, stąd mamy 2-podgrupy Sylowa o rzędzie równym 8 oraz 3-podgrupy Sylowa o rzędzie równym 3. Jeśli n_2 to liczba 2-podgrup Sylowa, to $n_2 \mid 24$ oraz $n_2 \equiv 1 \mod 2$, skąd $n_2 = 3$ lub $n_3 = 1$. Jeśli n_3 to liczba 3-podgrup Sylowa to $n_3 \mid 24$ i $n_3 \equiv 1 \mod 3$, skąd $n_3 = 4$ lub $n_3 = 1$. 3-podgrupy Sylowa są generowane przez elementy rzędu 3 w S_4. Elementami rzędu 3 są $(\cdot\ \cdot\ \cdot)$, zatem 3-podgrupami Sylowa są

$$\langle(1\ 2\ 3)\rangle,\ \langle(1\ 2\ 4)\rangle,\ \langle(2\ 3\ 4)\rangle \text{ oraz } \langle(1\ 3\ 4)\rangle$$

Wyznaczmy teraz 2-podgrupy Sylowa. 2-podgrupy Sylowa to podgrupy rzędu 8 w S_4. Jedną z podgrup będzie $f(D_8)$, gdzie $f : D_8 \hookrightarrow S_4$ to

$$f(D_8) = \{id, (1\ 2\ 3\ 4), (1\ 3)(4\ 2), (4\ 3\ 2\ 1), (1\ 2)(3\ 4), (1\ 3), (1\ 4)(3\ 2), (2\ 4)\} \leq S_4$$

Ta podgrupa nie jest normalna, zatem $gHg^{-1} \neq H$ dla pewnego $g \in S_4$, zatem istnieje jeszcze co najmniej jedna 2-podgrupa Sylowa. Innymi 2-podgrupami Sylowa będą

$$\{id, (1\ 2\ 4\ 3), (1\ 4)(3\ 2), (3\ 4\ 2\ 1), (1\ 2)(3\ 4), (1\ 4), (1\ 3)(4\ 2), (2\ 3)\} \leq S_4$$

oraz

$$\{id, (1\ 3\ 2\ 4), (1\ 2)(4\ 3), (4\ 2\ 3\ 1), (1\ 3)(2\ 4), (1\ 2), (1\ 4)(3\ 2), (3\ 4)\} \leq S_4$$

Zadanie 2.
Oblicz liczbę p-podgrup Sylowa w grupie S_p, gdzie p jest liczbą pierwszą.

Rozwiązanie:
Wiemy, że jeśli n_p to liczba p-podgrup Sylowa, to $n_p \equiv 1 \mod p$ oraz $n_p \mid p!$. p-podgrupy Sylowa mają p elementów, ponieważ $p^2 \nmid p!$. Ponadto p-podgrupa Sylowa dla p będącego liczbą pierwszą jest cykliczna. Elementy rzędu p w S_p to cykle długości p. Cykli długości p w S_p jest $(p-1)!$. Jeśli σ jest cyklem długości p w S_p, to w $\langle\sigma\rangle \simeq \mathbb{Z}_p$ jest $p-1$ elementów rzędu p. Skoro każde dwie grupy generowane przez p-cykl mają trywialne przecięcie, to liczba różnych p-podgryp Sylowa to $n_p = \frac{(p-1)!}{(p-1)} = (p-2)!$.

Ciekawostka z teorii liczb: Z twierdzenia Sylowa wiemy, że $n_p = (n-2)! \equiv 1 \mod p$, czyli $(p-1)! \equiv p-1 \equiv -1 \mod p$ - to twierdzenie to twierdzenie Wilsona.

Fakt: P jest jedyną podgrupą Sylowa wtedy i tylko wtedy, gdy $P \triangleleft G$.

Zadanie 3.
Niech G będzie grupą rzędu 12. Udowodnić, że

a) jeśli 3-podgrupa Sylowa nie jest podgrupą normalną, to 2-podgrupa Sylowa jest podgrupą normalną. Czy jest to prawda dla grup rzędu 24?

b) jeśli grupa G nie jest przemienna i ma 12 elementów oraz jej 2-podgrupa Sylowa jest normalna to G jest izomorficzna z A_4.

Rozwiązanie:

a) Skoro 3-podgrupa Sylowa nie jest normalna, to istnieją co najmniej dwie 3-podgrupy Sylowa. Wiemy, że jeśli n_3 to liczba 3-podgrup Sylowa, to $n_3 \mid 12$ oraz $n_3 \equiv 1 \mod 3$, skąd $n_3 = 4$. Każde dwie podgrupy Sylowa są rzędu 3, zatem mają trywialne przecięcie. Stąd w G jest $2 \cdot 4 = 8$ elementów rzędu 3 oraz jeden element rzędu 1. Wiemy, że w G istnieje 2-podgrupa Sylowa, czyli grupa rzędu 4 (bo rząd to największa liczba 2^i taka, że $2^i \mid 12$). Stąd w G istnieje co najwyżej $12 - 9 = 3$ elementy rzędu 2 lub 4. Wiemy, że w dowolnej grupie rzędu 4 istnieją dokładnie 3 elementy rzędu 2 lub 4, skąd istnieje co najwyżej jedna podgrupa rzędu 4. Zatem istnieje dokładnie jedna podgrupa rzędu 4, czyli ta 2-podgrupa Sylowa jest normalna.

   Teza nie jest prawdziwa dla grup rzędu 24, ponieważ w S_3 istnieje 3-podgrupa Sylowa która nie jest normalna (bo liczba 3-podgrup Sylowa wynosi 4) oraz każda z 2-podgrup Sylowa nie jest normalna (bo liczba 2-podgrup Sylowa wynosi 3).

b) Mamy dokładnie jedną 2-podgrupę Sylowa (niech będzie to H_2) oraz jedną lub cztery 3-podgrupy Sylowa (niech będzie to H_3). Jeśli mamy jedną 3-podgrupę Sylowa, to jest ona normalna. Mamy więc $|G| = 12$, $|H_2| = 4$, $|H_3| = 3$ oraz $H_2, H_3 \triangleleft G$ i stąd $G = H_2 \times H_3$. Grupa H_2 jest przemienna bo jej rząd jest kwadratem liczby pierwszej. Grupa H_3 jest przemienna, bo jest izomorficzna z $\mathbb{Z}_3$. Stąd G jest przemienne. Mamy więc sprzeczność, czyli mamy cztery 3-podgrupy Sylowa. Niech X to zbiór tych podgrup $X = \{H_{3_1}, H_{3_2}, H_{3_3}, H_{3_4}\}$.

Rozpatrzmy działanie grupy G na zbiorze X przez sprzęganie, czyli $\varphi : G \times X \to X$ będzie zadane wzorem $\varphi(g, H_i) = gHg^{-1} \in X$. Działanie to zadaje homomorfizm $f : G \to S_X = S_4$. Pokażemy, że $\ker(f) = \{1_G\}$. Mamy $\ker(f) = \{g \in G \mid f(g)(H_i) = H_i\} = \{g \in G \mid \forall_{H_i} gH_ig^{-1} = H_i\} \ldots$ Stąd istnieje monomorfizm $f : G \to S_4$ oraz $f(G) \simeq G$ (bo $f(G) = \mathrm{im}(f) \simeq G/\ker(f) = G/\{id\} = G$). Dalej $f(G) \leq S_4$ oraz $|f(G)| = 12$. Wiemy także, że w G jest osiem elementów rzędu 3 (bo mamy cztery 3-podgrupy Sylowa, każda o rzędzie równym 3, czyli w każdej dwa elementy mają rząd 3 i podgrupy te mają trywialne przecięcie), skąd wszystkie permutacje będące 3-cyklem należą do $f(G)$. Składając odpowiednio dwa cykle długości trzy, możemy wygenerować wszystkie permutacje postaci $(\cdot\ \cdot)(\cdot\ \cdot)$, skąd jako, że $|f(G)| = 12$, to $f(G) = A_4$, a stąd $G \simeq A_4$.

Zadanie 4.
Jedynym automorfizmem grupy skończonej jest identyczność. Udowodnij, że jest to $\mathbb{Z}_2$ lub $\{e\}$.

Rozwiązanie:
Rozważmy dwa przypadki

1. Grupa G nie jest przemienna. Wiemy, że $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ oraz, że $\mathrm{Inn}(G) \simeq G/Z(G)$. Skoro G nie jest przemienna, to $G \neq Z(G)$, czyli $\mathrm{Inn}(G) \simeq G/Z(G) \neq \{id\}$ i wówczas $\mathrm{Aut}(G) \neq \{id\}$

2. Grupa G jest przemienna. Funkcja $\varphi : g \to g^{-1}$ jest bijekcją. Dalej mamy

$$\varphi(gh) = (gh)^{-1} = h^{-1}g^{-1} \overset{G \text{ jest przemienna}}{=} g^{-1}h^{-1} = \varphi(g) \cdot \varphi(h)$$

skąd φ jest izomorfizmem, czyli $\varphi \neq id$ oraz $\varphi \in \mathrm{Aut}(G)$. Skoro $\mathrm{Aut}(G) = \{id\}$, to $\forall_{g \in G} g^{-1} = g$, czyli $g^2 = 1$. Z klasyfikacji skończonych grup abelowych mamy

$$G \simeq \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{n \text{ razy}}$$

dla pewnego $n \in \mathbb{N} \cup \{0\}$. Skonstruujmy nietrywialny homomorfizm

$$\psi : \underbrace{\mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{n \text{ razy}} \to \underbrace{\mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{n \text{ razy}}$$

dla $n \geq 2$ wzorem

$$\psi(\varepsilon_1, \ldots, \varepsilon_n) = (\varepsilon_2, \ldots, \varepsilon_n, \varepsilon_1)$$

gdzie $\varepsilon_1 \in \{0, 1\}$. ψ jest oczywiście bijekcją oraz ψ jest homomorfizmem, bo zgadza się na współrzędnych. Jeśli $n \geq 2$, to homomorfizm nie jest trywialny i stąd $\mathrm{Aut}(G) \neq \{id\}$. Jeśli $G = \{id\}$, to oczywiście $\mathrm{Aut}(G) = \{id\}$. Jeśli $G = \mathbb{Z}_2$, to również $\mathrm{Aut}(G) = \{id\}$.

Ćwiczenia 14

Twierdzenie Niech G, G_1, G_2 będą grupami. Wówczas grupa G jest izomorficzna z grupą $G_1 \times G_2$ wtedy i tylko wtedy, gdy istnieją podgrupy normalne N_1 i N_2 grupy G takie, że

- $N_i \simeq G_i$
- $N_1 \cap N_2 = \{e\}$
- $G = N_1 N_2$

Wniosek: Niech G będzie skończoną grupą i niech $H, N \triangleleft G$. Jeśli $|H|$ i $|N|$ są względnie pierwsze oraz $|G| = |N| \cdot |H|$, to $G \simeq H \times N$.

Zadanie 1.
Niech $|G| = 20$ oraz niech H będzie podgrupą normalną rzędu 4. Pokaż, że G jest abelowa.

Rozwiązanie:
Wiemy, że $|G| = 20 = 2^2 \cdot 5$, zatem z twierdzenia Cauchy'ego wiemy, że istnieje podgrupa $N \simeq \mathbb{Z}_5$ rzędu 5. N jest 5-podgrupą Sylowa. Niech n_5 to liczba takich podgrup. Wówczas $n_5 \equiv 1 \mod 5$ oraz $n_5 \mid 20$, skąd $n_5 = 1$, czyli $N \triangleleft G$. Jeśli $x \in H \cap N$, to $o(x) \in \{1, 5\}$ oraz $o(x) \in \{1, 2, 4\}$, skąd $o(x) = 1$, czyli x to element neutralny. Ponadto $NH \leq G$ oraz $|NH| = 4 \cdot 5 = 20$, skąd $NH = G$, zatem $G \simeq N \times H$. Mamy $N \simeq \mathbb{Z}_5$ oraz $H \simeq \mathbb{Z}_4$ lub $H \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Każda z tych grup jest przemienna, zatem G jest przemienna.

Zadanie 2.
Udowodnij, że grupy $\mathbb{Z}_2 \times S_3$ oraz D_{12} są izomorficzne.

Rozwiązanie:
I sposób: Grupa S_3 jest izomorficzna z $\langle \sigma, \rho^2 \rangle$, natomiast $\mathbb{Z}_2$ jest izomorficzna z $\langle \rho^3 \rangle$. Podgrupa $\langle \sigma, \rho^2 \rangle \leq D_{12}$ jest podgrupą normalną, bo ma indeks równy 2, natomiast podgrupa $\langle \rho^3 \rangle \leq D_{12}$ jest podgrupą normalną bo jest to centrum tej grupy. Dalej $\langle \sigma, \rho^2 \rangle \cap \langle \rho^3 \rangle = \{id\}$ oraz $|D_{12}| = 12 = 6 \cdot 2 = |\langle \sigma, \rho^2 \rangle| \cdot |\langle \rho^3 \rangle|$, czyli skoro $\langle \sigma, \rho^2 \rangle \cdot \langle \rho^2 \rangle \subseteq D_{12}$ to $\langle \sigma, \rho^2 \rangle \cdot \langle \rho^3 \rangle = D_{12}$. Stąd mamy $D_{12} \simeq \langle \sigma, \rho^2 \rangle \times \langle \rho^3 \rangle \simeq S_3 \times \mathbb{Z}_2$.

II sposób: Skonstruujemy homomorfizm $f : D_{12} \to S_3$. D_{12} to izometria sześciokąta foremnego. W sześciokącie foremnym mamy trzy główne przekątne. Oznaczmy je jako $1, 2, 3$. Homomorfizm będzie mówił nam jak dla danej izometrii $g \in D_{12}$, jaka jest permutacja głównych przekątnych

$$f(g) = \text{ permutacja przekątnych}$$

Jądro tego homomorfizmu to $\ker(f) = \{id, \rho^3\} \simeq \mathbb{Z}_2$. Wiemy, że $\ker(f) \triangleleft D_{12}$. Z twierdzenia o izomorfizmie, wiemy że $D_{12}/\ker(f) \simeq \text{im}(f)$, ale skoro $|D_{12}/\ker(f)| = 6$, to f jest „na". Szukamy więc $H \leq D_{12}$ takiego, że $f|H$ jest różnowartościowa. Wtedy $H \simeq f(H) \simeq S_3$. Niech więc $H = \langle \sigma, \rho^2 \rangle = \{id, \sigma, \rho^2, \rho^4, \sigma\rho^2, \sigma\rho^4\}$. Skoro H nie jest przemienna, to jest izomorficzna z S_3.

H jest normalna w D_{12}, bo $[D_{12} : H] = 2$. Dalej $\langle \sigma, \rho^2 \rangle \cap \langle \rho^3 \rangle = \{id\}$ oraz $|D_{12}| = 12 = 6 \cdot 2 = |\langle \sigma, \rho^2 \rangle| \cdot |\langle \rho^3 \rangle|$, czyli skoro $\langle \sigma, \rho^2 \rangle \cdot \langle \rho^2 \rangle \subseteq D_{12}$ to $\langle \sigma, \rho^2 \rangle \cdot \langle \rho^3 \rangle = D_{12}$. Stąd mamy $D_{12} \simeq \langle \sigma, \rho^2 \rangle \times \langle \rho^3 \rangle \simeq S_3 \times \mathbb{Z}_2$.

Definicja: Komutatorem elementów $a, b \in G$ nazwiemy element $[a, b] = aba^{-1}b^{-1}$. Komutantem G' grupy G nazwiemy podgrupę generowaną przez wszystkie komutatory w G, czyli $G' = \langle [a, b] \mid a, b \in G \rangle$.

Twierdzenie: Niech G będzie grupę z komutantem G'. Wówczas

1. $G' \triangleleft G$
2. G/G' jest grupą abelową
3. Niech $N \triangleleft G$. Wtedy grupa G/N jest abelowa wtedy i tylko wtedy, gdy $G' \subseteq N$

Fakt: Jeśli mamy homomorfizm $f : G \to H$ oraz H jest przemienna, to wówczas $G' \subseteq \ker(f)$.

Wniosek: Komutant to najmniejsza podgrupa normalna taka, że iloraz jest grupą abelową.

