1 Grupy

1.1 Grupy

Definicja. *Grupą* nazywamy niepusty zbiór G z działaniem $\cdot : G \times G \to G$, $(a, b) \mapsto ab$, spełniającym warunki:

(1) działanie $\cdot$ jest *łączne*, tzn. $a(bc) = (ab)c$ dla dowolnych $a, b, c \in G$;

(2) dla działania $\cdot$ istnieje *element neutralny*, tzn. istnieje $e \in G$ taki, że $ae = a = ea$ dla dowolnego $a \in G$;

(3) dla dowolnego $a \in G$ istnieje *element odwrotny do a względem $\cdot$*, tzn. istnieje $a' \in G$ taki, że $aa' = a'a$ jest elementem neutralnym dla $\cdot$.

Grupę G, w której działanie $\cdot$ jest *przemienne*, tzn. $ab = ba$ dla dowolnych $a, b \in G$, to *grupą abelową* (lub *grupą przemienną*). *Rzędem grupy* G nazywamy ilość jej elementów $|G|$.

Zauważmy, że powyższa definicja implikuje, że każda grupa jest niepusta.

Ćwiczenie 1.1.1. Jeśli G jest zbiorem z działaniem $\cdot : G \times G \to G$ spełniającym następujące warunki:

(1) działanie $\cdot$ jest *łączne*;

(2) dla działania $\cdot$ istnieje *lewostronny element neutralny* e, tzn. $ea = a$ dla dowolnego $a \in G$;

(3) dla dowolnego $a \in G$ istnieje *lewostronny element odwrotny do a względem $\cdot$*, tzn. istnieje $a' \in G$ taki, że $a'a = e$;

to G jest grupą.

Stwierdzenie 1.1.1. *W grupie G istnieje dokładnie jeden element neutralny oraz dla dowolnego elementu $a \in G$ istnieje dokładnie jeden element odwrotny.*

Dowód. Niech e' i e'' będą dwoma elementami neutralnymi w G. Wtedy

$$e' = e'e'' = e''.$$

Podobnie, niech $a \in G$, niech a' i a'' będą dwoma elementami odwrotnymi do a. Wtedy

$$a' = a'(aa'') = (a'a)a'' = a''.$$

□

Jeśli G jest grupą, w którym działanie oznaczmy $\cdot$, to element neutralny dla tego działania oznaczać będziemy przez 1, natomiast element odwrotny do a przez a^{-1}. W powyższej sytuacji mówimy o *notacji multiplikatywnej*. Można stosować też *notację addytywną* dla której działanie oznaczane jest przez $+$, element neutralny przez 0, zaś element odwrotny do a przez $-a$ (nazywamy go też czasami *elementem przeciwnym do a względem $\cdot$*). Notację addytywną stosuje się jedynie w sytuacji, gdy działanie $+$ jest przemienne.

Stwierdzenie 1.1.2. *Jeśli G jest grupą oraz $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.*

Dowód. Bezpośrednie sprawdzenie, że $(ab)(b^{-1}a^{-1}) = 1 = (ab)(b^{-1}a^{-1})$. □

Przykłady. (1) Zbiór liczb całkowitych z działaniem dodawania jest grupą, którą będziemy oznaczać $\mathbb{Z}$.

(2) Jeśli $m > 0$, to zbiór liczb całkowitych podzielnych przez m z działaniem jest grupą, którą będziemy oznaczać $m\mathbb{Z}$.

(3) Zbiór liczb naturalnych (liczb całkowitych nieujemnych) z działaniem dodawania nie jest grupą, gdyż w zbiorze liczb naturalnych nie istnieją elementy przeciwne dla liczb dodatnich.

(4) Jeśli $m > 0$ jest liczbą naturalną, to zbiór reszt z dzielenia przez m z działaniem dodawania modulo m jest grupą, którą będziemy oznaczać $\mathbb{Z}_m$.

(5) Jeśli K jest ciałem (np. K może być ciałem liczb wymiernych, rzeczywistych bądź zespolonych), to K z działaniem dodawania jest grupą, którą będziemy oznaczać K i nazywać *grupą addytywną ciała K*.

(6) Jeśli K jest ciałem, to K z działaniem mnożenia nie jest grupą, gdyż nie istnieje element odwrotny do 0 względem mnożenia.

(7) Jeśli K jest ciałem, to zbiór elementów ciała różnych od 0 z działaniem mnożenia jest grupą, którą będziemy oznaczać K^* i nazywać *grupą multiplikatywną ciała K*.

(8) Jeśli $m > 0$ jest liczbą naturalną, to zbiór reszt z dzielenia przez m względnie pierwszych z m z działaniem mnożenia jest grupą oznaczaną $(\mathbb{Z}/m\mathbb{Z})^*$.

(9) Jeśli K jest ciałem liczb wymiernych bądź ciałem liczb rzeczywistych, to zbiór liczb dodatnich w K z działaniem mnożenia jest grupą, którą będziemy oznaczać K_+.

(10) Zbiór liczb zespolonych o module 1 z działaniem mnożenia jest grupą, którą będziemy oznaczać $\mathbb{T}$.

(11) Zbiór liczb zespolonych z takich, że istnieje liczba naturalna $m > 0$ taka, że $z^m = 0$, z działaniem mnożenia jest grupą, którą będziemy oznaczać $\mathbb{C}_\infty$.

(12) Jeśli $m > 0$ jest liczbą naturalną, to zbiór pierwiastków m-tego stopnia z 1 w $\mathbb{C}$ z działaniem mnożenia jest grupą, która będziemy oznaczać $\mathbb{C}_m$.