Fakt: Dla każdego homomorfizmu $f : G \to H$ oraz $N \triangleleft G$ takiej, że $N \subseteq \ker(f)$, istnieje dokładnie jeden homomorfizm $\widetilde{f} : G/N \to H$ taki, że $\widetilde{f} \circ \pi = f$.

Zadanie 3.

a) Wyznacz komutant grupy D_{20}

b) Wyznacz liczbę homomorfizmów $D_{20} \to \mathbb{Z}_{26} \times \mathbb{Z}_{26}$

Rozwiązanie:

a) Weźmy $H = \langle \rho^2 \rangle$. Jest to podgrupa normalna w D_{20}, ponieważ jest to jedyna 5-podgrupa Sylowa w grupie D_{20}. Dalej mamy $|D_{20}/\langle \rho^2 \rangle| = 4 = 2^2$, zatem $D_{20}/\langle \rho^2 \rangle$ jest grupą przemienną, bo jej moc jest kwadratem liczby pierwszej. Stąd $D'_{20} \subseteq \langle \rho^2 \rangle$. Wiemy, że rząd podgrupy dzieli rząd grupy, zatem $|D'_{20}| \in \{1, 5\}$. Jeśli $D'_{20} = \{id\}$, to $D_{20}/D'_{20} = D_{20}$ a to nie jest grupa abelowa. Stąd $D'_{20} = \langle \rho^2 \rangle$.

b) Niech $|\hom(X \to Y)|$ to liczba homomorfizmów $X \to Y$. Wiemy że dla dowolnego homomorfizmu $f : D_{20} \to \mathbb{Z}_{26} \times \mathbb{Z}_{26}$ mamy $\langle \rho^2 \rangle \subseteq \ker(f)$, bo $\mathbb{Z}_{26} \times \mathbb{Z}_{26}$ jest przemienna. Dalej wiemy, że $|\hom(D_{20} \to \mathbb{Z}_{26} \times \mathbb{Z}_{26})| = |\hom(D_{20} \to \mathbb{Z}_{26})|^2$. Wiemy, że jeśli grupa H jest przemienna, to dowolny homomorfizm $\xi : G \to H$ faktoryzuje się przez iloraz G/G', gdzie G' jest komutantem grupy G. Stąd dla każdego $g : D_{20} \to \mathbb{Z}_{26}$ mamy $\langle \rho^2 \rangle \subseteq \ker(g)$. Z twierdzenia

o izomorfizmie wiemy, że istnieje dokładnie jeden homomorfizm $\widetilde{g} : D_{20}/\langle\rho^2\rangle \to \mathbb{Z}_{26}$. Dalej mamy $|D_{20}/\langle\rho^2\rangle| = 4$, czyli jest izomorficzne z $\mathbb{Z}_4$ lub z $\mathbb{Z}_2 \times \mathbb{Z}_2$, ale skoro w $D_{20}/\langle\rho^2\rangle$ nie ma elementu rzędu 4, to $D_{20}/\langle\rho^2\rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Stąd mamy

$$|\hom(D_{20} \to \mathbb{Z}_{26} \times \mathbb{Z}_{26})| = |\hom(D_{20} \to \mathbb{Z}_{26})|^2 = |\hom(\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_{26})|^2$$

Jako, że mamy $\mathbb{Z}_{26} = \mathbb{Z}_2 \times \mathbb{Z}_{13}$, to

$$|\hom(\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_{26})|^2 = (|\hom(\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2)| \cdot |\hom(\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_{13})|)^2$$

Jako, że $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$ oraz $|\mathbb{Z}_{13}| = 13$, to jedyny homomorfizm $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_{13}$ to homomorfizm trywialny, skąd

$$|\hom(\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_{26})|^2 = |\hom(\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2)|^2$$

Homomorfizmów $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$ jest 4, zatem

$$|\hom(D_{20} \to \mathbb{Z}_{26} \times \mathbb{Z}_{26})| = |\hom(\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2)|^2 = 4^2 = 16$$

bo każdy z generatorów $(1, 0)$ i $(0, 1)$ może przejść na dowolny element z $\mathbb{Z}_2$, co daje nam $2 \cdot 2 = 4$ możliwości.

Fakt: Jeśli $\varphi \in \hom(G \to H)$ oraz $NWD(|G|, |H|) = 1$, to φ jest homomorfizmem trywialnym i stąd $|\hom(G \to H)| = 1$.

Fakt: Niech G będzie grupą cykliczną rzędu n. Wówczas dla dowolnej liczby naturalnej k, dzielącej n, istnieje w grupie G dokładnie jedna podgrupa rzędu k.

Zadanie 4.
Niech G będzie skończoną grupą abelową. Wykaż, że G jest cykliczną p-podgrupą dla pewnej liczby pierwszej p wtedy i tylko wtedy, gdy dla dowolnych nietrywialnych podgrup F, H grupy G, zachodzi $F \cap H \neq \{e\}$.

Rozwiązanie:
Skoro G jest abelowa, to $G \simeq \mathbb{Z}_{p_1^{\alpha_1}} \times \ldots \times \mathbb{Z}_{p_n^{\alpha_n}}$.

$\Rightarrow$ Załóżmy, że $G \simeq \mathbb{Z}_{p^k}$. Przypuśćmy, że istnieją właściwe podgrupy F i H podgrupy G, takie że $F \cap H = \{e\}$. Niech $|F| = p^a$ oraz $|H| = p^b$, wówczas z twierdzenia Cauchy'ego istnieje $\alpha \in F$ takie że $o(\alpha) = p$ oraz istnieje $\beta \in H$ takie, że $o(\beta) = p$. Zatem $\langle\alpha\rangle \leq F$ oraz $\langle\beta\rangle \leq H$. Ale skoro w $\mathbb{Z}_{p^k}$ istnieje dokładnie jedna podgrupa rzędu p, to $\langle\alpha\rangle = \langle\beta\rangle$ i stąd $F \cap H \neq \{e\}$.

$\Leftarrow$ Załóżmy, że dla każdych F, H nietrywialnych podgrup G zachodzi $F \cap H \neq \{e\}$. Przypuśćmy nie wprost, że $n \geq 2$, wtedy $F = \mathbb{Z}_{p_1^{\alpha_1}} \times \{0\} \times \ldots \times \{0\}$ oraz $H = \{0\} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \{0\}$ są podgrupami w G. Wówczas $F \cap H = \{(0, \ldots, 0)\} = \{e\}$. Mamy więc sprzeczność, czyli $G \simeq \mathbb{Z}_{p^\alpha}$.

Ćwiczenia 15

Zadanie 1.
Które z poniższych grup są izomorficzne?

$$\mathbb{Z}_2 \times S_3, \quad \mathbb{Z}_2 \times \mathbb{Z}_6, \quad \mathbb{Z}_3 \times \mathbb{Z}_4, \quad D_{12}$$

Rozwiązanie:
Policzmy największy rząd elementów w każdej grupie. W $\mathbb{Z}_2 \times S_3$ będzie to 6, w $\mathbb{Z}_2 \times \mathbb{Z}_6$ będzie to 6, w $\mathbb{Z}_3 \times \mathbb{Z}_4$ będzie to 12, natomiast w D_{12} będzie to 6. Stąd $\mathbb{Z}_3 \times \mathbb{Z}_4$ nie jest izomorficzna z pozostałymi grupami. Dalej $\mathbb{Z}_2 \times \mathbb{Z}_6$ jest grupą abelową, zatem jako że pozostałe dwie nie są, to nie może być z nimi izomorifczna. Pokażemy, że $\mathbb{Z}_2 \times S_3$ jest izomorficzna z D_{12}. Mamy $S_3 \simeq D_6 \simeq \langle \sigma, \rho^2 \rangle$ (gdzie $\sigma, \rho \in D_{12}$), natomiast $\mathbb{Z}_2 \simeq \langle \rho^3 \rangle$. Podgrupa $\langle \sigma, \rho^2 \rangle \leq D_{12}$ jest podgrupą normalną, bo ma indeks równy 2, natomiast podgrupa $\langle \rho^3 \rangle \leq D_{12}$ jest podgrupą normalną bo jest to centrum tej grupy. Dalej $\langle \sigma, \rho^2 \rangle \cap \langle \rho^3 \rangle = \{id\}$ oraz $|D_{12}| = 12 = 6 \cdot 2 = |\langle \sigma, \rho^2 \rangle| \cdot |\langle \rho^3 \rangle|$, czyli skoro $\langle \sigma, \rho^2 \rangle \cdot \langle \rho^2 \rangle \subseteq D_{12}$ to $\langle \sigma, \rho^2 \rangle \cdot \langle \rho^3 \rangle = D_{12}$. Stąd mamy $D_{12} \simeq \langle \sigma, \rho^2 \rangle \times \langle \rho^3 \rangle \simeq S_3 \times \mathbb{Z}_2$.

Zadanie 2.
Pokaż, że grupa addytywna liczb wymiernych $\mathbb{Q}$ nie jest iloczynem prostym żadnych dwóch swoich podgrup właściwych.

Rozwiązanie:
Załóżmy przeciwnie, że $\mathbb{Q} \simeq A \times B$, wówczas niech $\frac{m}{n} \in A$ oraz niech $\frac{p}{q} \in B$. Skoro A i B to podgrupy, to

$$\underbrace{\frac{m}{n} + \ldots + \frac{m}{n}}_{p \cdot n \text{ razy}} = m \cdot p \in A$$

oraz

$$\underbrace{\frac{p}{q} + \ldots + \frac{p}{q}}_{q \cdot m \text{ razy}} = m \cdot p \in B$$

Stąd $m \cdot p \in A \cap B$. Dalej mamy $|A \cdot B| = \frac{|A| \cdot |B|}{|A \cap B|} \neq |A| \cdot |B| = |\mathbb{Q}|$. Zatem $\mathbb{Q}$ nie może być iloczynem prostym żadnych dwóch swoich podgrup właściwych.

Zadanie 3.
Czy grupy $\mathrm{Aut}(\mathbb{Z}_8)$ i $\mathrm{Aut}(\mathbb{Z}_{10})$ są izomorficzne? Wskaż, o ile istnieją, dwie podgrupy właściwe H, F w $\mathrm{Aut}(\mathbb{Z}_8)$ takie, że $\mathrm{Aut}(\mathbb{Z}_8) = F \times H$.

Rozwiązanie:
Elementami rzędu 8 w grupie $\mathbb{Z}_8$ są $1, 3, 5, 7$, zatem $\mathrm{Aut}(\mathbb{Z}_8)$ ma 4 elementy $\phi_1(1) = 1$, $\phi_2(1) = 3$, $\phi_3(1) = 5$ oraz $\phi_4(1) = 7$, przy czym $o(\phi_1) = 1$ oraz $o(\phi_2) = o(\phi_3) = o(\phi_4) = 2$. Elementami rzędu 10 w grupie $\mathbb{Z}_{10}$ są $1, 3, 7, 9$, zatem $\mathrm{Aut}(\mathbb{Z}_8)$ ma 4 elementy $\psi_1(1) = 1$, $\psi_2(1) = 3$, $\psi_3(1) = 7$ oraz $\psi_4(1) = 9$, przy czym $o(\psi_1) = 1$, $o(\psi_2) = o(\psi_3) = 4$ oraz $o(\psi_4) = 2$. Wiemy, że automorfizm zachowuje rzędy elementów, zatem jako, że rzędy elementów obu grup są różne, to $\mathrm{Aut}(\mathbb{Z}_8)$ i $\mathrm{Aut}(Z_{10})$ nie są izomorficzne.

Zauważmy, że $\phi_2 \circ \phi_3 = \phi_3 \circ \phi_2 = \phi_4$, bo $\phi_2(\phi_3(1)) = \phi_2(5) = 7$ oraz $\phi_3(\phi_2(1)) = \phi_3(3) = 7$. Zatem generatory $\mathrm{Aut}(\mathbb{Z}_8)$ to ϕ_2 oraz ϕ_3. Zauważmy też, że $\mathrm{Aut}(\mathbb{Z}_8) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, ponieważ $\mathrm{Aut}(\mathbb{Z}_8)$ ma trzy elementy rzędu 2. Weźmy więc $F = \{\phi_1, \phi_2\}$ oraz $H = \{\phi_1, \phi_3\}$, wówczas

$$F \times H = \{\phi_1, \phi_2, \phi_3, \phi_2 \circ \phi_3 = \phi_4\} = \mathrm{Aut}(\mathbb{Z}_8)$$

Zadanie 4.
Wykaż, że jeśli G jest grupą abelową rzędu 78, to G jest cykliczna.

Rozwiązanie:
Mamy $|G| = 78 = 3 \cdot 2 \cdot 13$, zatem z twierdzenia Cauchy'ego, w G istnieje element rzędu 2, 3 i 13. Niech $o(a) = 2$, $o(b) = 3$ oraz $o(c) = 13$. Wówczas oczywiście $abc \in G$ oraz $o(abc) = NWW(2, 3, 13) = 2 \cdot 3 \cdot 13 = 78$. Stąd w G istnieje element rzędu 78, czyli G jest cykliczna.

Zadanie 5.
Udowodnij, że jeśli G jest grupą rzędu 10 i G ma dokładnie jeden element rzędu 2, to G jest grupą cykliczną.

Rozwiązanie:
Mamy $|G| = 10 = 2 \cdot 5$, skąd w G istnieje podgrupa rzędu 5. Niech n_5 to liczba 5-podgrup Sylowa. Wówczas $n_5 \equiv 1 \mod 5$ oraz $n_5 \mid 10$, skąd $n_5 = 1$. Mamy więc jedną 2-podgrupę Sylowa $\langle a \rangle \simeq \mathbb{Z}_2$, zatem jest ona normalna oraz jedną 5-podgrupę Sylowa $\langle b \rangle \simeq \mathbb{Z}_5$, która również jest normalna. Dalej jeśli $x \in \langle a \rangle \cap \langle b \rangle$, to $o(x) \in \{1, 2\}$ oraz $o(x) \in \{1, 5\}$, bo moc elementu dzieli moc grupy, skąd $o(x) = 1$ czyli $x = 1$. Dalej $|\langle a \rangle| \cdot |\langle b \rangle| = |G|$, czyli mamy $G \simeq \langle a \rangle \times \langle b \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_5$. Teraz skoro $NWD(2, 5) = 1$, to $G \simeq \mathbb{Z}_{10}$.

Zadanie 6.
Niech $|G| = 20$ oraz niech H będzie podgrupą normalną rzędu 4. Pokaż, że G jest abelowa.

Rozwiązanie:
Mamy $|G| = 20 = 2^2 \cdot 5$, zatem z twierdzenia Cauchy'ego wiemy, że istnieje podgrupa rzędu 5. Jest to 5-podgrupa Sylowa. Mamy $n_5 \equiv 1 \mod 5$ oraz $n_5 \mid 20$, skąd $n_5 = 1$. Mamy więc grupy normalne $H \triangleleft G$ oraz $N \triangleleft G$, przy czym dodatkowo $N \simeq \mathbb{Z}_5$. Dalej jeśli $x \in H \cap N$, to $o(x) \in \{1, 2, 4\}$ oraz $o(x) \in \{1, 5\}$, skąd $x = 1$ i jako że $|H \cdot N| = 4 \cdot 5 = 20$, to $G \simeq H \times N$. Grupa N jest abelowa, bo jest cykliczna, natomiast H jest izomorficzna z $\mathbb{Z}_2 \times \mathbb{Z}_2$ lub $\mathbb{Z}_4$, zatem też jest abelowa. Stąd G również jest przemienna.

Zadanie 7.
Grupa kwaternionów to grupa $H = \{1, -1, i, -i, j, -j, k, -k\}$, w której działanie zdefiniowane jest przez warunki:

$$1 \cdot x = x \cdot 1 = x, \quad (-1) \cdot x = x \cdot (-1) = -x,$$

$$i \cdot j = k = j \cdot (-i), \quad j \cdot k = i = k \cdot (-j), \quad k \cdot i = j = i \cdot (-k), \quad i^2 = j^2 = k^2 = -1$$

Pokaż, że $F = \{1, -1\}$ jest podgrupą normalną w H. Z którą z grup $\mathbb{Z}_2 \times \mathbb{Z}_2$ lub $\mathbb{Z}_4$ jest izomorficzna grupa H/F?

Rozwiązanie:
Dla dowolnego $g \in Q_8$ mamy

$$gF = \{g, -g\} = Fg$$

zatem F jest podgrupą normalną. Dalej mamy

$$H/F = \{F = \{1, -1\}, iF = \{i, -i\}, jF = \{j, -j\}, kF = \{k, -k\}\}$$

oraz $o(F) = 1$, $o(iF) = 2$, bo $i^2 = -1 \in F$, $o(jF) = 2$, bo $j^2 = -1 \in F$ oraz $o(kF) = 2$, bo $k^2 = -1 \in F$. Stąd oczywiście $H/F \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Zadanie 8.
Wykaż, że grupa $\mathbb{Q}/\mathbb{Z}$ jest izomorficzna z grupą F wszystkich pierwiastków zespolonych z 1 (wszystkich możliwych stopni) względe działania mnożenia.

Rozwiązanie:
Niech G to grupa wszystkich pierwiastków zespolonych z 1 wszystkich możliwych stopni. Dowolny element $\in \mathbb{Q}/\mathbb{Z}$ możemy napisać w postaci $q + \mathbb{Z}$, gdzie $q \in [0, 1) \cap \mathbb{Q}$.

Elementy grupy G są postaci

$$\cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right)$$

gdzie n to stopień pierwiastka, a $k \in \{0, 1, \ldots, n-1\}$ to k-ty pierwiastek danego stopnia. Zauważmy teraz, że dla każdej liczby $q \in [0, 1) \cap \mathbb{Q}$ możemy przedstawić ją w postaci $\frac{k}{n}$, gdzie n to liczba naturalna oraz $k \in \{0, 1, \ldots, n-1\}$.

Rozważmy więc funkcję $f : \mathbb{Q}/\mathbb{Z} \to G$ zadaną wzorem $f(q + \mathbb{Z}) = \cos(2q\pi) + i \sin(2q\pi)$ dla $q \in [0, 1) \cap \mathbb{Q}$. Pokażemy, że funkcja ta jest izomorfizmem.

- Funkcja ta jest homomorfizmem, ponieważ

$$\begin{aligned} f((q_1 + \mathbb{Z}) + (q_2 + \mathbb{Z})) &= f((q_1 + q_2) + \mathbb{Z}) = \cos(2(q_1 + q_2)\pi) + i \sin(2(q_1 + q_2)\pi) = \\ &= (\cos(2q_1\pi)\cos(2q_2\pi) - \sin(2q_1\pi)\sin(2q_2\pi)) + \\ &\quad + (i \sin(2q_1\pi)\cos(2q_2\pi) + i \cos(2q_1\pi)\sin(2q_2\pi)) = \\ &= (\cos(2q_1\pi) + i \sin(2q_1\pi)) \cdot (\cos(2q_2\pi) + i \sin(2q_2\pi) = \\ &= f(q_1 + \mathbb{Z}) \cdot f(q_2 + \mathbb{Z}) \end{aligned}$$

- Funkcja ta jest różnowartościowa, ponieważ

$$f(q_1 + \mathbb{Z}) = f(q_2 + \mathbb{Z}) \Leftrightarrow \cos(2q_1\pi) + i \sin(2q_1\pi) = \cos(2q_2\pi) + i \sin(2q_2\pi) \Leftrightarrow$$

$$\Leftrightarrow \cos(2q_1\pi) = \cos(2q_2\pi) \ \wedge \ \sin(2q_1\pi) = \sin(2q_2\pi) \Leftrightarrow q_1 = q_2 \quad (\text{bo } q_1, q_2 \in [0, 1) \cap \mathbb{Q})$$

- Pokażemy, że $g(\cos(2q\pi) + i \sin(2q\pi)) = q + \mathbb{Z}$ jest funkcją odwrotną do f

$$g \circ f(q + \mathbb{Z}) = g(\cos(2q\pi) + i \sin(2q\pi)) = q + \mathbb{Z}$$

$$f \circ g(\cos(2q\pi) + i \sin(2q\pi)) = f(q + \mathbb{Z}) = \cos(2q\pi) + i \sin(2q\pi)$$

Zatem f jest izomorfizmem, czyli grupy $\mathbb{Q}/\mathbb{Z}$ oraz G są izomorficzne.

Zadanie 9.
Ile jest homomorfizmów $S_3 \to \mathbb{Z}_2 \times \mathbb{Z}_6$? Wyznacz jeden z nietrywialnych homomorfizmów.

Zadanie 10.
Niech

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid a, d \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R} \right\}$$

Niech

$$H = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \mid b \in \mathbb{R} \right\}$$

Udowodnij, że

a) H jest podgrupą normalną w grupie G (w której działaniem jest mnożenie macierzy)

b) $G/H \simeq \mathbb{R}^* \times \mathbb{R}^*$, gdzie $\mathbb{R}^*$ oznacza multiplikatywną grupę ciała liczb rzeczywistych.

Zadanie 11.
W grupie S_{12} dane są dwa elementy σ_1, σ_2 rzędu 21. Udowodnij, że są one w tej grupie sprzężone, czyli $\sigma_1 = \tau\sigma_2\tau^{-1}$ dla pewnego $\tau \in S_{12}$.

Rozwiązanie:
Jeśli rozłożymy $\sigma \in S_{12}$ na cykle parami rozłączne, to rząd elementu to NWW z rzędów poszczególnych cykli. Mamy $21 = 7 \cdot 3$, zatem σ_1 to iloczyn cyklu długości 3 i cyklu długości 7. Również σ_2 to iloczyn cyklu długości 3 i cyklu długości 7. Skoro cykle są parami rozłączne, to są przemienne. Dalej wiemy, że dwa elementy w S_n są ze sobą sprzężone, jeśli mają taki sam rozkład na cykle. Stąd σ_1 i σ_2 są ze sobą sprzężone.

Zadanie 12.
Wskaż element maksymalnego rzędu w grupie S_6.

Rozwiązanie:
Musimy znaleźć taki rozkład na cykle, że NWW długości cykli jest największy. Elementem maksymalnego rzędu będzie więc $(\cdot\ \cdot\ \cdot)(\cdot\ \cdot)$.

Zadanie 13.
Dana jest permutacja $\sigma \in A_n$. Wyznacz centralizator oraz klasę sprzężoności elementu σ w grupie S_n i A_n dla $\sigma_1 = (1\ 2\ 3\ 4\ 5) \in A_5$ oraz $\sigma_2 = (1\ 2)(3\ 4) \in A_4$.

Rozwiązanie:
Wyznaczmy centralizatory w każdej grupie.

Wyznaczmy centralizator σ_1 w S_5. Wiemy, że $[S_5 : C_{S_5}(\sigma_1)] = |S_5(\sigma_1)| = 4!$, skąd $|C_{S_5}(\sigma_1)| = \frac{5!}{4!} = 5$. Dalej mamy $\langle\sigma_1\rangle \subset C_{S_5}(\sigma_1)$, bo $\sigma_1^i \cdot \sigma_1 \cdot \sigma_1^{-i} = \sigma_1$. Ale jako, że $|\langle\sigma_1\rangle| = 5$, to $\langle\sigma_1\rangle = C_{S_5}(\sigma)$.

Wyznaczmy centralizator σ_1 w A_5. Wiemy, że $C_{A_5}(\sigma_1) \subseteq C_{S_5}(\sigma_1)$, bo $A_5 \subseteq S_5$. Mamy również $\sigma_1 \in A_5$, skąd $\langle\sigma_1\rangle \subseteq C_{A_5}(\sigma_1)$, czyli $C_{A_5}(\sigma_1) = \langle\sigma_1\rangle$.

Wyznczmy centralizator σ_2 w S_4. Wiemy, że $[S_4 : C_{S_4}(\sigma_2)] = |S_4(\sigma_2)| = 3$, skąd $|C_{S_4}(\sigma_2)| = \frac{4!}{3} = 8$. Mamy $C_{S_4}(\sigma_2) = \{g \in S_4 \mid g\sigma_2 g^{-1} = \sigma_2\}$. W szczególności jeśli $\sigma_2 = (1\ 2)(3\ 4)$, to $g\sigma_2 g^{-1} = (g(1)\ g(2))(g(3)\ g(4))$. Będziemy więc przeprowadzać pary elementów na pary elementów

$$\begin{array}{r|cccccccc} g(1) = & 1 & 2 & 1 & 2 & 3 & 4 & 3 & 4 \\ g(2) = & 2 & 1 & 2 & 1 & 4 & 3 & 4 & 3 \\ g(3) = & 3 & 3 & 4 & 4 & 1 & 1 & 2 & 2 \\ g(4) = & 4 & 4 & 3 & 3 & 2 & 2 & 1 & 1 \end{array}$$

Otrzymujemy

$$C_{S_4}(\sigma_2) = \{id, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4\ 2\ 3), (1\ 3\ 2\ 4), (1\ 4)(2\ 3)\}$$

Wyznaczmy centralizator σ_2 w A_4. Wiemy, że $C_{A_4}(\sigma_2) \subseteq C_{S_4}(\sigma_2)$, ponadto elementy zbioru $C_{A_4}(\sigma_2)$ to permutacje parzyste, zatem

$$C_{A_4}(\sigma_2) = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Wyznaczmy klasy sprzężoności w każdej grupie.

Wyznaczmy klasy sprzężoności σ_1 w S_5. Są to te elementy, które mają jednakowy rozkład na cykle co σ_1. Jest ich $\frac{5!}{5} = 4! = 24$.

Wyznaczmy klasy sprzężoności σ_1 w A_5. Jest ich $|A_5(\sigma_1)| = [A_5 : C_{A_5}(\sigma_1)] = \frac{\frac{5!}{2}}{5} = 12$.

Zadanie 14.
Rozpatrujemy wszystkie działania grupy G rzędu 27 na zbiorze X mocy 32. Jaka może być minimalna liczba punktów stałych? Zdefiniuj to działanie.

Rozwiązanie:
Wiemy, że $|G| = 27$ oraz $|X| = 32$. Ponadto $|G(x)| \mid |G|$, czyli $|G(x)| \in \{1, 3, 9, 27\}$. Zauważmy, że rząd orbity jest potęgą trójki, a więc minimalna liczba punktów stałych to $32 \mod 3 = 2$. Niech $X = \{x_1, x_2, \ldots, x_{32}\}$ oraz niech x_1 i x_2 to punkty stałe, czyli $G(x_1) = \{x_1\}$ oraz $G(x_2) = \{x_2\}$. Niech działanie to ma pozostałe orbity o rzędach 27 i 3, czyli niech $|G(x_3)| = 27$ i $|G(x_{30})| = 3$. Konstruujemy działanie G na orbitach $X_1 = \{x_3, \ldots, x_{29}\}$ i $X_2 = \{x_{30}, x_{31}, x_{32}\}$. Na każdej orbicie działanie to jest tranzytywne. Aby skonstruować działanie G na X_1, to szukamy w G podgrup o indeksie równym $|X_1| = 27$. Jest to podgrupa trywialna. Istnieje więc bijekcja $f_1 : X_1 \to G/\{id\}$. Zdefiniujmy działanie $\varphi_1 : G \times G \to G$ wzorem $\varphi_1(g, h) = gh$, wówczas działanie $\psi_1 : G \times X_1 \to X_1$ będzie określone wzorem

$$\psi_1(g, x) = f_1^{-1}(\varphi_1(g, f_1(x)))$$

Skonstruujmy teraz działanie G na X_2. Szukamy w G podgrupy o indeksie równym $|X_2| = 3$. Niech N to ta podgrupa. Istnieje więc bijekcja $f_2 : X_2 \to G/N$. Zdefiniujmy działanie $\varphi_2 : G \times G/N \to G/N$ wzorem $\varphi_2(g, hN) = ghN$, wówczas działanie $\psi_2 : G \times X_2 \to X_2$ będzie określone wzorem

$$\varphi_2(g, x) = f_2^{-1}(\varphi_2(g, f_2(x)))$$

Wówczas działanie $\psi : G \times X \to X$ zdefiniujemy następująco

$$\psi(g, x) = \begin{cases} x & \text{dla } x \in \{x_1, x_2\} \\ \psi_1(g, x) & \text{dla } x \in X_1 \\ \psi_2(g, x) & \text{dla } x \in X_2 \end{cases}$$

Zadanie 15.
Czy istnieje działanie tranzytywne grupy $S_4 \times A_5$ na zbiorze X mocy 144?

Rozwiązanie:
Działanie tranzytywne to działanie mające jedną orbitę. Wiemy, że moc orbity dzieli moc grupy. Mamy $|S_4 \times A_5| = 4! \cdot \frac{5!}{2} = 1440$, zatem istnieje orbita o 144 elementach - jest to cały zbiór X. Stąd działanie takie istnieje.

Zadanie 16.
Podgrupy normalne N_1, N_2 skończonej grupy G spełniają $N_1 \cap N_2 = \{1\}$, zaś grupy ilorazowe G/N_1 i G/N_2 są cykliczne.

a) Pokaż, że grupa G jest izomorficzna z pewną podgrupą grupy $G/N_1 \times G/N_2$ i wywnioskuj, że G jest przemienna

b) Załóżmy dodatkowo, że indeksy podgrup N_1 i N_2 w grupie G są względnie pierwsze. Udowodnij, że G jest cykliczna.

Rozwiązanie:

a) Szukamy monomorfizmu $f : G \to G/N_1 \times G/N_2$. Mamy rzutowanie $\pi_i : G \to G/N_i$ dla $i = 1, 2$ zadane wzorem $\pi_i(g) = gN_i$. Niech więc $f : G \to G/N_1 \times G/N_2$ będzie zadane wzorem $f(g) = (gN_1, gN_2)$. Jest to homomorfizm. Dalej mamy

$$\ker(f) = \{g \in G \mid gN_1 = N_1 \ \wedge \ gN_2 = N_2\} = \{g \in G \mid g \in N_1 \ \wedge \ g \in N_2\} =$$

$$= \{g \in G \mid g \in N_1 \cap N_2\} = \{g \in G \mid g = 1\} = \{1\}$$

Stąd f jest monomorfizmem. Zatem

$$G \simeq G/\ker(f) \simeq f(G) \leq G/N_1 \times G/N_2$$

Dalej mamy $G/N_1 \simeq \mathbb{Z}_m$ oraz $G/N_2 \simeq \mathbb{Z}_n$, bo te grupy są przemienne. Mamy więc $G \leq \mathbb{Z}_m \times \mathbb{Z}_n$ i skoro $\mathbb{Z}_m \times \mathbb{Z}_n$ jest przemienna, to G też jest przemienne.

b) Niech $[G : N_1] = m$ oraz $[G : N_2] = n$. Skoro $NWD(m, n) = 1$ to mamy $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{nm}$, ale wówczas skoro $G/N_1 \times G/N_2 \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, to $G/N_1 \times G/\mathbb{Z}_n \simeq \mathbb{Z}_{mn}$. Grupa $G/N_1 \times G/N_2$ jest więc cykliczna, skąd jako że każda jej podgrupa jest cykliczna, to G również jest cykliczna.

Zadanie 17.
W grupie G dana jest podgrupa normalna H oraz podgrupa F. Pokaż, że

a) HF jest podgrupą w G

b) H jest podgrupą normalną w HF

c) $F \cap H$ jest podgrupą normalną w F

d) $(HF)/H \simeq F/(F \cap H)$

Rozwiązanie:

a) Mamy

$$HF = \{h \cdot f \mid h \in H,\ f \in F\}$$

Dalej niech $a \in HF$, czyli $a = h_1 \cdot f_1$ oraz niech $b \in HF$, czyli $b = h_2 \cdot f_2$. Wówczas

$$a \cdot b = h_1 \cdot f_1 \cdot h_2 \cdot f_2 = \underbrace{h_1}_{\in H} \cdot \underbrace{f_1 \cdot h_2 \cdot f_1^{-1}}_{\in H,\text{ bo } H \lhd G} \cdot \underbrace{f_1}_{\in F} \cdot \underbrace{f_2}_{\in F}$$

skąd jako, że $H \leq G$ i $F \leq G$ mamy $a \cdot b \in HF$. Dalej

$$a^{-1} = (h_1 \cdot f_1)^{-1} = f_1^{-1} \cdot h_1^{-1} = \underbrace{f_1^{-1} \cdot h_1^{-1} \cdot f_1}_{\in H,\text{ bo } H \lhd G} \cdot \underbrace{f_1^{-1}}_{\in F}$$

skąd jako, że $H \leq G$ i $F \leq G$ mamy $a^{-1} \in HF$.

b) Skoro $HF \leq G$ i skoro $\forall_{g \in G}\ \forall_{h \in H}\ ghg^{-1} \in H$, to również równość ta zachodzi dla każdego $g \in HF$, zatem $H \lhd HF$.

c) Chcemy pokazać, że $\forall_{g \in F}\ \forall_{h \in H \cap F}\ ghg^{-1} \in H \cap F$. Mamy $h \in H \cap F$, czyli w szczególności $h \in F$, skąd $ghg^{-1} \in F$. Dalej $H \lhd G$, czyli dla każdego $g \in G$ a w szczególności dla $g \in F$ oraz dla każdego $h \in H$ a w szczególności dla $h \in H \cap F$ mamy $ghg^{-1} \in H$. Stąd $ghg^{-1} \in H \cap F$, czyli $H \cap F \lhd F$.