(13) Jeśli V jest przestrzenią liniową, to V z działaniem dodawania wektorów jest grupą, którą będziemy oznaczać V.

(14) Jeśli K jest ciałem oraz $m > 0$ jest liczbą naturalną, to zbiór $n \times n$ macierzy odwracalnych o współczynnikach w K z działaniem mnożenia macierzy jest grupą, którą oznaczamy $\mathrm{GL}_n(K)$. Grupy tej postaci nazywamy *głównymi grupami liniowymi*.

(15) Jeśli K jest ciałem oraz $m > 0$ jest liczbą naturalną, to zbiór $n \times n$ macierzy o współczynnikach w K i wyznaczniku równym 1 z działaniem mnożenia macierzy jest grupą, którą oznaczamy $\mathrm{SL}_n(K)$. Grupy tej postaci nazywamy *specjalnymi grupami liniowymi*.

(16) Jeśli X jest zbiorem, to zbiór wszystkich funkcji odwracalnych $X \to X$ jest grupą z działaniem składania funkcji, którą będziemy oznaczać $S(X)$ i nazywać *grupą symetrii zbioru* X. Jeśli $X = \{1, \ldots, n\}$, $n > 0$, to zamiast $S(X)$ będziemy pisać S_n. Grupy S_n nazywamy *grupami symetrycznymi*.

(17) Jeśli V jest przestrzenią liniową, to zbiór wszystkich odwracalnych przekształceń liniowych $V \to V$ jest grupą liniową, którą oznaczamy $\mathrm{GL}(V)$.

(18) Niech $n \geq 1$. Przekształcenie $f : \mathbb{R}^n \to \mathbb{R}^n$ nazywamy izometrią, jeśli $\|fx - fy\| = \|x - y\|$ dla dowolnych $x, y \in \mathbb{R}^n$. Zbiór wszystkich izometrii przestrzeni $\mathbb{R}^n$ z działaniem składania funkcji jest grupą, którą oznaczamy $\mathrm{Iso}(\mathbb{R}^n)$.

(19) Niech $n \geq 3$ oraz niech P_n będzie (standardowym) n-kątem foremnym (tzn. wielokątem wypukłym o wierzchołkach $(\cos \frac{2\pi k}{n}, \sin \frac{2\pi k}{n})$, $k = 0, \ldots, n-1$). Symetrią wielokąta P_n nazywamy taką izometrię f płaszczyzny $\mathbb{R}^2$, że $f(P_n) = P_n$. Zbiór wszystkich symetrii n-kąta foremnego jest grupą, którą oznaczamy D_n. Grupy tej postaci nazywamy *grupami*

*dyhedralnymi*7. Grupa D_n ma $2n$ elementów: składa się ona z identyczności, $n-1$ obrotów o kąty $\frac{2\pi k}{n}$, $k = 1, \ldots, n-1$, oraz n odbić względem n osi symetrii.

Niech G z działaniem $\cdot$ będzie grupą oraz $a \in G$. Definiujemy indukcyjnie a^m dla $m \geq 0$ w następujący sposób:

$$a^m = \begin{cases} 1 & m = 0 \\ a^{m-1}a & m > 0 \end{cases}.$$

Ponadto dla $m < 0$ oznaczamy $a^m = (a^{-1})^{-m}$. Analogicznie definiujemy elementy ma w sytuacji, gdy działanie w G oznaczane jest przez $+$.

Stwierdzenie 1.1.3. *Niech G będzie grupą.*

(1) $a^m a^n = a^{m+n}$, $a \in G$, $m, n \in \mathbb{Z}$.

(2) $(a^m)^n = a^{mn}$, $a \in G$, $m, n \in \mathbb{Z}$.

(3) *Jeśli ponadto działanie $\cdot$ jest przemienne, to* $(ab)^n = a^n b^n$, $a, b \in G$, $n \in \mathbb{Z}$.

Dowód. Ćwiczenie. □

1.2 Podgrupy

Definicja. Niech G będzie grupą. Podzbiór $H \subseteq G$ nazywamy *podgrupą grupy G*, jeśli spełnione są następujące warunki:

(1) $1 \in H$;

(2) jeśli $a, b \in H$, to $ab \in H$;

(3) jeśli $a \in H$, to $a^{-1} \in H$.

Jeśli H jest podgrupą grupy G, to piszemy $H \leq G$. Ponadto, gdy $H \neq G$, to piszemy $H < G$.

Ćwiczenie 1.2.1. Niech G będzie grupą. Udowodnić, że podzbiór $H \subseteq G$ jest podgrupą wtedy i tylko wtedy, gdy $H \neq \emptyset$ oraz jeśli $a, b \in H$, to $ab^{-1} \in H$.

Zauważmy, że podgrupa H grupy G jest grupą ze względu na działanie $\cdot$ obcięte do H. Jeśli K jest podgrupą grupy H oraz H jest podgrupą grupy G, to K jest podgrupą grupy G. Ponadto, jeśli K jest podgrupą grupy G oraz H jest podgrupą grupy G zawierającą K, to K jest podgrupą grupy H.

Ponadto, jeśli X i Y są dwoma podzbiorami, to przez XY oznaczać będziemy zbiór złożony z wszystkich iloczynów postaci xy, $x \in X$, $y \in Y$. Zamiast $\{a\}Y$ i $X\{a\}$ piszemy aY i Ya odpowiednio. Podobnie przez X^{-1} oznaczać będziemy zbiór wszystkich elementów postaci x^{-1}, $x \in X$. Zauważmy, że ze Stwierdzenia 1.1.2 wynika, że $(XY)^{-1} = Y^{-1}X^{-1}$. Ponadto, gdy grupa jest abelowa, to $XY = YX$. W przypadku notacji addytywnej analogicznie wprowadzamy oznaczenie $X + Y$ oraz $-X$.

Korzystając z powyższej notacji definicję podgrupy możemy zapisać następująco: podzbiór H grup G jest podgrupą, jeśli

(1) $1 \in H$;

(2) $HH \subseteq H$;

(3) $H^{-1} \subseteq H$.

Przykłady. (1) Jeśli G jest grupą, to $\{1\}$ oraz G są podgrupami grupy G.

(2) Jeśli $m > 0$, to $m\mathbb{Z} \leq \mathbb{Z}$.

(3) Jeśli $m > 0$, to $\mathbb{Z}_m$ nie jest podgrupą grupy $\mathbb{Z}$.

(4) Jeśli L jest podciałem ciała K, to $L \leq K$ oraz $L^* \leq K^*$.

(5) $\mathbb{Z} < \mathbb{Q}$.

(6) $\mathbb{Q}_+ < \mathbb{Q}^*$, $\mathbb{R}_+ < \mathbb{R}^*$ oraz $\mathbb{Q}_+ < \mathbb{R}_+$.

(7) $\mathbb{C}_\infty < \mathbb{T} < \mathbb{C}^*$ oraz jeśli $m > 0$, to $\mathbb{C}_m < \mathbb{C}_\infty$.

(8) Jeśli $m, n > 0$, to $\mathbb{C}_m < \mathbb{C}_n$ wtedy i tylko wtedy, gdy m dzieli n.

(9) Jeśli K jest ciałem oraz $n > 0$, to $\mathrm{SL}_n(K) < \mathrm{GL}_n(K)$.

(10) Jeśli V jest przestrzenią liniową, to $\mathrm{GL}(V) < S(V)$.

(11) Jeśli $n > 0$, to $\mathrm{Iso}(\mathbb{R}^n) < S(\mathbb{R}^n)$.

(12) Jeśli $n > 0$, to $D_n < \mathrm{Iso}(\mathbb{R}^2)$.

Jeśli H jest podgrupą grupy G, to przez $\sim_H$ oznaczać będziemy relację w G zdefiniowaną poprzez warunek:

$$a \sim_H b \text{ wtedy i tylko wtedy } a^{-1}b \in H.$$

Stwierdzenie 1.2.1. *Niech H będzie podgrupą grupy G. Relacja $\sim_H$ jest relacją równoważności w G. Klasa abstrakcji elementu $a \in G$ względem $\sim_H$ jest równa aH. Ponadto $|H| = |aH|$ dla każdego $a \in H$.*

Dowód. Bezpośrednio z definicji oraz własności podgrupy wynika, że relacja $\sim_H$ jest zwrotna, symetryczna i przechodnia, zatem istotnie jest relacją równoważności. Zauważmy, że $a \sim_H b$ wtedy i tylko wtedy, gdy $a^{-1}b \in H$, a więc $b = a(a^{-1}b) \in aH$. Ponadto łatwo widać, że funkcja $H \ni b \mapsto ab \in aH$ jest bijekcją – funkcja odwrotna dana jest wzorem $aH \ni b \mapsto a^{-1}b \in H$. □

Zauważmy, że z powyższego stwierdzenia wynika między innymi, że jeśli H jest podgrupą grupy G oraz $a \in H$, to $aH = H$. Istotnie, gdy $a \in H$, to $a \sim_H 1$, a więc $aH = 1H = H$.

Jeśli H jest podgrupą grupy G, to zbiór klas abstrakcji relacji $\sim_H$ oznaczać będziemy G/H, a jego elementy nazywać *warstwami lewostronnymi podgrupy H w G*. Ilość warstw lewostronnych oznaczać będziemy $[G : H]$ oraz nazywać *indeksem podgrupy H w G* (może być to nieskończona liczba kardynalna).

Przykłady. (1) $[G : G] = 1$ oraz $[G : \{1\}] = |G|$.

(2) Jeśli $m > 0$, to $[\mathbb{Z} : m\mathbb{Z}] = m$.

(3) Jeśli L jest podciałem ciała K takim, że $\dim_L K < \infty$, to $[K : L] = |L|^{\dim_L K - 1}$. W szczególności $[\mathbb{C} : \mathbb{R}] = 2^{\aleph_0}$.

(4) $[\mathbb{Q} : \mathbb{Z}] = \aleph_0$ i $[\mathbb{R} : \mathbb{Z}] = 2^{\aleph_0}$.

(5) $[\mathbb{R}^* : \mathbb{Q}^*] = [\mathbb{C}^* : \mathbb{R}^*] = [\mathbb{C}^* : \mathbb{Q}^*] = 2^{\aleph_0}$.

(6) $[\mathbb{Q}^* : \mathbb{Q}_+] = [\mathbb{R}^* : \mathbb{R}_+] = 2$.

(7) $[\mathbb{C}_* : \mathbb{T}] = [\mathbb{T} : \mathbb{C}_\infty] = 2^{\aleph_0}$ oraz jeśli $m > 0$, to $[\mathbb{T} : \mathbb{C}_m] = 2^{\aleph_0}$.

(8) Jeśli $m, n > 0$ oraz m dzieli n, to $[\mathbb{C}_n : \mathbb{C}_m] = \frac{m}{n}$.

(9) Jeśli K jest ciałem oraz $n > 0$, to $[\mathrm{GL}_n(K) : \mathrm{SL}_n(K)] = |K^*|$.