Zadanie 18.
Załóżmy, że grupa G działa na zbiorze X. Załóżmy, że $G(x) = G(y)$ dla pewnych $x, y \in X$. Pokaż. że podgrupy G_x, G_y są sprzężone (to znaczy $gG_xg^{-1} = G_y$ dla pewnego $g \in G$), gdzie G_x to stabilizator elementu x.

Rozwiązanie:
Mamy $G(x) = \{\varphi(g, x) \mid g \in G\}$, $G(y) = \{\varphi(g, y) \mid g \in G\}$, $G_x = \{g \in G \mid \varphi(g, x) = x\}$ oraz $G_y = \{g \in G \mid \varphi(g, y) = y\}$. Mamy $y = \varphi(1, y) \in G(y)$, zatem skoro $G(x) = G(y)$, to istnieje $g \in G$ takie, że $\varphi(g, x) = y$. Teraz dla danego g ustalmy $h \in G_x$ (czyli $\varphi(h, x) = x$). Wówczas $ghg^{-1} \in gG_xg^{-1}$, bo $gG_xg^{-1} = \{ghg^{-1} \mid h \in G_x\}$. Dalej mamy

$$\varphi(ghg^{-1}, y) = \varphi(ghg^{-1}, \varphi(g, x)) = \varphi(ghg^{-1} \cdot g, x) = \varphi(gh, x) = \varphi(g, \varphi(h, x)) = \varphi(g, x) = y$$

Skąd $ghg^{-1} \in G_y$, czyli $gG_xg^{-1} \subseteq G_y$. Niech teraz $f \in G_y$ (czyli $\varphi(f, y) = y$), wówczas $g^{-1}fg \in g^{-1}G_yg$. Dalej mamy

$$\varphi(g^{-1}fg, x) = \varphi(g^{-1}f, \varphi(g, x)) = \varphi(g^{-1}f, y) = \varphi(g^{-1}, \varphi(f, y)) =$$

$$= \varphi(g^{-1}, y) = \varphi(g^{-1}, \varphi(g, x)) = \varphi(g^{-1} \cdot g, x) = \varphi(1, x) = x$$

Zadanie 19.
Niech G będzie grupą skończoną, a X niech będzie zbiorem wszystkich podgrup grupy G. Dla każdego $g \in G$ definiujemy funkcję $\varphi_g : X \to X$ wzorem $\varphi_g(H) = gHg^{-1}$, dla $H \in X$. Wykaż, że

definiuje to działanie grupy G na zbiorze X. Wykaż, że jeśli G jest p-grupą skończoną (dla pewnej liczby pierwszej p), to liczba podgrup G nie będących podgrupami normalnymi w G jest podzielna przez p.

Zadanie 20.
Załóżmy, że grupa $G/Z(G)$ jest cykliczna. Pokaż, że G jest abelowa.

Rozwiązanie:
Wiemy, że $G/Z(G)$ jest cykliczna. Chcemy pokazać, że G jest przemienna. Skoro $G/Z(G)$ jest cykliczna, to istnieje $g \in G$ takie, że $G/Z(G) = \langle gZ(G)\rangle$, zatem dla $x, y \in G/Z(G)$ mamy $x = g^k Z(G)$ oraz $y = g^l Z(G)$. Czyli dla każdego $x', y' \in G$ mamy $x' = g^k \cdot z_1$ i $y' = g^l \cdot x_2$, gdzie $z_1, z_2 \in Z(G)$. Mamy $z_1 \cdot z_2 \in Z(G)$, bo $Z(G)$ jest podgrupą. Ponadto skoro $z_1, z_2 \in Z(G)$ to są przemienne z dowolnym elementem z G, czyli

$$x'y' = g^k \cdot z_1 \cdot g^l \cdot z_2 = g^k \cdot g^l \cdot z_1 \cdot z_2 = g^{k+l} \cdot z_1 \cdot z_2$$

analogicznie

$$y'x' = g^l \cdot z_2 \cdot g^k \cdot z_1 = g^l \cdot g^k \cdot z_2 \cdot z_1 = g^{k+l} \cdot z_1 \cdot z_2$$

czyli $x'y' = y'x'$, czyli G jest przemienna.

TEORIA PIERŚCIENI

Ćwiczenia 16

Definicja: Pierścieniem nazywamy niepusty zbiór R z dwoma 2-argumentowymi działaniami $+$, $\cdot$, zwanymi dodawaniem i mnożeniem odpowiednio, spełniającymi warunki

1. $(R, +)$ jest grupą abelową
2. $(R, \cdot)$ jest półgrupą (czyli zbiór z działaniem łącznym)
3. mnożenie jest rozdzielne względem dodawania, to znaczy dla dowolnych $a, b, c \in R$

$$a(b+c) = ab + ac \qquad (b+c)a = bc + ca$$

R jest pierścieniem z jedynką, jeżeli $(R, \cdot)$ jest monoidem, czyli istnieje $e \in R$ takie że dla każdego $a \in R$ mamy $a \cdot e = e \cdot a = a$. Mówimy, że R jest pierścieniem przemiennym jeżeli mnożenie w R jest przemienne, czyli dla dowolnych $a, b \in R$ mamy $ab = ba$.

Definicja: Element $x \in R$ nazywamy dzielnikiem zera wtedy i tylko wtedy, gdy istnieje element niezerowy $y \in R$, dla którego $xy = 0$. Element $x \in R$ nazywamy odwracalnym wtedy i tylko wtedy, gdy istnieje element $y \in R$, zwany odwrotnością elementu x, dla którego $xy = 1$. Zbiór elementów odwracalnych oznaczać będziemy jako $U(R)$. Element $x \in R$ nazywamy nilpotentnym jeżeli istnieje liczba całkowita dodatnia n dla której $x^n = 0$. Element $x \in R$ nazywamy idempotentnym jeśli $x^2 = x$.

Przykłady:

- Dowolne ciało K jest pierścieniem przemiennym z jedynką, na przykład $(\mathbb{C}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$
- Pierścień liczb całkowitych $(\mathbb{Z}, +, \cdot)$
- Pierścień reszt modulo $(\mathbb{Z}_n, +, \cdot)$
- Zbiór wszystkich macierzy $n \times n$ o współczynnikach w ciele K jest pierścieniem $(M_n(K), +, \cdot)$ - jest to pierścień nieprzemienny
- Pierścień macierzy ściśle górnotrójkątnych $(T_n(K), +, \cdot)$, gdzie $T_n(K) = \left\{ \begin{bmatrix} 0 & * \\ 0 & 0 \end{bmatrix} \in M_n(K) \right\}$ - jest to pierścień nieprzemienny bez jedynki
- Pierścień wielomianów $R[x] = \{v_0 + v_1 x + \ldots + v_n x^n \mid v_i \in \mathbb{R}\}$. Jedynką jest $f \equiv 1$. Stopień wielomianu $\deg(f)$ to największe n takie, że $v_n \neq 0$ lub $-\infty$ jeśli $f \equiv 0$. Działania w tym pierścieniu to

$$(v_0 + v_1 x + \ldots) + (w_0 + w_1 x + \ldots) = (v_0 + w_0) + (v_1 + w_1)x + \ldots$$

oraz

$$(v_0 + v_1 x + \ldots) \cdot (w_0 + w_1 x + \ldots) = v_0 w_0 + (v_1 w_0 + v_0 w_1)x + \ldots$$

czyli przy x^n mamy $\sum_{i=0}^{n} v_i w_{n-i}$.

- Pierścień szeregów formalnych $R[[x]] = \left\{ \sum_{i=0}^{\infty} v_i x^i \mid v_i \in \mathbb{R} \right\}$

Zadanie 1.
Znajdź elementy odwracalne, dzielniki zera i nilpotenty w $\mathbb{Z}_n$.

Rozwiązanie:
Element $a \in \mathbb{Z}_n$ jest odwracalny wtedy i tylko wtedy, gdy istnieje $b \in \mathbb{Z}_n$ taki że $ab = 1$. Pokażemy, że elementy odwracalne w $\mathbb{Z}_n$ to takie elementy $a \in \mathbb{Z}_n$, że $NWD(a, n) = 1$. Jeśli $NWD(a, n) = 1$, to z algorytmu Euklidesa wiemy, że istnieje $\alpha, \beta \in \mathbb{Z}$ takie że $\alpha \cdot a + n \cdot \beta = 1$ czyli elementem odwrotnym do a będzie $b = \alpha \mod n$. Załóżmy, że a jest elementem odwracalnym w $\mathbb{Z}_n$ oraz $NWD(a, n) = k > 1$. Niech $a = ka'$ oraz $n = kn'$. Wówczas skoro a jest odwracalne, to istnieje $b \in \mathbb{Z}$ takie, że $a \cdot b \equiv 1 \mod n$, czyli $ka' \cdot b \equiv 1 \mod kn'$, skąd $ka' \cdot b + kn' \cdot \beta = 1$ dla pewnego β. Lewa strona jest podzielna przez k, natomiast prawa nie dzieli się przez k, czyli mamy sprzeczność.

Element a jest dzielnikiem zera w $\mathbb{Z}_n$ jeśli istnieje $b \neq 0$ taki że $a \cdot b \equiv 0 \mod n$. Pokażemy, że dzielniki zera w $\mathbb{Z}_n$ to takie elementy $a \in \mathbb{Z}_n$, że $NWD(a, n) \neq 1$. Niech $NWD(a, n) = k$, wówczas $k \mid n$, czyli istnieje element b taki że $b \cdot k = n$. Wówczas $a \cdot b = a \cdot \frac{n}{k} = \frac{a}{k} \cdot n = 0$. Niech $a \in \mathbb{Z}_n$ będzie elementem takim, że $NWD(a, n) = 1$. Wówczas wiemy, że a jest odwracalny w $\mathbb{Z}_n$, czyli istnieje b takie że $ba = 1$. Załóżmy, że a jest dzielnikiem zera, czyli istnieje $c \in \mathbb{Z}_n$ takie, że $ac = 0$. Mamy więc $c = 1 \cdot c = ba \cdot c = b \cdot ac = b \cdot 0 = 0$.

Element $a \in \mathbb{Z}_n$ nazywamy nilpotentnym jeżeli istnieje liczba całkowita dodatnia m dla której $a^m = 0$. Jeśli element a jest nilpotentny to jest on dzielnikiem zera w $\mathbb{Z}_n$. Niech $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Pokażemy, że elementem nilpotentnym w $\mathbb{Z}_n$ będzie element postaci $p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k} \cdot N$ dla dowolnego $N \in \mathbb{Z}$, gdzie $0 < \beta_i \leq \alpha_i$. Jest to element nilpotentny, bo $p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \mid p_1^{\beta_1 \cdot m} \cdot \ldots \cdot p_k^{\beta_k \cdot m} \cdot N^m$ dla na przykład $m = NWW(\alpha_1, \ldots, \alpha_k)$. Niech a nie będzie postaci $p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k} \cdot N$, czyli $p_1 \cdot \ldots \cdot p_k \not| \, a$. Niech bez straty ogólności $p_1 \not| \, a$, wówczas nie istnieje m takie, że $a^m = 0$, bo a^m nie będzie podzielne przez $p_1^{\alpha_1}$.

Fakt: Elementy odwracalne w R nie są dzielnikami zera.

Definicja: Powiemy, że R jest dziedziną jeśli R nie zawiera właściwych, to znaczy różnych od 0 dzielników zera.

Przykłady:

- Dowolne ciało
- Pierścień liczb całkowitych

Fakt: Jeśli R jest dziedziną to $R[x]$ (lub $R[[x]]$) też jest dziedziną.

Zadanie 2.
Pokaż, że R jest dziedziną wtedy i tylko wtedy, gdy zachodzi następujące prawo skracania. Jeśli $a \in R$ jest niezerowy oraz $ax = ay$, to $x = y$.

Rozwiązanie:
Niech $a \neq 0$, wówczas $ax = ay \Leftrightarrow a(x - y) = 0$. Jeśli R jest dziedziną, to $x - y = 0 \Leftrightarrow x = y$. Załóżmy, że jeśli $a \neq 0$ i $ax = ay$ to $x = y$. Niech $ab = 0$ i $a \neq 0$, wówczas $ab = a(b - 0)$, czyli $a \cdot b = a \cdot 0$, skąd $b = 0$. Zatem R jest dziedziną.

Fakt: Pierścień R przemienny z jedynką jest ciałem wtedy i tylko wtedy, gdy dowolny niezerowy element jest odwracalny.

Zadanie 3.
Przypuśćmy, że pierścień R jest skończony. Pokaż, że jest dziedziną wtedy i tylko wtedy, gdy jest ciałem.

Rozwiązanie:
Jeśli skończony pierścień R jest ciałem, to jest oczywiście dziedziną. Niech R będzie skończoną dziedziną, czyli $R = \{x_1, \ldots, x_k\}$. Weźmy $x \neq 0$ w R, wówczas $xR = \{xx_1, \ldots, xx_k\}$. Jeśli w xR występuje 1, to x jest odwracalny w R, bo $xx_l = 1$. Załóżmy więc że w xR nie ma jedynki, wówczas co najmniej dwa elementy są takie same, czyli $xx_i = xx_j$ dla $i \neq j$, skąd z własności skracania mamy $x_i = x_j$, wbrew temu, że elementy z R były różne. Stąd dowolny element $x \in R$ jest odwracalny w R, czyli R jest ciałem.

Definicja: Podpierścieniem pierścienia z jedynką R nazywamy podzbiór $P \subseteq R$ taki, że

- P jest podgrupą grupy addytywnej pierścienia R
- $1 \in P$
- $\forall_{a,b \in P}\ a \cdot b \in P$

Zadanie 4.
Czy A jest podpierścieniem w R?

a) $R = R[x]$, $A = \{f \in R[x] \mid f(1) = 0\}$

b) $R = \mathbb{Q}$, $A = \left\{\frac{m}{n} \in \mathbb{Q} \mid NWD(m, n) = 1,\ 2 \not| \ m\right\} \cup \{0\}$

Rozwiązanie:

a) Wiemy, że $1 \in R[x]$, jednak $1 \notin A$, skąd A nie jest podpierścieniem.

b) Mamy oczywiście $1 \in A$. Niech $\frac{n}{m} \in A$ oraz $\frac{n'}{m'} \in A$, wówczas $\frac{nn'}{mm'} \in A$ (oczywiście po skróceniu), bo 2 nie dzieli mm'. Sprawdźmy, czy $A \leq (\mathbb{Q}, +)$, czyli czy $\frac{n}{m} - \frac{n'}{m'} \in A$. Mamy $\frac{n}{m} - \frac{n'}{m'} = \frac{nm' - n'm}{mm'} \in A$. Stąd A jest podpierścieniem R.

Definicja: Podpierścień generowany przez zbiór Z to najmniejszy podpierścień S w R taki, że $Z \subseteq S$.

Zadanie 5.
Wyznacz podpierścień R generowany przez zbiór Z, gdzie $R = \mathbb{R}$, $Z = \{\sqrt{2}\}$.