Lemat 1.2.2. *Niech H będzie podgrupą grupy G. Wtedy istnieją elementy a_i, $i \in G/H$, takie, że $G = \bigcup_{i \in G/H} a_i H$ oraz $a_i H \cap a_j H = \emptyset$ dla $i \neq j$. Ponadto, jeśli istnieją element b_k, $k \in I$, takie, że $G = \bigcup_{k \in I} b_k H$ oraz $b_k H \cap b_l H = \emptyset$ dla $k \neq l$, to $|I| = |G/H|$.*

Dowód. Pierwsza część lematu jest sformułowaniem faktu, że jeśli $\sim$ jest relacją równoważności na zbiorze X, to X jest sumą wszystkich klas abstrakcji oraz dwie różne klasy abstrakcji są rozłączne, w przypadku $\sim = \sim_H$ oraz $X = G$ z wykorzystaniem Stwierdzenia 1.2.1. Dla dowodu drugiej części rozważmy funkcję $f : I \to G/H$ daną wzorem $f(k) = b_k H$, $k \in I$. Z założenia $G = \bigcup_{k\in I} b_k H$ wynika, że f jest surjekcją, z faktu, że $b_k H \cap b_l H = \emptyset$ dla $k \neq l$ otrzymujemy, że f jest injekcją. Zatem f jest bijekcją, co kończy dowód. □

Twierdzenie 1.2.3 (Lagrange). *Jeśli H jest podgrupą grupy G, to $|G| = [G : H]|H|$. W szczególności, jeśli grupa G jest skończona, to $|H|$ dzieli $|G|$.*

Dowód. Z Lematu 1.2.2 wiemy, że istnieją elementy a_i, $i \in G/H$, takie, że $G = \bigcup_{i\in G/H} a_i H$ oraz $a_i H \cap a_j H = \emptyset$ dla $i \neq j$. Ponadto ze Stwierdzenia 1.2.1 wynika też, że $|a_i H| = |H|$ dla wszystkich $i \in G/H$, co kończy dowód twierdzenia. □

Twierdzenie 1.2.4. *Jeśli $K \leq H \leq G$, to $[G : K] = [G : H][H : K]$.*

Dowód. Z Lematu 1.2.2 wiemy, że istnieją elementy a_i, $i \in G/H$, taki, że $G = \bigcup_{i\in G/H} a_i H$ oraz $a_i H \cap a_j H = \emptyset$ dla $i \neq j$. Analogicznie istnieją elementy b_k, $k \in H/K$, takie, że $H = \bigcup_{k\in H/K} b_k K$ oraz $b_k H \cap b_l H = \emptyset$ dla $k \neq l$. Wtedy $aH = \bigcup_{k\in H/K} ab_k K$ dla dowolnego $a \in G$, skąd $G = \bigcup_{i\in G/H} \bigcup_{k\in H/K} a_i b_k K$. Na mocy lematu 1.2.2 wystarczy udowodnić, że jeśli $(i, k) \neq (j, l)$, to $a_i b_k K \cap a_j b_l K = \emptyset$, co na mocy Stwierdzenia 1.2.1 oraz własności relacji równoważności jest równoważne temu, że $a_i b_k K \neq a_j b_l K$. Przypuśćmy zatem, że $a_i b_k K = a_j b_l K$. Oznacza to, że $b_l k{-}1 a_i^{-1} a_j b_l \in K$, skąd wynika, że $a_i^{-1} a_j \in b_k K b_l^{-1}$. Ponieważ $b_k, b_l \in H$ oraz $K < H$, więc wnioskujemy stąd, że $a_i^{-1} a_j \in H$, a więc $i = j$. Wykorzystując ten fakt otrzymujemy, że $b_k^{-1} b_l \in K$, $k = l$, co kończy dowód. □

1.3 Kongruencje, dzielniki normalne i grupy ilorazowe

Definicja. Niech G będzie grupą. Relację równoważności $\sim$ w G nazywamy *kongruencją w G*, jeśli dla dowolnych $a, b, c, d \in G$, z faktu, że $a \sim b$ oraz $c \sim d$ wynika, że $ab \sim cd$.

Zauważmy, że jeśli $\sim$ jest kongruencją w grupie G oraz $a \sim b$, to $a^{-1} \sim b^{-1}$. Istotnie, ponieważ $a \sim b$ oraz $a^{-1} \sim a^{-1}$, więc $1 = aa^{-1} \sim ba^{-1}$. Wykorzystując dodatkowo fakt, że $1 = bb^{-1}$ oraz, że $b^{-1} \sim b^{-1}$ otrzymujemy, że $b^{-1} = b^{-1}bb^{-1} \sim b^{-1}ba^{-1} = a^{-1}$.

Ćwiczenie 1.3.1. Udowodnić, że relacja równoważności $\sim$ w grupie G jest kongruencją wtedy i tylko wtedy, gdy dla dowolnych $a, b, c \in G$, z faktu, że $a \sim b$ wynika, że $ac \sim bc$ oraz $ca \sim cb$.

Jeśli $\sim$ jest kongruencją w grupie G, to przez $N_\sim$ oznaczać będziemy klasę abstrakcji 1.

Przykłady. (1) W dowolnej grupie G relacja $=$ (tzn. a jest w relacji z b wtedy i tylko wtedy, gdy $a = b$) jest kongruencją oraz $N_= = \{1\}$. Podobnie relacja totalna $G \times G$ (tzn. dowolne dwa elementy są ze sobą w relacji) jest kongruencją oraz $N_{G\times G} = G$.

(2) Jeśli $m > 0$ to relacja $\equiv_m$ przystawania modulo m jest kongruencją w $\mathbb{Z}$ oraz $N_{\equiv m} = m\mathbb{Z}$.

(3) Jeśli K jest ciałem oraz $n > 0$, to relacja $\sim$ w $\mathrm{GL}_n(K)$ zadana poprzez warunek $A \simeq B$ wtedy i tylko wtedy, gdy $\det A = \det B$ jest kongruencją oraz $N_\sim = \mathrm{SL}_n(K)$.

Stwierdzenie 1.3.1. *Jeśli $\sim$ jest kongruencją w grupie G, to $N_\sim \leq G$ oraz $aN_\sim a^{-1} \subseteq N_\sim$ dla dowolnego $a \in G$.*

Dowód. Prosta konsekwencja własności relacji kongruencji. □

Definicja. Podgrupę N grupy G będziemy nazywać *dzielnikiem normalnym grupy G* wtedy i tylko wtedy, gdy $aNa^{-1} \subseteq N$ dla dowolnego $a \in G$. Jeśli N jest dzielnikiem normalnym grupy G, to piszemy $N \trianglelefteq G$. Ponadto, gdy $N \neq G$, to piszemy $N \triangleleft G$.

Zauważmy, że w grupie abelowej każda podgrupa jest dzielnikiem normalnym. W przypadku dzielników normalnych nie musi być prawdą stwierdzenie, że jeśli N jest dzielnikiem normalnym grupy G oraz M jest dzielnikiem normalnym grupy N, to M jest dzielnikiem normalnym grupy G. Z drugiej strony, gdy N jest dzielnikiem normalnym grupy G oraz H jest podgrupą grupy G zawierającą N, to N jest dzielnikiem normalnym grupy H.

Lemat 1.3.2. *Niech N będzie podgrupą grupy G.*

(1) *N jest dzielnikiem normalnym grupy G wtedy i tylko wtedy, gdy dla dowolnego $a \in N$ zachodzi $aNa^{-1} = N$.*

(2) *N jest dzielnikiem normalnym grupy G wtedy i tylko wtedy, gdy dla dowolnego $a \in N$ zachodzi $aN = Na$.*

Dowód. (1) Oczywiście, jeśli $aNa^{-1} = N$ dla dowolnego $a \in N$, to N jest dzielnikiem normalnym. Przypuśćmy teraz, że N jest dzielnikiem normalnym. Aby udowodnić, że $aNa^{-1} = N$ dla dowolnego $a \in N$. musimy pokazać, że $N \subseteq aNa^{-1}$ dla dowolnego $a \in N$. Wiemy jednak, że $N = aa^{-1}Naa^{-1}$.

Ponieważ $(a^{-1})^{-1} = a$, więc $a^{-1}Na \subseteq N$, skąd $N \subseteq aNa^{-1}$, co kończy dowód pierwszej części lematu.

(2) Jeśli N jest dzielnikiem normalnym, to korzystając z punktu (1) mamy ciąg równości $Na = aNa^{-1}a = aN$ dla dowolnego $a \in G$. Załóżmy zatem, że $aN = Na$ dla dowolnego $a \in N$. Wtedy $aNa^{-1} = Naa^{-1} = N$, co kończy dowód. □

Zauważmy, że punkt (2) powyższego lematu implikuje, że jeśli N jest dzielnikiem normalnym grupy G, to $XN = NX$ dla dowolnego zbioru X. Istotnie, $XN = \bigcup_{x\in X} xN = \bigcup_{x\in X} Nx = NX$.

Stwierdzenie 1.3.3. *Jeśli N jest dzielnikiem normalnym grupy G, to relacja $\sim_N$ jest relacją kongruencji oraz $N_{\sim_N} = N$. Z drugiej strony, jeśli $\sim$ jest relacją kongruencji, to $\sim_{N_\sim}=\sim$.*

Dowód. Ze Stwierdzenia 1.2.1 wiemy, że $\sim_N$ jest relacją równoważności. Przypuśćmy zatem, że $a \sim_N b$ oraz $c \sim_N d$, tzn. $aN = bN$ oraz $cN = dN$. Wtedy $acN = adN = aNd = bNd = bdN$, skąd $ac \sim_N bd$, a więc $\sim_N$ jest istotnie kongruencją. Przypomnijmy, że $N_{\sim_N}$ jest warstwą 1 w relacji $\sim_N$, a ta na mocy Stwierdzenia 1.2.1 jest równa $1N = N$. Na koniec zauważmy, że $a \sim_{N_\sim} b$ wtedy i tylko wtedy, gdy $a^{-1}b \in N_\sim$, a więc $a^{-1}b \sim 1$, co oznacza, że $b \sim a$, gdyż zawsze $a \sim a$. □

Stwierdzenie 1.3.4. *Jeśli $\sim$ jest relacją kongruencji, to w zbiorze klas abstrakcji $G/\sim$ następująca definicja działania $\cdot$*

$$[a]_\sim \cdot [b]_\sim = [ab]_\sim,\ a, b \in G,$$

jest poprawna oraz $G/\sim$ z działaniem $\cdot$ jest grupą.

Dowód. Poprawność definicji jest natychmiastową konsekwencją definicji relacji kongruencji. Łączność działania $\cdot$ jest oczywista. Elementem naturalnym jest $[1]_\sim$, zaś elementem odwrotnym do $[a]_\sim$, klasa $[a^{-1}]_\sim$. □

Wniosek 1.3.5. *Jeśli N jest dzielnikiem normalnym, to w zbiorze G/N następująca definicja działania $\cdot$*

$$aN \cdot bN = abN$$

jest poprawna oraz G/N z działaniem $\cdot$ jest grupą.