Rozwiązanie:
Jeśli $\sqrt{2}, 1 \in S$, to $a + b\sqrt{2} \in S$ dla dowolnych $a, b \in \mathbb{Z}$. Zatem jeśli pokażemy, że zbiór $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ jest podpierścieniem, to jest podpierścień generowany przez zbiór Z. Oczywiście $1 \in \mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{2}]$ jest podgrupą oraz jeśli $(a + b\sqrt{2}), (c + d\sqrt{2}) \in Z[\sqrt{2}]$, to ich iloczyn też. Stąd $\mathbb{Z}[\sqrt{2}]$ jest podpierścieniem generowanym przez $\{\sqrt{2}\}$.

Zadanie 6.
Niech $R = \mathbb{Z}\left[\frac{1}{2}\right]$ będzie podzbiorem liczb wymiernych złożonych ze wszystkich liczb postaci $\frac{k}{2^l}$, gdzie $k \in \mathbb{Z}$, $l \in \mathbb{N}$. Sprawdź, że R jest podpierścieniem ciała $\mathbb{Q}$. Czy jest on ciałem? Czy jest on dziedziną? Znajdź elementy odwracalne.

Rozwiązanie:
Mamy $1 \in R$, $\frac{k}{2^l} \cdot \frac{k'}{2^{l'}} = \frac{kk'}{2^{l+l'}} \in R$ oraz $\frac{k}{2^l} - \frac{k'}{2^{l'}} = \frac{k-k'}{2^{l+l'}}$, czyli R jest podgrupą $\mathbb{Q}$. Stąd R jest podpierścieniem w $\mathbb{Q}$. Jest on generowany przez $\frac{1}{2}$. R nie jest ciałem, bo $\frac{3}{2} \in R$, ale $\frac{2}{3} \notin R$. Wiemy, że $\mathbb{Q}$ jest ciałem, czyli w szczególności jest dziedziną. Wiemy, że dowolny podzbiór dziedziny jest dziedziną. Stąd jako, że R jest podzbiorem $\mathbb{Q}$, to R jest dziedziną. Pokażemy, że elementy odwracalne w R należą do zbioru $U = \{\pm 2^k \mid k \in \mathbb{Z}\}$. Jest jasne, że takie elementy są odwracalne, bo $2^{-k} \in R$ oraz $2^k \cdot 2^{-k} = 1$. Weźmy $\frac{m}{2^l} \notin U$ takie, że $NWD(m, 2^l) = 1$ oraz $m \neq \pm 1$. Wówczas jeśli $\frac{m}{2^l}$ jest odwracalny, to istnieje $\frac{k}{2^j}$ takie, że $\frac{m}{2^l} \cdot \frac{k}{2^j} = 1$, czyli $m \cdot k = 2^{l+j}$, skąd $m \mid 2^{l+j}$, co jest sprzeczne z wyborem m. Stąd elementy odwracalne w R należą do zbioru U.

Ćwiczenia 17

Zadanie 1.
Niech R będzie pierścieniem, zaś $u \in R$ elementem odwracalnym oraz niech n będzie elementem nilpotentnym, czyli istnieje $k \in \mathbb{N}$ takie że $n^k = 0$.

a) Pokaż, że u^k jest odwracalny dla każdego $k \in \mathbb{N}$

b) Załóżmy, że $u = u_1 u_2$ dla pewnych $u_1, u_2 \in R$. Pokaż, że u_1, u_2 są odwracalne.

c) Pokaż, że $u + n$ jest odwracalny

Rozwiązanie:

a) Skoro u jest elementem odwracalnym, to istnieje $v \in R$ takie, że $uv = 1$. Mamy

$$u^k \cdot v^k \overset{R \text{ jest przemienny}}{=} (uv)^k = 1^k = 1$$

czyli u^k jest elementem odwracalnym, gdzie elementem odwrotnym jest v^k.

b) Niech $u \cdot v = 1$, wówczas $(u_1 u_2) \cdot v = 1$, czyli $u_1 \cdot (u_2 \cdot v) = 1$, skąd u_1 jest elementem odwracalnym. Analogicznie u_2 jest elementem odwracalnym.

c) Wystarczy, że znajdziemy element $v \in U(R)$ taki że $v = (u + n) \cdot w$ dla pewnego $w \in R$. Dla nieparzystego m mamy

$$u^m + n^m = (u + n)(u^{m-1} - u^{m-2}n + \ldots + n^{m-1})$$

Niech więc m będzie tak duże że $n^m = 0$, wówczas niech $v = u^m + n^m = u^m \in U(R)$ oraz niech $w = (u^{m-1} - u^{m-2}n + \ldots + n^{m-1})$. Dla tak dobranych v i w otrzymujemy, że $u + n \in U(R)$.

Fakt: Jeśli m i n to elementy nilpotentne w R, to $m + n$ również jest nilpotentem w R.
Dowód: Skoro m i n to elementy nilpotentne w R, to istnieje $k = \max(k_m, k_n)$ takie że $n^k = 0$ i $m^k = 0$. Dalej mamy

$$(n + m)^N = \sum_{i=0}^{N} \binom{N}{i} n^i m^{N-i}$$

Niech więc $N = 2k$, wówczas $(n + m)^N = 0$, czyli $n + m$ jest elementem nilpotentnym w R.

Zadanie 2.
Niech R będzie pierścieniem.

a) Uzasadnić, że jeśli R jest dziedziną, to $R[[x]]$ też jest dziedziną

b) Opisać elementy odwracalne w $R[[x]]$

c) Opisać elementy nilpotentne $R[x]$

d) Uzasadnić, że jeśli $a \in R$ jest elementem nilpotentnym, to $1+a$ jest elementem odwracalnym

e) Opisać elementy odwracalne w $R[x]$

Rozwiązanie:

a) Niech $u = \sum_{i=0}^{\infty} u_i x^i$ oraz $v = \sum_{j=0}^{\infty} v_j x^j$. Współczynnik przy x^n w $u \cdot v$ to $\sum_{k=0}^{n} u_k v_{n-k}$. Przypuśćmy, że $u \neq 0$ i $v \neq 0$, ale $u \cdot v = 0$. Istnieją więc l, m takie że $u_l \neq 0$ oraz $v_m \neq 0$, a stąd $u_l v_m \neq 0$. Weźmy więc najmniejsze $l \neq 0$ i $m \neq 0$ takie, że $u_l \neq 0$ i $v_m \neq 0$. Współczynnik przy x^{l+m} to $\sum_{k=0}^{l+m} u_k v_{m+l-k}$. Współczynnik ten jest niezerowy, bo dla $k = l$ mamy $u_l v_{m+l-l} = u_l v_m \neq 0$. Stąd $u \cdot v \neq 0$ co jest sprzeczne z założeniem.

b) Niech $u \in U(R[[x]])$ i $u = \sum_{i=0}^{\infty} u_i x^i$. Istnieje więc $v = \sum_{j=0}^{\infty} v_j x^j$ taki że $u \cdot v = 1$. Współczynnik przy x^n w $u \cdot v$ to $\sum_{k=0}^{n} u_k v_{n-k}$, czyli jeśli $u \cdot v = 1$, to $u_0 \cdot v_0 = 1$, skąd u_0 jest odwracalny w R. Pokażemy, że jeśli $u_0 \in U(R)$, to $u \in U(R[x])$. Skoro $u_0 \in U(R)$, to istnieje $v_0 \in R$ takie, że $u_0 v_0 = 1$. Niech $v_1 = -u_0^{-1}(u_1 \cdot v_0) = -u_0^{-2} u_1$, wówczas $u_0 v_1 + u_1 v_0 = 0$, a to jest współczynnik przy x^1 w $u \cdot v = 1$. Rekurencyjnie możemy więc wyznaczyć dowolne v_n, takie że $u_0 v_n + u_1 v_{n-1} + \ldots + u_n v_0 = 0$. Stąd istnieje v, zdefiniowany jako $\sum_{i=0}^{\infty} v_i x^i$ takie, że $u \cdot v = 1$. Zatem

$$U(R[[x]]) = \left\{ \sum_{i=0}^{\infty} u_i x^i \mid u_0 \in U(R) \right\}$$

c) Szukamy takich elementów $f \in R[x]$, że istnieje k dla którego $f^k = 0$. Niech $f = a_0 + a_1 x + \ldots + a_n x^n$ oraz $a_n \neq 0$. Jeśli $f^k = 0$, to $a_0^k = 0$ oraz $a_n^k = 0$, czyli a_0 i a_n to nilpotenty w R. Pokażemy, że elementy nilpotentne w $R[x]$ to takie wielomiany, których wszystkie współczynniki są nilpotentne w R. Niech $f = a_0 + a_1 x + \ldots + a_n x^n$ oraz niech a_i jest nilpotentny w R dla każdego i. Wystarczy, że pokażemy że $a_i x^i$ jest nilpotentem w $R[x]$. Wiemy, że a_i jest nilpotentem w R, czyli istnieje N takie że $a_i^N = 0$, stąd $(a_i x^i)^N = a_i^N x^{iN} = 0$, czyli rzeczywiście $a_i x^i$ jest elementem nilpotentnym. Stąd $f = a_0 + a_1 x + \ldots + a_n x^n$ jest nilpotentem w $R[x]$ jako suma elementów nilpotentnych. Niech teraz f będzie nilpotentem w $R[x]$. Stąd a_0 i a_n są nilpotentne. Pokażemy, że dla każdego i element a_i jest nilpotentny, stosując indukcję względem stopnia wielomianu. Jeśli $\deg(f) = 0$, to $f = a_0$, no a wiemy że a_0 jest nilpotentem. Dalej załóżmy, że jeśli $\deg(f) = n-1$, to dla każdego i elementy a_i są nilpotentne. Rozpatrzmy więc wielomian f taki, że $\deg(f) = n$, czyli $f = a_0 + a_1 x + \ldots + a_n x^n$. Wówczas wielomian $g = f - a_n x^n$ ma stopień mniejszy niż n oraz g jest nilpotentny w $R[x]$ (jako suma elementów nilpotentnych), czyli z założenia indukcyjnego wszystkie współczynniki są nilpotentne.

d) Element 1 jest odwracalny w $R[x]$, zatem jako, że a jest nilpotentny, to $1+a$ jest odwracalny.

e) Jeśli $f = \sum_{i=0}^{n} a_i x^i \in U(R[x])$, to istnieje $g = \sum_{j=0}^{k} b_j x^j$ takie, że $f \cdot g = 1$, czyli $a_0 b_0 = 1$, skąd $a_0 \in U(R)$. Wiemy, że jeśli $n \in U(R[x])$ oraz h jest nilpotentny, to $n + h \in U(R[x])$. Stąd $\{f = \sum_{i=0}^{n} a_i x^i \mid a_0 \in U(R),\ \forall_{i \geq 0} a_i \text{ jest nilpotentny}\}$ jest zawarty w $U(R[x])$. Pokażemy, że zachodzi równość. Niech $f = a_0 + a_1 x + \ldots + a_n x^n \in U(R[x])$, czyli istnieje $g = \sum_{j=0}^{k} b_j x^j$ takie, że $f \cdot g = 1$, stąd $a_0 \in U(R)$. Dalej

$$a_n b_k = 0$$

$$a_n b_{k-1} + a_{n-1} b_k = 0$$

$$a_n b_{k-2} + a_{n-1} b_{k-1} + a_{n-2} b_k = 0$$

$$\vdots$$

A stąd

$$a_n b_k = 0$$

$$a_n^2 b_{k-1} + a_{n-1} a_n b_k = 0$$

$$a_n^3 b_{k-2} + a_{n-1} a_n^2 b_{k-1} + a_{n-2} a_n^2 b_k = 0$$

$$\vdots$$

czyli

$$a_n b_k = 0$$

$$a_n^2 b_{k-1} = 0$$

$$a_n^3 b_{k-2} = 0$$

$$\vdots$$

Mamy więc $a_n^{k+1} b_0 = 0$, ale jako, że b_0 jest odwracalne, to $a_n^{k+1} = 0$, czyli a_n jest nilpotentem. Korzystając z indukcji po stopniu wielomianu pokażemy, że każdy współczynnik jest nilpotentem. Niech $g = f - a_n x^n$. Wiemy, że $a_n x^n$ jest nilpotentem oraz $f \in U(R[x])$, skąd $g \in U(R[x])$. Z założenia indukcyjnego otrzymujemy więc, że wszystkie współczynniki w g są nilpotentne, skąd również wszystkie współczynniki w f są nilpotentne.

Definicja: Przekształcenie $\varphi : R \to P$ pierścieni przemiennych z jedynką nazywamy homomorfizmem, jeżeli są spełnione następujące warunki

- φ jest homomorfizmem grup addytywnych
- $\forall_{a,b \in R}\ \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
- $\varphi(1) = 1$

Przykłady:

- Niech $f : \mathbb{Z} \to \mathbb{Z}$ będzie homomorfizmem, wówczas $f(1) = 1$ i stąd $f(k) = k$, czyli $f = id$
- Niech $f : R[x] \to R$ będzie taki, że $\varphi(f) = f(a)$ dla $a \in R$
- Niech $f : \mathbb{Z} \to \mathbb{Z}_n$ będzie taki, że $f(k) = k \mod n$

Definicja: Podzbiór I pierścienia R nazywamy ideałem jeśli

- I jest podgrupą R ze względu na dodawanie
- dla dowolnych $a \in R$ oraz $b \in I$ mamy $ab \in I$

Piszemy $I \triangleleft R$.

Fakt: Jądro homomorfizmu pierścieni jest ideałem.

Definicja: Niech $r \in R$. Ideałem generowanym przez r nazywamy zbiór

$$(r) = \{rx \mid x \in R\}$$

Ideałem generowanym przez zbiór $\{r_1, \ldots, r_k\}$ nazywamy zbiór

$$(\{r_1, \ldots, r_k\}) = r_1R + r_2R + \ldots + r_kR$$

Ideał generowany przez zbiór to najmniejszy ideał zawierający ten zbiór.

Definicja: Ideał jest główny jeśli jest generowany przez jeden element.

Fakt: $1 \in I \triangleleft R$ wtedy i tylko wtedy gdy $I = R$.

Zadanie 3.
Sprawdź czy w pierścieniu $k[x]$ następujące zbiory są ideałami

a) bez wyrazu wolnego

b) zależne tylko od x

c) spełniające $f(x, y) = (x, -y)$

d) spełniające $f(x, y) = (y, x)$

e) postaci $(x - 1)f + yg$, gdzie $f, g \in k[x]$

Które są podpierścieniami $\mathbb{Z}[x]$?

Rozwiązanie:

a) Mamy $I = \{f \in k[x] \mid f(0) = 0\}$. I jest podgrupą w $(R, +)$, bo jeśli $f, g \in I$, czyli $f(0) = 0$ oraz $g(0) = 0$, to $(f - g)(0) = f(0) - g(0) = 0$, czyli $f - g \in I$. Jeśli $f \in I$ oraz $h \in R$, to $(f \cdot h)(0) = f(0) \cdot h(0) = 0 \cdot h(0) = 0$, czyli $f \cdot h \in I$. Zatem I jest ideałem. Możemy zdefiniować homomorfizm $\varphi : k[x] \to k$ taki że $\varphi(f) = f(0)$, wówczas $\ker(\varphi) = \{f \mid \varphi(f) = 0\} = \{f \mid f(0) = 0\} = I$.

b) Mamy $I = \{f(x, y) \in k[x, y] \mid f$ zależy tylko od $x\}$. Gdyby I było ideałem, to dla każdego innego $h(x, y) \in k[x, y]$ wielomian $f(x, y) \cdot h(x, y)$ zależy tylko od x. Tak być nie musi, bo na przykład dla $h(x, y) = y$ oraz $f(x, y) = x$ mamy $f \in I$, ale $f \cdot h = xy$, czyli $f \cdot h \notin I$. Stąd I nie jest ideałem.

e) Mamy $I = \{(x - 1)h(x, y) + yg(x, y)\}$. Jest to ideał generowany przez zbiór $\{x - 1, y\}$, czyli $I = (x - 1, y)$.

Ćwiczenia 18

Fakt: Jeśli R to dziedzina, to w $R[x]$ zachodzi związek $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Fakt: Jeśli $I \triangleleft R$, to $I = R$ wtedy i tylko wtedy gdy istnieje $u \in U(R)$ takie, że $u \in I$.