Dowód. Jest to przeformułowanie wcześniejszego stwierdzenia wykorzystujące Stwierdzenie 1.3.3 oraz Stwierdzenie 1.2.1. □

1.4 Homomorfizmy grup

Definicja. Jeśli G i H są grupami, to funkcję $f : G \to H$ nazywamy *homomorfizmem grup* jeśli

(1) $f(ab) = f(a)f(b)$ dla dowolnych $a, b \in G$;

(2) $f(1) = 1$;

(3) $f(a^{-1}) = (f(a))^{-1}$ dla dowolnego $a \in G$.

Homomorfizm f nazwiemy *monomorfizmem*, jeśli f jest injekcją, *epimorfizmem*, jeśli f jest surjekcją, *izomorfizmem*, jeśli f jest bijekcją. Jeśli $G = H$, to homomorfizm f nazywamy *endomorfizmem*, zaś gdy jest on dodatkowo *izomorfizmem*, to mówimy, że jest to *automorfizm*. *Jądrem homomorfizmu* f nazywamy zbiór wszystkich $a \in G$, dla których $f(a) = 1$. *Obrazem homomorfizmu* f nazywamy obraz zbioru G przy działaniu funkcji f. Jądro homomorfizmu f będziemy oznaczać $\operatorname{Ker} f$, zaś jego obraz $\operatorname{Im} f$. Jeśli istnieje izomorfizm $G \to H$ to mówimy, że *grupy G i H są izomorficzne* oraz piszemy $G \simeq H$.

Lemat 1.4.1. *Jeśli G i H są grupami oraz $f : G \to H$ jest funkcją spełniającą warunek* (1) *z definicji homomorfizmu, to f jest homomorfizmem.*

Dowód. Mamy $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$. Mnożąc tę równość stronami (z dowolnej strony) przez $f(1)^{-1}$ otrzymujemy, że $f(1) = 1$. Podobnie $1 = f(1) = f(aa^{-1}) = f(a)f(a^{-1})$. Mnożąc tę równość stronami z prawej strony przez $(f(a))^{-1}$ dostajemy, że $f(a^{-1}) = (f(a))^{-1}$. □

Przykłady. (1) Jeśli H jest podgrupą grupy G, to funkcja $f : H \to G$ dana wzorem $f(a) = a$ jest homomorfizmem grup takim, że $\operatorname{Ker} f = \{1\}$ oraz $\operatorname{Im} f = H$. Homomorfizmy tej postaci nazywamy *naturalnymi włożeniami*.

(2) Jeśli N jest dzielnikiem normalnym grupy G, to funkcja $f : G \to G/N$ dana wzorem $f(a) = aN$ jest homomorfizmem grup takim, że $\operatorname{Ker} f = N$ oraz $\operatorname{Im} f = G/N$. Homomorfizmy tej postaci nazywamy *naturalnymi rzutowaniami*.

(3) Jeśli $f : G \to H$ jest homomorfizmem grup oraz $g : H \to K$ jest homomorfizmem grup, to $g \circ f : G \to K$ jest homomorfizmem grup.

(4) Jeśli $m > 0$, to funkcja $f : \mathbb{Z} \to \mathbb{Z}$ dana wzorem $f(k) = mk$ dla $k \in \mathbb{Z}$, jest homomorfizmem grup takim, że $\operatorname{Ker} f = \{0\}$ oraz $\operatorname{Im} f = m\mathbb{Z}$.

(5) Jeśli $m > 0$, to funkcja $f : m\mathbb{Z} \to \mathbb{Z}$ dana wzorem $f(k) = \frac{k}{m}$ dla $k \in \mathbb{Z}$, jest homomorfizmem grup takim, że $\operatorname{Ker} f = \{0\}$ oraz $\operatorname{Im} f = \mathbb{Z}$.

(6) Jeśli $m > 0$, to funkcja $f : \mathbb{Z} \to \mathbb{Z}_m$ dana wzorem $f(k) =$ reszta z dzielenia k przez m dla $k \in \mathbb{Z}$, jest homomorfizmem grup takim, że $\operatorname{Ker} f = m\mathbb{Z}$ oraz $\operatorname{Im} f = \mathbb{Z}_m$.

(7) Jeśli $m > 0$, to funkcja $f : \mathbb{Z} \to \mathbb{T}$ dana wzorem $f(k) = \cos(\frac{2\pi k}{m}) + i \sin(\frac{2\pi k}{m})$ dla $k \in \mathbb{Z}$, jest homomorfizmem grup takim, że $\operatorname{Ker} f = m\mathbb{Z}$ oraz $\operatorname{Im} f = \mathbb{C}_m$.

(8) Funkcja $f : \mathbb{Q} \to \mathbb{T}$ dana wzorem $f(q) = \cos(2\pi q) + i \sin(2\pi q)$ dla $q \in \mathbb{Q}$, jest homomorfizmem grup takim, że $\operatorname{Ker} f = \mathbb{Z}$ oraz $\operatorname{Im} f = \mathbb{C}_\infty$.

(9) Funkcja $f : \mathbb{R} \to \mathbb{T}$ dana wzorem $f(x) = \cos(2\pi x) + i \sin(2\pi x)$ dla $x \in \mathbb{R}$, jest homomorfizmem grup takim, że $\operatorname{Ker} f = \mathbb{Z}$ oraz $\operatorname{Im} f = \mathbb{T}$.