Definicja: Niech $R \neq \{0\}$. Powiemy, że pierścień R jest pierścieniem Euklidesa jeżeli dana jest funkcja $N : R \to \mathbb{N}$ spełniająca następujące warunki

1. $N(r) = 0$ wtedy i tylko wtedy gdy $r = 0$
2. $N(rs) = N(r)N(s)$
3. $\forall_{r \in R}\ \forall_{0 \neq s \in R}\ \exists_{t,h \in R}\ r = st + h$ oraz $N(h) < N(s)$

Przykłady:

- Niech $R = \mathbb{Z}$ i niech $N(k) = |k|$, wówczas R jest pierścieniem Euklidesa
- Niech $R = \mathbb{F}[x]$ i niech $N(f) = 2^{\deg(f)}$, wówczas R jest pierścieniem Euklidesa

Fakt: Jeśli R jest dziedziną Euklidesową, czyli jest pierścieniem Euklidesowym i nie ma niezerowych dzielników zera, to R jest dziedziną ideałów głównych, czyli R jest dziedziną i każdy ideał w nim jest główny.

Zadanie 1.
Czy $(2, x)$ jest ideałem głównym w

a) $\mathbb{Z}[x]$

b) $\mathbb{Q}[x]$

Rozwiązanie:

a) Przypuśćmy, że $(2, x) \triangleleft \mathbb{Z}[x]$ jest ideałem głównym, zatem istnieje wielomian $p(x)$, który generuje ten ideał, czyli $(2, x) = (p(x))$ dla pewnego $p(x) \in \mathbb{Z}[x]$. Stąd $(p(x))$ jest najmniejszym ideałem, który zawiera 2 i x, czyli $2, x \in p(x)$. Dalej istnieją $q(x), g(x) \in \mathbb{Z}[x]$ takie, że $2 = p(x)q(x)$ oraz $x = p(x)q(x)$. $\mathbb{Z}$ jest dziedziną, więc $0 = \deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x))$, skąd $\deg(p(x)) = 0$, czyli $p(x) = c \in \mathbb{Z}$. Dalej $x = c \cdot g(x)$. Współczynniki w $g(x)$ są całkowite oraz $c \in \mathbb{Z}$, skąd $c \in \{-1, 1\}$. Stąd otrzymujemy $(2, x) = (1) = (-1) = \mathbb{Z}[x]$. Aby pokazać, że $(2, x) \neq \mathbb{Z}[x]$ wskażemy element z $\mathbb{Z}[x]$ który nie należy od do ideału $(2, x)$. Gdyby $1 \in (2, x)$ to istniałyby $\alpha(x), \beta(x) \in \mathbb{Z}[x]$ takie, że $1 = 2\alpha(x) + x\beta(x)$. Tak jednak nie może być, ponieważ wyraz wolny po prawej stronie jest parzysty. Stąd $1 \notin (2, x)$, czyli $(2, x)$ nie jest ideałem głównym w $\mathbb{Z}[x]$.

b) $\mathbb{Q}[x]$ jest pierścieniem Euklidesa, ponieważ $\mathbb{Q}$ jest ciałem. Stąd każdy ideał w $\mathbb{Q}[x]$, czyli w szczególności $(2, x)$ jest ideałem głównym.

Wyznaczmy generator tego ideału. Zauważmy, że $1 \in (2, x)$, ponieważ $1 = 2 \cdot \frac{1}{2}$. Stąd $(2, x) = (1) = \mathbb{Q}[x]$.

Definicja: Ideał I pierścienia R jest pierwszy jeśli dla dowolnych $a, b \in R$, takich że $ab \in I$ zachodzi $a \in I$ lub $b \in I$. Ideał $I \neq R$ pierścienia R jest maksymalny jeśli jest on maksymalny ze względu na relację zawierania.

Jeśli $I \triangleleft R$, to R/I też jest pierścieniem, ponieważ R jest abelowa, czyli każda jej podgrupa w szczególności I jest normalna, czyli R/I jest grupą. Dodatkowo ten zbiór ma strukturę pierścienia (przemiennego z jedynką). Mamy $R/I = \{r+I \mid r \in R\}$. Mnożenie zdefiniowane jest w następujący sposób $(a + I) \cdot (b + I) = ab + I$.

Fakt: Ideał I jest pierwszy wtedy i tylko wtedy, gdy R/I jest dziedziną, bo jeśli R/I jest dziedziną, to $(a + I) \cdot (b + I) = 0 + I = I$ i wówczas $(a + I) = 0 + I \Leftrightarrow a \in I$ lub $(b + I) = 0 + I \Leftrightarrow b \in I$. Z drugiej strony mamy $(a + I) \cdot (b + I) = 0 + I = I \Leftrightarrow ab + I = I$, czyli $ab \in I$.

I jest maksymalny wtedy i tylko wtedy, gdy R/I jest ciałem.

Fakt: Jeśli I jest maksymalny, to jest pierwszy.

Fakt: Jeśli R jest dziedziną ideałów głównych (DIG), to I jest maksymalny wtedy i tylko wtedy gdy I jest pierwszy.

Zadanie 2.

a) Znaleźć ideały w pierścieniach $\mathbb{Z}$ i $\mathbb{Z}_n$

b) Wskazać, które ideały są pierwsze, a które maksymalne

c) Znaleźć pierścienie ilorazowe

Rozwiązanie:

a) Skoro $I \triangleleft \mathbb{Z}$, to $(I, +) \leq (\mathbb{Z}, +)$. Podgrupy w $\mathbb{Z}$ mają postać $n\mathbb{Z} = \langle n \rangle = \{nk \mid k \in \mathbb{Z}\}$, zatem jeśli I jest ideałem, to $I = \langle n \rangle$ dla pewnego n. Zauważmy, że $(n\mathbb{Z}) \cdot \mathbb{Z} \subseteq n\mathbb{Z}$, skąd $I = n\mathbb{Z} = (n) \triangleleft \mathbb{Z}$.

... Ideały w $\mathbb{Z}_n$ są postaci $\varphi((k)\mathbb{Z})$, gdzie $k \mid n$ lub po prostu $(k)\mathbb{Z}_n$.

b) Wyznaczmy ideały pierwsze w $\mathbb{Z}$. Szukamy takich n dla których jeśli $ab \in (n) \Leftrightarrow n \mid ab$, to $a \in (n) \Leftrightarrow n \mid a$ oraz $b \in (n) \Leftrightarrow n \mid b$. Niech p to liczba wówczas $ab \in (p) \Leftrightarrow p \mid ab$, stąd $p \mid a$ lub $p \mid b$, zatem (p) jest ideałem pierwszym. Jeśli n nie jest liczbą pierwszą, to $n = p \cdot q$ dla pewnych liczb p i q różnych od 1. Niech więc $a = p$ i $b = q$, wówczas $ab \in (n)$ oraz $a \notin (n)$ oraz $b \notin (n)$. Stąd (n) nie jest ideałem pierwszym. Wiemy, że $\mathbb{Z}$ jest dziedziną euklidesową, stąd $\mathbb{Z}$ jest dziedziną ideałów głównych, czyli jeśli I jest maksymalny to jest pierwszy. Stąd (p) dla liczb pierwszych p są ideałami maksymalnymi.

Ideały pierwsze w $\mathbb{Z}_n$ to $(p)\mathbb{Z}_n$, gdzie p to liczba pierwsza dzieląca n, co uzasadniamy analogicznie jak w $\mathbb{Z}$.

c) Dla $I = \mathbb{Z}$ mamy $\mathbb{Z}/(p) \simeq \mathbb{Z}_p$, gdzie p jest liczbą pierwszą.

Fakt: Niech $n \in \mathbb{Z}$, wówczas $\mathbb{Z}_n \simeq \mathbb{Z}/(n)$.

Dowód: Niech $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ będzie homomorfizmem takim że $\varphi(k) = k \mod n$, wówczas $\ker(\varphi) = \{m \in \mathbb{Z} \mid \varphi(m) = 0\} = \{m \in \mathbb{Z} \mid n \mid m\} = (n)$. Z twierdzenia o izomorfizmie $\mathbb{Z}_n = \mathrm{Im}(\varphi) \simeq \mathbb{Z}/\ker(\varphi) = \mathbb{Z}/(p)$.

Zadanie 3.
Wykazać, że suma i iloczyn ideałów jest ideałem, to znaczy jeśli $I, J \in R$ są ideałami, to podzbiory

a) $I + J = \{a + b \mid a \in I, b \in J\}$

b) $I \cdot J = \{\sum a_i b_i \mid a_i \in I, b_i \in J\}$

są ideałami w R. Ponadto pokazać, że zachodzą zwierania $IJ \subseteq I \cap J \subseteq I \subseteq I + J$. Podać przykłady ideałów i pierścienia takich, by te zawierania nie były trywialne.

Rozwiązanie:

a)

b) Niech $x, y \in I \cdot J$, wówczas dla $x = \sum a_i b_i$ oraz $y = \sum a'_i b'_i$ mamy

$$x - y = \sum a_i b_i + \sum (-a'_i) b'_i \in I \cdot J$$

Dalej weźmy dowolne $r \in R$, wówczas

$$xr = \sum a_i b_i r = \sum (a_i r) b_i \in I \cdot J$$

bo skoro I jest ideałem, to $a_i r \in I$. Stąd $I \cdot J \lhd R$.

Oczywiście $I \cap J \subseteq I$. Jeśli $a \in I$, to $a = a + 0 \in I + J$, skąd $I \subseteq I + J$. Pozostaje więc pokazać zawieranie $I \cdot J \subseteq I \cap J$. Niech $x \in \sum a_i b_i$. Skoro $b_i \in J$, to w szczególności $b_i \in R$. Skoro I jest ideałem, to $a_i b_i \in I$. Analogicznie $a_i b_i \in J$, skąd $a_i b_i \in I \cap J$, czyli $x \in I \cap J$.

Niech $R = \mathbb{Z}$ oraz $I = (n)$, $J = (m)$. Mamy $I \cdot J = (nm)$, bo niech $x = \sum a_i b_i$, gdzie $a_i \in I \Rightarrow a_i = n a'_i$ oraz $b_i \in J \Rightarrow b_i = m b'_i$, czyli $x = nm \sum a'_i b'_i \in (nm)$. Jeśli $x \in (nm)$, to $x = nmk$

dla $k \in \mathbb{Z}$ i wówczas $x = nmk = n \cdot (mk) \in (n) \cdot (m) = I \cdot J$. Mamy $I \cap J = (NWW(n,m))$. Mamy $I + J = (NWD(n,m))$. Dla $n = 4$ i $m = 6$ mamy $nm = 24$, $NWW(4,6) = 12$, $n = 4$ oraz $NWD(4,6) = 2$, skąd

$$(24) \subsetneq (12) \subsetneq (4) \subsetneq (2)$$

Zadanie 4.
Czy pierścień $\mathbb{Z}[x]/(x^2-1)$ jest dziedziną?

Rozwiązanie:
Ideał (x^2-1) nie jest pierwszy, bo $x^2-1 = (x-1)(x+1)$, ale $(x-1) \notin (x^2-1)$ oraz $(x+1) \notin (x^2-1)$, stąd $\mathbb{Z}[x]/(x^2-1)$ nie jest dziedziną.

Pokażemy, że $\mathbb{Z}[x]/(x^2-1)$ nie jest dziedziną wprost z definicji. Oznaczmy $I = (x^2-1)$. Szukamy $f, g \in \mathbb{Z}[x]$ takie, że $(f+I) \cdot (g+I) = 0 + I$, ale $f + I \neq 0 + I$ oraz $g + I \neq 0 + I$. Mamy $(f+I) \cdot (g+I) = fg + I$. Niech $f = x-1$ oraz $g = x+1$, wówczas $f + I \neq 0 + I$ oraz $g + I \neq 0 + I$, czyli $f \notin I$ oraz $g \notin I$. Ale wówczas mamy $(f+I) \cdot (g+I) = (x^2-1) + I = 0 + I = I$, czyli $fg \in I$.

Twierdzenie: (Pierwsze o izomorfizmie) Niech $f : R \to T$ będzie homomorfizmem pierścieni. Wówczas

1. Istnieje dokładnie jeden homomorfizm $g : R/\ker(f) \to T$ taki, że $f = g \circ \pi$
2. $R/\ker(f) \simeq \mathrm{Im}(f)$
3. Jeśli f jest na to $R/\ker(f) \simeq T$

Przykłady:

- Niech $\varphi : k[x] \to k$ zadane będzie wzorem $\varphi(f) = f(a)$ dla $a \in k$. Mamy $\ker(\varphi) = \{f \in k[x] \mid f(a) = 0\} = \{f \in k[x] \mid (x-a) \mid f\} = (x-a)$. Stąd $k[x]/(x-a) \simeq k$
- Niech $\varphi : \mathbb{R}[x] \to \mathbb{C}$ będzie zadany wzorem $\varphi(f) = f(i)$. Jest to epimorfizm bo $a+bx \mapsto a+bi$. Mamy $\ker(f) = \{f \in \mathbb{R}[x] \mid f(i) = 0\} = (x^2+1)$. Skąd z twierdzenia o izomorfizmie mamy $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$, czyli $\mathbb{R}[x]/(x^2+1)$ jest maksymalny w $\mathbb{R}[x]$ (wiąże się to z nierozkładalnością wielomianu x^2+1 w $\mathbb{R}$).

Ćwiczenia 19

Twierdzenie: Niech R będzie dziedziną i $f \in R[x]$. Jeżeli $a_1, \ldots, a_m \in R$ są parami różnymi pierwiastkami f krotności $k_1, \ldots, k_m$ odpowiednio, to wielomian f jest podzielny przez $(x - a_1)^{k_1} \ldots (x - a_m)^{k_m}$.

Zadanie 1.
Niech $\{a_1, \ldots, a_r\}$ będzie podzbiorem ciała k. Wykazać, że przekształcenie $\varphi : k[x] \to k \times \ldots \times k$ określone wzorem $\varphi(f) = (f(a_1), \ldots, f(a_r))$ jest epimorfizmem pierścieni. Znaleźć jego jądro.

Rozwiązanie:
Sprawdźmy, czy φ jest homomorfizmem. Sprawdźmy czy dla każdych $a, b \in k[x]$ mamy $\varphi(a+b) = \varphi(a) + \varphi(b)$. Mamy

$$\begin{aligned} \varphi(f(x) + g(x)) &= (f(a_1) + g(a_1)), \ldots, f(a_r) + g(a_r)) = \\ &= (f(a_1), \ldots, f(a_r)) + (g(a_1), \ldots, g(a_r)) = \\ &= \varphi(f(x)) + \varphi(g(x)) \end{aligned}$$

Sprawdźmy, czy $\varphi(1) = 1$. Oczywiście ten warunek jest spełniony. Warunek $\varphi(ab) = \varphi(a) \cdot \varphi(b)$ również jest spełniony. Sprawdźmy więc, czy φ jest epimorfizmem. Niech $(b_1, \ldots, b_r) \in k \times \ldots \times k$. Chcemy pokazać, że istnieje $f(x)$ takie, że $\varphi(f) = (b_1, \ldots, b_r)$, czyli szukamy wielomianu f takiego, że $f(a_1) = b_1, \ldots, f(a_r) = b_r$. Niech więc

$$f(x) = \sum_{i=0}^{n} b_i \prod_{j=0 \ j \neq i}^{r} \frac{x - a_i}{a_i - a_j}$$

wówczas $\varphi(f) = (b_1, \ldots, b_r)$. Wyznaczmy jądro tego homomorfizmu

$$\begin{aligned} \ker(\varphi) &= \{f \in k[x] \mid f(a_1) = \ldots = f(a_r) = 0\} = \\ &= \{f \in k[x] \mid (x - a_1) \ldots (x - a_r) \mid f\} = \\ &= ((x - a_1) \ldots (x - a_r)) \end{aligned}$$

Z twierdzenia o izomorfizmie mamy $\frac{k[x]}{((x-a_1)\ldots(x-a_r))} \simeq k \times \ldots \times k$.

Definicja: Niech R_1, R_2 będą pierścieniami. Pierścień produktowy to zbiór par (r_1, r_2) z działaniami po współrzędnych, a więc $(a, b) \cdot (c, d) = (ac, bd)$ oraz $(a, b) + (c, d) = (a + c, b + d)$.

Fakt: Niech $\varphi : R \to S$ będzie epimorfizmem, wówczas jeśli $K \lhd R$, to $\varphi(K) \lhd S$.

Zadanie 2.
Pokazać, że każdy ideał pierścienia $P \times R$ jest postaci $I \times J$, gdzie I i J są ideałami pierścieni P i R odpowiednio. Ustalić, kiedy ideał $I \times J$ jest pierwszy, a kiedy maksymalny.

Rozwiązanie:
Niech $S \triangleleft P \times R$. Dla $P \times R$ mamy naturalne rzutowania

$$\pi_1 : P \times R \to P,\ \pi_1(p,r) = p \quad \text{oraz} \quad \pi_2 : P \times R \to R,\ \pi_2(p,r) = r$$

Niech więc $\pi_1(S) := I$ oraz $\pi_2(S) := J$. Mamy $I \triangleleft P$ oraz $J \triangleleft R$. Jeśli $(s_1, s_2) \in S$, to oczywiście $s_1 \in I$ oraz $s_2 \in J$, skąd $(s_1, s_2) \in I \times J$, czyli $S \subseteq I \times J$. Niech $(i,j) \in I \times J$, czyli $i \in \pi_1(S)$ oraz $j \in \pi_2(S)$. Istnieje więc $x \in R$ takie, że $\pi_1(i,x) = i$, czyli $(i,x) \in S$ oraz istnieje $y \in P$ takie, że $\pi_2(y,j) = j$, czyli $(y,j) \in S$. Dalej mamy $(i,j) = (i,x) \cdot (1,0) + (y,j) \cdot (0,1) \in S$, bo S jest ideałem.

Pokażemy, że $\frac{P \times R}{I \times J} \simeq \frac{P}{I} \times \frac{R}{J}$. Niech $\varphi : P \times R \to \frac{P}{I} \times \frac{R}{J}$ będzie homomorfizmem zadanym wzorem $\varphi(p,r) = (p+I, r+J)$. Jest to epimorfizm oraz $\ker(\varphi) = I \times J$, skąd $\frac{P \times R}{I \times J} \simeq \frac{P}{I} \times \frac{R}{J}$. Stąd $I \times J$ jest pierwszy wtedy i tylko wtedy, gdy $\frac{P \times R}{I \times J}$ jest dziedziną, czyli gdy $\frac{P}{I} \times \frac{R}{J}$ jest dziedziną. Jeśli $I \neq P$ i $J \neq R$, to istnieje $(p+J, 0) \neq (0,0)$ oraz $(0, r+J) \neq (0,0)$ i wówczas $(p+I, 0) \cdot (0, r+J) = (0,0)$. Musi więc zachodzić $I = P$ i wówczas $\frac{R}{J}$ musi być dziedziną lub $J = R$ i wtedy $\frac{P}{J}$ musi być dziedziną. Czyli $I \times J$ jest pierwszy, gdy $I = P$ i J jest pierwszy lub gdy $J = R$ i I jest pierwszy.

Analogicznie $I \times J$ jest maksymalny, gdy $I = P$ i J jest maksymalny lub gdy $J = R$ i I jest maksymalny.

Definicja: Pierścień R nazywamy lokalnym jeżeli zawiera dokładnie jeden ideał maksymalny.

Zadanie 3.
Pokazać, że dla pierścienia R następujące warunki są równoważne

1. suma elementów nieodwracalnych jest elementem nieodwracalnym
2. zbiór elementów nieodwracalnych jest ideałem
3. R jest pierścieniem lokalnym

Rozwiązanie:
1. $\Rightarrow$ 2. Wystarczy sprawdzić czy jeśli $r \notin U(R)$ oraz $s \in R$, to $rs \notin U(R)$, bo z 1. wynika, że $U(R)$ jest podgrupą. Wiemy, że jeśli $rs \in U(R)$, to $r \in U(S)$ oraz $s \in U(R)$, skąd wynika teza.

2. $\Rightarrow$ 3. Niech $I = R \setminus U(R)$ i niech I będzie ideałem. I jest ideałem maksymalnym, bo jeśli $I \subsetneq J \subseteq R$, to istnieje $r \in J$ takie, że $r \in U(R)$ i wówczas $1 \in J$, czyli $J = R$. Jeśli $I' \triangleleft R$ jest maksymalny, to $I' \neq R$ i wówczas $I' \subset R \setminus U(R) = I$. Zatem R na jeden ideał maksymalny $I = R \setminus U(R)$.

3. $\Rightarrow$ 1. Załóżmy, że R jest pierścieniem lokalnym i niech $x, y \notin U(R)$. Rozpatrzmy ideały generowane przez x i y, czyli (x) oraz (y). Wówczas z lematu Kuratowskiego-Zorna, dowolny ideał możemy rozszerzyć do ideału maksymalnego, czyli istnieje M_x maksymalny taki, że $(x) \subseteq M_x$ oraz $(y) \subseteq M_y$. Skoro R jest lokalny, to $M_x = M_y = M$, czyli $(x), (y) \subseteq M$, skąd $(x,y) \subseteq M$. Mamy $x + y \in (x,y) \subseteq M \neq R$, skąd $x + y \notin U(R)$.

Zadanie 4.
Niech R będzie pierścieniem lokalnym. Udowodnić, że jeśli $x \in R$ oraz $x^2 = x$, to $x = 0$ lub $x = 1$.

Zadanie 5.
Pokaż, że ideał $(2, x)$ jest maksymalny w pierścieniu $\mathbb{Z}[x]$. Z czym jest izomorficzny iloraz $\mathbb{Z}[x]/(2, x)$?

Rozwiązanie:
Wystarczy, że udowodnimy, że $\frac{\mathbb{Z}[x]}{(2,x)}$ jest ciałem. Pokażemy, że $\frac{\mathbb{Z}[x]}{(2,x)} \simeq \mathbb{Z}_2$. W tym celu konstruujemy homomorfizm $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_2$ wzorem $\varphi(a_0 + a_1x + \ldots + a_nx^n) = f(0) \mod 2 = a_0 \mod 2$. Jest to suriekcja w oczywisty sposób. Również φ jest homomorfizmem. Dalej mamy

$$\begin{aligned}
\ker(\varphi) &= \{f(x) = a_0 + a_1x + \ldots + a_nx^n \mid a_0 \mod 2 = 0\} = \\
&= \{f \in \mathbb{Z}[x] \mid f = 2\widetilde{a} + x \cdot g(x)\} = \\
&= \{f \in \mathbb{Z}[x] \mid f = 2 \cdot h(x) + x \cdot g(x)\} = \\
&= (2, x)
\end{aligned}$$

przy czym $a_0 = 2\widetilde{a}$. Stąd z twierdzenia o izomorfizmie $\frac{\mathbb{Z}[x]}{(2,x)} \simeq \mathbb{Z}_2$. Dalej $\mathbb{Z}_2$ jest ciałem, skąd ideał $\mathbb{Z}[x]/(2, x)$ jest maksymalny.

Do odwołania R jest przemienną dziedziną. $U(R)$ oznacza grupę elementów odwracalnych pierścienia R.

Definicja: Niech $a, b, u \in R \setminus \{0\}$

1. powiemy, że a dzieli b (oznaczamy $a \mid b$) jeśli $b = ac$ dla pewnego $c \in R$
2. $u \in U(R)$ wtedy i tylko wtedy, gdy $u \mid 1$
3. powiemy, że a, b są stowarzyszone (oznaczamy $a \sim b$) jeśli $a \mid b$ i $b \mid a$
4. $a \sim b$ wtedy i tylko wtedy, gdy $a = ub$ dle pewnego elementu odwracalnego u
5. $u \in U(R)$ wtedy i tylko wtedy, gdy $u \sim 1$
6. $\sim$ jest relacją równoważności na $R \setminus \{0\}$
7. element a jest rozkładalny jeżeli można go przedstawić w postaci iloczynu dwóch elementów nieodwracalnych
8. powiemy, że element a jest nierozkładalny jeżeli a nie jest odwracalny i a nie jest rozkładalny (czyli jeśli $a \notin U(R)$ i $a = bc$, to $a \in U(R)$ lub $b \in U(R)$)
9. $p \notin U(R)$ jest pierwszy wtedy i tylko wtedy, gdy jeśli $p \mid ab$ to $p \mid a$ lub $p \mid b$ dla $a, b \in R$ lub równoważnie $p \in R$ jest pierwszy wtedy i tylko wtedy, gdy $(p) \triangleleft R$ jest ideałem pierwszym

Fakt: Jeśli R jest dziedziną ideałów głównych to dowolny nierozkładalny element $a \in R$ jest pierwszy (bo zawsze element pierwszy jest nierozkładalny) oraz jeśli $a \notin U(R)$, $a \neq 0$, to (a) jest pierwszy wtedy i tylko wtedy, gdy (a) jest maksymalny.

Zadanie 6.
Znajdź wielomiany nierozkładalne w $\mathbb{R}[x]$ i w $\mathbb{C}[x]$.

Rozwiązanie:
Jeśli R jest dziedziną, to $U(R) = \{a_0 \mid a \in U(R)\}$. Oczywiście $\mathbb{R}$ oraz $\mathbb{C}$ to dziedzina.

Rozpatrzymy $\mathbb{C}[x]$. Jeśli $f \in \mathbb{C}[x]$, to $f(x) = \alpha(x - a_1)\dots(x - a_k)$, dla $\alpha, a_i \in \mathbb{C}$. Elementy odwracalne w $\mathbb{C}[x]$ to po prostu liczby zespolone różne od zera. Zatem w f element $\alpha \in U(\mathbb{C}[x])$ oraz $(x-a_i) \notin U(\mathbb{C}[x])$. Stąd elementy nierozkładalne to elementy postaci $x-a$ dla $a \in \mathbb{C}$, ponieważ jeśli mielibyśmy wielomian stopnia 2, to możemy go przedstawić w postaci iloczynu wielomianów stopnia 1 a one są nieodwracalne. Z drugiej strony jeśli $x - a$ byłby rozkładalny, to $x - a = h \cdot g$, gdzie g, h są nieodwracalne (czyli $\deg(h), \deg(g) \geq 1$), a stąd, jako że $\det(hg) = \det(h)+\det(g)$ (bo $\mathbb{C}$ jest ciałem), mamy $1 = \deg(hg) = \deg(h)+\deg(g) \geq 2$ co jest sprzecznością. Stąd nierozkładalne w $\mathbb{C}[x]$ są wielomiany stopnia 1.

Rozpatrzmy $\mathbb{R}[x]$. Jeśli $f \in \mathbb{R}$, to f rozkłada się na iloczyn wielomianów stopnia co najwyżej 2. Jeśli $\deg(f) \geq 3$, to f jest rozkładalny, bo jest iloczynem co najmniej dwóch wielomianów nieodwracalnych. Jeśli $\deg(f) = 1$, to $f(x) = a(x + b)$, czyli wielomiany te są nierozkładalne (argument jak dla $\mathbb{C}$). Jeśli $\deg(f) = 2$, to po ewentualnym przeskalowaniu mamy $f(x) = x^2 + ax + b$. Pokażemy, że wielomian ten jest nierozkładalny jeśli $a^2 - 4b < 0$. Są one nierozkładalne, bo w przeciwnym razie wielomian f miałby pierwiastek rzeczywisty (a nie ma). Jeśli $a^2 - 4b \geq 0$, to wielomian f możemy rozłożyć na czynniki liniowe i stąd f jest rozkładalny.

Mamy $\mathbb{C}[x]/(x-a) \simeq \mathbb{C}$, $\mathbb{R}[x]/(x-a) \simeq \mathbb{R}$ oraz jeśli x^2+ax+b nie ma rzeczywistych pierwiastków, to $\mathbb{R}[x]/x^2 + ax + b \simeq \mathbb{C}$.

Obserwacja: Niech k będzie ciałem. Rozpatrzmy $f \in k[x]$ taki, że $\deg(f) \leq 3$. Elementy odwracalne w $k[x]$ to niezerowe elementy ciała k. Jeśli f jest rozkładalny, to $f = hg$ przy czym $\deg(h), \deg(g) \geq 1$. Mamy więc $3 \geq \deg(f) = \deg(h) + \deg(g)$ (bo k to ciało), skąd $\deg(g)$ lub $\deg(h)$ musi być równe 1, czyli f ma pierwiastek w k.

Fakt: Niech k będzie ciałem. Rozpatrzmy $f \in k[x]$ taki, że $\deg(f) \leq 3$. Wówczas f jest rozkładalny wtedy i tylko wtedy, gdy f ma pierwiastek w k.

Zadanie 7.
Zbadaj rozkładalność wielomianu $x^2 + 1$ nad ciałami $\mathbb{Z}_3$ oraz $\mathbb{Z}_5$.

Rozwiązanie:
Przyjrzyjmy się wielomianowi $f(x) = x^2 + 1 \in \mathbb{Z}_3[x]$. Mamy $f(0) = 1$, $f(1) = 2$ oraz $f(2) = 2$ (bo jesteśmy w $\mathbb{Z}_3$), skąd f nie ma pierwiastka w $\mathbb{Z}_3$ i jako, że jest stopnia mniejszego od 3, to jest nierozkładalny.

Przyjrzyjmy się wielomianowi $f(x) = x^2+1 \in \mathbb{Z}_5[x]$. Mamy $f(0) = 1$, $f(1) = 2$, $f(2) = 0$, $f(3) = 0$ oraz $f(4) = 2$ (bo jesteśmy w $\mathbb{Z}_5$), skąd f ma pierwiastek w $\mathbb{Z}_5$ i stąd f jest rozkładalny. Mamy $f = (x - 2)(x - 3)$

Ćwiczenia 20

Zadanie 1.
Wyznacz elementy odwracalne w $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

Rozwiązanie:
Wiemy, że $\mathbb{Z}[i]$ jest dziedziną euklidesową. Ponadto mamy zdefiniowaną normę $N : \mathbb{Z}[i] \to \mathbb{Z}_+$ wzorem $N(a + bi) = a^2 + b^2$. Jeśli $\alpha \in U(Z[i])$, to istnieje element $\beta \in \mathbb{Z}[i]$ taki, że $\alpha\beta = 1$, skąd $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$, czyli jako że $N(x) \in \mathbb{Z}_+$, to $N(\alpha) = 1$. Stąd mamy $\alpha = a + bi$, gdzie $a^2 + b^2 = 1$ dla $a, b \in \mathbb{Z}$, zatem $\alpha \in \{1, -1, i, -i\}$. Każdy z tych elementów jest odwracalny. Zatem elementy odwracalne w $\mathbb{Z}[i]$ należą do zbioru $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

Zadanie 2.
Pokaż, że $1 + 2i$ jest elementem nierozkładalnym w $\mathbb{Z}[i]$.

Rozwiązanie:
Jeśli $1 + 2i$ jest nierozkładalny, to jeśli $1 + 2i = \alpha\beta$ dla $\alpha, \beta \in \mathbb{Z}[i]$, to $\alpha \in U(R)$ lub $\beta \in U(R)$. Mamy $N(1 + 2i) = 5$, zatem $N(\alpha)N(\beta) = 5$, skąd $N(\alpha) = 1$ lub $N(\beta) = 1$, czyli α lub β jest odwracalny. Zatem $1 + 2i$ jest nierozkładalny.

Fakt: Jeśli $N(a)$ jest liczbą pierwszą dla $a \in \mathbb{Z}[i]$, to a jest elementem nierozkładalnym.

Rozpatrzmy epimorfizm $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[i]$ zadany wzorem $\varphi(f) = f(i) \in \mathbb{Z}[i]$. Jest to surjekcja, ponieważ wielomiany obraz wielomianów liniowych to przeciwdziedzina. Dalej mamy $\ker(\varphi) = \{f \mid f(i) = 0\} = (x^2 + 1)$. Stąd z twierdzenia o izomorfizmie mamy $\mathbb{Z}[x]/(x^2 + 1) \simeq \mathbb{Z}[i]$.

Uwaga: NWD jest zdefiniowane z dokładnością do stowarzyszenia.

Zadanie 3.
Niech $a = 7$, $b = 1 + 2i \in \mathbb{Z}[i]$. Czy $a\mathbb{Z}[i] + b\mathbb{Z}[i]$ jest ideałem maksymalnym w $\mathbb{Z}[i]$?

Rozwiązanie:
Wiemy, że jeśli $I = (a)$ oraz $J = (b)$, to $I + J = (NWD(a, b))$ o ile NWD istnieje. Wyznaczmy więc $NWD(7, 1 + 2i)$.