(10) Funkcja $f : \mathbb{R}_+ \to \mathbb{R}$ dana wzorem $f(x) = \ln x$ dla $x > 0$ jest homomorfizmem taki, że $\operatorname{Ker} f = \{1\}$ oraz $\operatorname{Im} f = \mathbb{R}$.

(11) Jeśli K jest ciałem oraz $n > 0$, to funkcja $f : \mathrm{GL}_n(K) \to K^*$ dana wzorem $f(A) = \det A$ dla $A \in \mathrm{GL}_n(K)$, jest homomorfizmem grup takim, że $\operatorname{Ker} f = \mathrm{SL}_n(K)$ oraz $\operatorname{Im} f = K^*$.

Lemat 1.4.2. *Niech $f : G \to H$ będzie homomorfizmem grup.*

(1) *Jeśli K jest podgrupą grupy G, to $f(K)$ jest podgrupą grupy H.*

(2) *Jeśli K jest podgrupą grupy H, to $f^{-1}(K)$ jest podgrupą grupy H.*

(3) *Jeśli N jest dzielnikiem normalnym grupy G oraz f jest epimorfizmem, to $f(N)$ jest dzielnikiem normalnym grupy H.*

(4) *Jeśli N jest dzielnikiem normalnym grupy H, to $f^{-1}(N)$ jest dzielnikiem normalnym grupy G.*

Dowód. Bezpośrednie rachunki. □

Stwierdzenie 1.4.3. *Niech $f : G \to H$ będzie homomorfizmem grup.*

(1) $\operatorname{Ker} f$ *jest dzielnikiem normalnym grupy G.*

(2) $\operatorname{Im} f$ *jest podgrupą grupy H.*

(3) *f jest monomorfizmem wtedy i tylko wtedy, gdy* $\operatorname{Ker} f = \{1\}$.

(4) *f jest epimorfizmem wtedy i tylko wtedy, gdy* $\operatorname{Im} f = H$.

(5) *f jest izomorfizmem wtedy i tylko wtedy, gdy* $\operatorname{Ker} f = \{1\}$ *oraz* $\operatorname{Im} f = H$.

(6) *Jeśli f jest izomorfizmem, to funkcja odwrotna do f też jest homomorfizmem.*

Dowód. Pierwsze dwa punkty wynikają natychmiast z powyższego lematu, gdyż $\operatorname{Ker} f = f^{-1}(\{1\})$ oraz $\operatorname{Im} f = f(G)$. Dla dowodu punktu (3) zauważmy, że jeśli f jest monomorfizmem, to oczywiście $\operatorname{Ker} f = \{1\}$. Przypuśćmy teraz, że $\operatorname{Ker} f = \{1\}$ oraz $f(a) = f(b)$. Wtedy $f(ab^{-1}) = 1$, tzn. $ab^{-1} \in \operatorname{Ker} f$, skąd natychmiast wynika, że $a = b$. Punkt (4) jest oczywisty. Punkt (5) jest natychmiastową konsekwencją punktów (3) oraz (4) i definicji izomorfizmu. Dla dowodu punktu (6) oznaczmy przez g funkcję odwrotną do f. Jeśli $c, d \in H$, to istnieją elementu $a, b \in G$ taki, że $c = f(a)$ oraz $d = g(b)$. Oczywiście wtedy $g(c) = a$ oraz $g(d) = b$. Ponadto $g(cd) = g(f(a)f(b)) = g(f(ab)) = ab = g(c)g(d)$, co kończy dowód na mocy Lematu 1.4.1. □

Zauważmy, że zbiór wszystkich automorfizmów grupy G tworzy grupę, którą nazywamy *grupą automorfizmów grupy G* oraz oznaczamy $\operatorname{Aut}(G)$. Zauważmy, że $\operatorname{Aut}(G)$ jest podgrupą grupy $S(G)$.

Wniosek 1.4.4. *Jeśli $f : G \to H$ jest monomorfizmem grup, to funkcja $g : G \to \operatorname{Im} f$ dana wzorem $g(a) = f(a)$ jest izomorfizmem.*

Dowód. Zauważmy, że funkcja g jest dobrze określone i jest homomorfizmem. Ponadto $\operatorname{Ker} g = \operatorname{Ker} f = \{1\}$ oraz $\operatorname{Im} g = \operatorname{Im} f$, zatem jest g izomorfizmem. □

Twierdzenie 1.4.5. *Niech $f : G \to H$ będzie homomorfizmem grup oraz N dzielnikiem normalnym grupy G takim, że $N \subseteq \operatorname{Ker} f$. Wtedy odwzorowanie $g : G/N \to H$ dane wzorem $g(aN) = f(a)$ jest poprawnie określone oraz jest homomorfizmem,* $\operatorname{Ker} g = \operatorname{Ker} f/N$ *i* $\operatorname{Im} g = \operatorname{Im} f$.