I sposób: Wiemy, że $\mathbb{Z}[i]$ jest dziedziną z jednoznacznością rozkładu, zatem wystarczy że znajdziemy rozkład liczb na nierozkładalne czynniki. Jest on jednoznaczny z dokładnością do elementów odwracalnych. Znajdźmy rozkład 7 na czynniki nierozkładalne. Mamy $N(7) = 49$, zatem jeśli $7 = \alpha\beta$ dla $\alpha, \beta \notin U(\mathbb{Z}[i])$ to $N(\alpha) = N(\beta) = 7$ (bo $N(7) = N(\alpha\beta) = N(\alpha)N(\beta)$ i skoro α, β są nieodwracalne, to ich norma jest różna od 1). Niech $\alpha = a + bi$, chcemy sprawdzić czy istnieje $a, b \in \mathbb{Z}$ takie że $a^2 + b^2 = 7$. Kwadrat dowolnej liczby całkowitej daje resztę 0 lub 1 przy dzieleniu przez 4, zatem $a^2 + b^2$ daje resztę $0, 1$ lub 2 przy dzieleniu przez 4. Z kolei 7 daje resztę 3 przy dzieleniu przez 7, skąd takie a i b nie istnieją. Zatem jeśli $7 = \alpha\beta$, to α lub β musi być odwracalne, czyli 7 jest nierozkładalne. Mamy $N(1 + 2i) = 5$, zatem również $1 + 2i$ jest nierozkładalne. Stąd $NWD(7, 1 + 2i) \sim 1$.

II sposób: Chcemy policzyć $NWD(7, 1+2i)$. Skorzystamy z algorytmu Euklidesa. Chcemy przedstawić 7 jako $7 = q(1+2i)+r$, gdzie $N(r) < N(1+2i)$. Mamy $7 = (1-2i)(1+2i)+2$, zatem $NWD(7, 1+2i) = NWD(2, 1+2i)$. Mamy $1+2i = 2i+1$, zatem $NWD(7, 1+2i) = NWD(2, 1) = 1$. Stąd $(7) + (1+2i) = (1) = \mathbb{Z}[i]$, czyli $a\mathbb{Z}[i] + b\mathbb{Z}[i]$ nie jest ideałem maksymalnym w $\mathbb{Z}[i]$.

Zadanie 4.
Oblicz $NWD(1+3i, 1+5i)$ w $\mathbb{Z}[i]$.

Zadanie 5.
Znaleźć następujące ilorazy

a) $\mathbb{R}[x]/(x^2+x+1)$

b) $\mathbb{Z}[x]/(x^2+1)$

c) $\mathbb{Z}[i]/(3+i)$

Rozwiązanie:

c) Niech $I = (3+i)$. Zauważmy, że zachodzi równość warstw $-3+I = i+I$, skąd mamy $(a+bi)+I = (a-3b)+I$. Wystarczy więc, ż wyznaczymy jakie liczby całkowite należą do ideału I. Oczywiście $N(3+i) = 10 \in I$, czyli $0+I = 10+I$. Rozpatrzmy homomorfizm $\varphi : \mathbb{Z} \to \mathbb{Z}[i]/I$ taki, że $\varphi(a) = a+I$. Jest to epimorfizm, ponieważ

$$\varphi(a-3b) = (a-3b)+I = (a+bi)+I \in \mathbb{Z}[i]/I$$

Dalej mamy $(10) \subseteq \ker(\varphi)$, ponieważ $10+I = 0+I$. Mamy

$$\ker(\varphi) = \{a \in \mathbb{Z} \mid a \in I\} = \{a \in \mathbb{Z} \mid (3+i) \mid a\}$$

Mamy

$$\frac{a}{3+i} = \frac{a(3-i)}{10} = \frac{3a}{10} + \frac{-ia}{10}$$

czyli $10 \mid 3a$ oraz $10 \mid -a$, skąd $a = 10$. Zatem $\ker(f) = \{a \in \mathbb{Z} \mid 10 \mid a\} = (10) \triangleleft \mathbb{Z}$. Stąd z twierdzenia o izomorfizmie mamy $\mathbb{Z}[i]/(3+i) \simeq \mathbb{Z}/(10) = \mathbb{Z}_{10}$.

Uwaga: Dla $a, b \in \mathbb{Z}$ takich, że $NWD(a,b) = 1$ mamy $\mathbb{Z}[i]/(a+bi) \simeq \mathbb{Z}_{N(a+bi)}$.

Zadanie 6.
Oblicz $NWD(f,g)$ oraz znajdź takie wielomiany $a, b \in R[x]$, że $af + bg = NWD(f,g)$, gdzie

a) $f = x^5 - 2x + 3x^2 - 3x - 2$,

b) $f = x^4 + 4$, $g = 2x^3 + x^2 - 2x - 6$, $R = \mathbb{Z}_3[x]$

Rozwiązanie:

a) Skoro działamy w $\mathbb{Z}_3$, to $f = x^4 + 1$ oraz $g = 2x^3 + x^2 + x$. Podzielmy z resztą te wielomiany, wiemy, że $2 \cdot 2 = 1$ w $\mathbb{Z}_3$, zatem

$$x^4 + 1 = 2x \cdot (2x^3 + x^2 + x) - 2x^3 - 2x^2 + 1 = 2x(2x^3 + x^2 + x) + x^3 + x^2 + 1 =$$

$$= 2x(2x^3 + x^2 + 1) + 2(2x^3 + x^2 + x) - x^2 - 2x + 1 =$$

$$= 2x(2x^3 + x^2 + 1) + 2(2x^3 + x^2 + x) + 2x^2 + x + 1 =$$

$$= (2x + 2)(2x^3 + x^2 + 1) + 2x^2 + x + 1$$

Skąd mamy $NWD(f, g) = NWD(g, h)$, gdzie $h = 2x^2 + x + 1$. Dalej mamy

$$2x^3 + x^2 + x = x(2x^2 + x + 1) + 0$$

czyli mamy $NWD(f, g) = 2x^2 + x + 1$. Dalej mamy

$$2x^2 + x + 1 = f(x) - (2x + 2)(g(x) = f(x) + (x + 1)g(x)$$

stąd $a = 1$ i $b = x + 1$.

Zadanie 7.
Pokaż, że $\mathbb{Z}_2[x]/(x^2+x+1)$, $\mathbb{Z}_2[x]/(x^3+x+1)$ i $\mathbb{Z}_2[x]/(x^4+x+1)$ są ciałami. Ile mają elementów?

Rozwiązanie:
Wiemy, że jeśli k to ciało (lub dziedzina ideałów głównych), to $k[x]/(f)$ jest ciałem wtedy i tylko wtedy, gdy (f) jest maksymalny, czyli gdy f jest nierozkładalny w k. Chcemy więc sprawdzić czy wielomiany $f = x^2 + x + 1$, $g = x^3 + x + 1$ oraz $h = x^4 + x + 1$ są rozkładalne. Jako, że stopnie wielomianów f, g są mniejsze od 3, to wielomiany f i g są rozkładalne wtedy i tylko wtedy, gdy mają pierwiastek w $\mathbb{Z}_2$. Mamy $f(0) = 1$, $f(1) = 1$ oraz $g(0) = 1$, $g(1) = 1$, zatem wielomiany f i g nie mają pierwiastka i stąd są nierozkładalne. Dalej przyjrzyjmy się pierścieniowi $\mathbb{Z}_2[x]/(f)$. Jeśli $a \in \mathbb{Z}_2[x]$, to zachodzi równość warstw $a + (f) = \widetilde{a} + (f)$, gdzie $\deg(a) < 2$ (bo możemy podzielić z resztą a przez f). Zatem baza $\mathbb{Z}_2[x]/(f)$ nad $\mathbb{Z}_2$ to $\{1, x\}$, czyli $|\mathbb{Z}_2[x]/(f)| = 2^2$. Analogicznie baza $\mathbb{Z}_2[x]/(g)$ nad $\mathbb{Z}_2$ to $\{1, x, x^2\}$, skąd $|\mathbb{Z}_2[x]/(g)| = 2^3 = 8$. Z kolei wielomian h może być rozkładalny. Jeśli mamy $x^4 + x + 1 = (x + ax + 1)(x^2 + bx + 1)$, to jako, że współczynniki przy x muszą się zgadzać, to $1 = a + b$ i jako, że współczynniki przy x^3 muszą się zgadzać, to $0 = a + b$, czyli mamy sprzeczność. Zatem również h nie jest rozkładalny. Stąd $\mathbb{Z}_2[x]/(h)$ jest ciałem i ma 16 elementów.

Zadanie 8.
Niech $R = \mathbb{Z}[-\sqrt{3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

a) Czy element $2 \in R$ jest nierozkładalny?

b) Czy element $2 \in R$ jest pierwszy?

c) Czy ideał $(2, 1 + \sqrt{-3})$ jest główny?

Rozwiązanie:
Zdefiniujmy „normę" $N(a+b\sqrt{3}) = a^2+3b^2$, wówczas $N(\alpha\beta) = N(\alpha)N(\beta)$. Mamy $U(R) \subseteq \{\alpha \mid N(\alpha)=1\}$. Jeśli $\alpha = a+b\sqrt{-3}$, to $a^2+3b^2 = 1 \Leftrightarrow a \in \{-1,1\}, b=0$. Stąd jako, że $-1,1$ są odwracalne w R, to $U(R) = \{1,-1\}$.

a) Chcemy sprawdzić, czy element 2 jest nierozkładalny. Jeśli $2=\alpha\beta$, to $N(\alpha)N(\beta) = 4 = 1\cdot 4 = 2\cdot 2$. Jeśli $\alpha = a+b\sqrt{-3}$ i $N(\alpha)=2$, to $a^2+3b^2=2$, czyli $b=0$ oraz $a^2=2$, co jest niemożliwe. Stąd $N(\alpha)=1$ lub $N(\beta)=1$, zatem α lub β są odwracalne, czyli 2 jest nierozkładalny.

b) Chcemy rozstrzygnąć, czy 2 jest pierwszy, czyli czy z tego, że $2 \mid \alpha\beta$ wynika, że $2 \mid \alpha$ lub $2 \mid \beta$. Mamy $4 = (1+\sqrt{-3})(1-\sqrt{-3})$, czyli $2 \mid 4$ oraz $2 \nmid (1+\sqrt{-3})$ i $2 \nmid (1-\sqrt{-3})$, bo jeśli $2 \mid (1\pm\sqrt{-3})$, to $(1\pm\sqrt{-3}) = 2\cdot\gamma$ i wówczas $N(\gamma)=1$ i stąd $\gamma \in U(R)$, co sprowadza się do tego, że $2 = \pm(1\pm\sqrt{-3})$, co nie jest prawdą. Zatem 2 nie jest pierwszy.

Ćwiczenia 21

Zadanie 1.
Rozważmy homomorfizm $\varphi : \mathbb{Q}[x] \to \mathbb{R}$ taki, że $x \mapsto \sqrt[3]{2}$. Wyznacz jego obraz oraz jądro.

Rozwiązanie:
Mamy homomorfizm $\varphi : \mathbb{Q}[x] \to \mathbb{R}$ zadany wzorem $\varphi(f(x)) = f(2^{\frac{1}{3}})$. Mamy

$$\text{im}(\varphi) = \{f(2^{\frac{1}{3}}) \mid f(x) \in \mathbb{Q}[x]\} = \{a + b \cdot 2^{\frac{1}{3}} + c \cdot 2^{\frac{2}{3}} \mid a, b, c \in \mathbb{Q}\} = \mathbb{Q}[\sqrt[3]{2}]$$

Mamy

$$\ker(\varphi) = \{f \mid f(\sqrt[3]{2} = 0\}$$

Oczywiście $(x^3 - 2) \subseteq \ker(\varphi)$. Mamy również $\varphi(x) = \sqrt[3]{2} \neq 0$, zatem $\ker(\varphi) \neq \mathbb{Q}[x]$, czyli jeśli pokażemy, że (x^3-2) jest maksymalny, to $\ker(\varphi) = (x^3-2)$. Wiemy, że $\mathbb{Q}[x]$ jest dziedziną ideałów głównych, zatem jeśli ideał generowany przez dowolny wielomian (f) jest maksymalny wtedy i tylko wtedy, gdy f jest maksymalny. Pokażemy więc, że $x^3 - 2$ jest nierozkładalny. Przypuśćmy nie wprost, że jest rozkładalny, wówczas skoro stopień jest mniejszy od trzech, to wielomian ten ma pierwiastek w $\mathbb{Q}$. Jednak $\sqrt[3]{2}$ jest niewymierne, czyli wielomian ten nie ma pierwiastka w $\mathbb{Q}$, skąd nie jest rozkładalny. Stąd

$$\ker(\varphi) = (x^3 - 2)$$

Z twierdzenia o izomorfizmie mamy $\mathbb{Q}[x]/(x^3 - 2) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2^2} \mid a, b, c \in \mathbb{Q}\}$. Skoro $(x^3 - 2)$ jest maksymalny, to $\mathbb{Q}[x]/(x^3 - 2)$ jest ciałem

Zadanie 2.
Rozważmy element $f = x^3 - 2$ w pierścieniu $R = \mathbb{Q}[x]$.

a) Niech $g = x + 1 + (f) \in R/(f)$. Wyznacz g^3

b) Wyznacz $(g + (f))^{-1} \in R/(f)$.

Rozwiązanie:
Niech $I = (f)$.

a) Mamy

$$g^3 = (x + 1)^3 + I = x^3 + 3x^2 + 3x + 1 + I = 3x^2 + 3x + 3 + (x^3 - 2) + I = 3x^2 + 3x + 3 + I$$

b) Mamy $(g + I)^{-1} = (h + I)$, gdzie h jest takie, że $g \cdot h = 1 + I \Leftrightarrow gh - 1 \in I$. Czyli $gh - 1 = (x^3 - 2) \cdot q(x)$, gdzie $q(x) \in \mathbb{Q}[x]$. Szukamy więc $h(x)$ i $q(x)$ takich, że $1 = g(x)h(x) - (x^3 - 2)q(x)$. Tu oczywiście musimy skorzystać z algorytmu Euklidesa. Mamy

$$x^3 - 2 = x^2(x + 1) - x^2 - 2 = x^2(x + 1) - x(x + 1) + x - 2 = (x^2 - x + 1)(x + 1) - 3$$

Skoro $3 \in U(\mathbb{Q})$, to

$$\frac{1}{3}(x^3 - 2) + 1 = \frac{1}{3}(x^2 - x + 1)(x + 1)$$

skąd

$$(x + 1) \cdot \frac{1}{3}(x^2 - x + 1) + I = 1 + I \Leftrightarrow (x + 1 + I)^{-1} = \frac{1}{3}(x^2 - x + 1) + I$$

Twierdzenie: (Kryterium Eisensteina) Niech R będzie dziedziną z jednoznacznością rozkładu oraz niech $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$. Jeśli istnieje element pierwszy R taki, że

- $p \nmid a_n$
- $p \mid a_i$ dla $0 \leq i < n$
- $p^2 \nmid a_0$

to f jest rozkładalny w $\mathbb{Q}[R][x]$.

Zadanie 3.
Sprawdź, czy wielomian f jest nierozkładalny w pierścieniu R, gdzie

a) $f = x^2 + y^2 + z^2$, $R = \mathbb{C}[x, y, z]$

b) $f = 3x^3 + 24ix^2 - 18x - 3 + 9i$, $R = \mathbb{Z}[i][x]$

c) $f = 3x^3 + 24ix^2 - 18x - 3 + 9i$, $R = \mathbb{Q}[i][x]$

Rozwiązanie:

b) Mamy

$$f = 3 \cdot (x^3 + 8ix^2 - 6x + (-1 + 3i))$$

każdy z czynników jest nieodwracalny w $\mathbb{Z}[i][x]$, ponieważ $U(R[x]) = \{a_0 + \ldots + a_nx^n \mid a_0 \in U(R) \text{ i } a_1, \ldots, a_n \text{ są nilpotentne w } R\}$, a $R = \mathbb{Z}[i]$ to dziedzina czyli $U(\mathbb{Z}[i][x]) = \{a_0 \mid a_0 \in U(\mathbb{Z}[i])\}$.