Dowód. Przypuśćmy, że $aN = bN$ dla $a, b \in G$. Wtedy $a = a \cdot 1 = bn$ dla pewnego $n \in N$, skąd $f(a) = f(bn) = f(b)f(n) = f(b) \cdot 1 = f(b)$. Zatem definicja funkcji g jest poprawna. Ponadto $g(aN \cdot bN) = g(abN) = f(ab) = f(a)f(b) = g(aN)g(bN)$, a więc g jest homomorfizmem. Oczywiście g jest epimorfizmem. Ponadto $aN \in \operatorname{Ker} g$ wtedy i tylko wtedy, gdy $f(a) = 1$, tzn. $a \in \operatorname{Ker} f$, a więc $\operatorname{Ker} g = \operatorname{Ker} f/N$. □

Wniosek 1.4.6 (Pierwsze Twierdzenie o Izomorfizmie). *Jeśli $f : G \to H$ jest homomorfizmem grup, to funkcja $G/\operatorname{Ker} f \in a \operatorname{Ker} f \mapsto f(a) \in \operatorname{Im} f$ jest izomorfizmem grup.*

Dowód. Niech $g : G/\operatorname{Ker} f \to H$ będzie funkcją daną wzorem $g(a \operatorname{Ker} f) = f(a)$. Z poprzedniego twierdzenia zastosowanego dla $N = \operatorname{Ker} f$ wynika, że g jest homomorfizmem, $\operatorname{Ker} g = \operatorname{Ker} f/\operatorname{Ker} f = \{1\}$ oraz $\operatorname{Im} f = \operatorname{Im} g$. Korzystając z Wniosku 1.4.4 otrzymujemy tezę wniosku. □

Przykłady. (1) Jeśli $m > 0$, to funkcja $\mathbb{Z}/m\mathbb{Z} \ni k + m\mathbb{Z} \mapsto$ reszta z dzielnie k przez $m \in \mathbb{Z}_m$ jest izomorfizmem.

(2) Jeśli $m > 0$, to funkcja $\mathbb{Z}/m\mathbb{Z} \ni k + m\mathbb{Z} \mapsto \cos(\frac{2\pi k}{m}) + i \sin(\frac{2\pi k}{m}) \in \mathbb{C}_m$ jest izomorfizmem.

(3) Jeśli $m > 0$, to funkcja $\mathbb{Z}_m \ni k \mapsto \cos(\frac{2\pi k}{m}) + i \sin(\frac{2\pi k}{m}) \in \mathbb{C}_m$ jest izomorfizmem.

(4) Funkcje $\mathbb{R}/\mathbb{Z} \ni x + \mathbb{Z} \mapsto \cos(2\pi x) + i \sin(2\pi x) \in \mathbb{T}$ oraz $\mathbb{Q}/\mathbb{Z} \ni q + \mathbb{Z} \mapsto (2\pi q) + i \sin(2\pi q) \in \mathbb{C}_\infty$ są izomorfizmami.

(5) Funkcja $\mathbb{R}_+ \ni x \mapsto \ln x \in \mathbb{R}$ jest izomorfizmem.

(6) Jeśli K jest ciałem, to $\operatorname{GL}_n(K)/\operatorname{SL}_n(K) \ni A \in \operatorname{SL}_n(K) \mapsto \det AK^*$ jest izomorfizmem.

Przypomnijmy, że punkt (2) Lematu 1.3.2 implikuje, jeśli N jest dzielnikiem normalnym grupy G, to $XN = NX$ dla dowolnego podzbioru X grupy G.

Lemat 1.4.7. *Niech G będzie grupą, niech H będzie podgrupą grupy G oraz niech N będzie dzielnikiem normalnym grupy G.*

(1) *$H \cap N$ jest dzielnikiem normalnym grupy H.*

(2) *HN jest podgrupą grupy G.*

Dowód. Punkt pierwszy jest prostym ćwiczeniem wykorzystującym definicję podgrupy i dzielnika normalnego. Dla dowodu punkt (2) zauważmy najpierw, że $1 \in H$ oraz $1 \in N$, więc $1 = 1 \cdot 1 \in HN$. Ponadto, $HNHN = HHNN \subseteq HN$ oraz $(HN)^{-1} = N^{-1}H^{-1} \subseteq NH = HN$, co kończy dowód. □

Wniosek 1.4.8 (Drugie Twierdzenie o Izomorfizmie). *Jeśli G jest grupą, H jest podgrupą grupy G oraz N jest dzielnikiem normalnym grupy G, to funkcja $H/(H \cap N) \ni a(H \cap N) \mapsto aN \in HN/N$ jest izomorfizmem grup.*

Dowód. Niech $f : H \to HN/N$ będzie odwzorowaniem danym wzorem $f(a) = aN$. Funkcja f jest homomorfizmem grup, gdyż jest złożeniem naturalnego włożenia $H \to HN$ oraz naturalnego rzutowania $HN \to HN/N$. Łatwo sprawdzić, że $\operatorname{Im} f = HN/N$, gdyż $abN = aN = f(a)$ dla $a \in H$ oraz $b \in N$. Ponadto $\operatorname{Ker} f = H \cap N$, gdyż $aN = N$ wtedy i tylko wtedy, gdy $a \in N$. Teza wynika zatem z Pierwszego Twierdzenia o Izomorfizmie. □

Wniosek 1.4.9 (Trzecie Twierdzenie o Izomofizmie). *Jeśli M i N są dzielnikami normalnymi grupy G takimi, że $M \subseteq N$, to N/M jest dzielnikiem normalnym grupy G/M oraz funkcja $(G/M)/(N/M) \ni (aM)(N/M) \mapsto aN \in G/N$ jest izomorfizmem.*

Dowód. Niech $f : G \to G/N$ będzie naturalnym rzutowaniem. Wiadomo, że $\operatorname{Ker} f = N$ i $\operatorname{Im} f = G/N$. Z Twierdzenia 1.4.5 zastosowanego dla M wynika, że funkcja $g : G/M \to G/N$ dana wzorem $g(aM) = aN$ jest homomorfizmem, $\operatorname{Ker} g = N/M$ oraz $\operatorname{Im} g = G/N$. Stosując teraz Pierwsze Twierdzenie o Izomorfizmie dla g dostajemy tezę. □

1.5 Grupy cykliczne

Stwierdzenie 1.5.1. *Jeśli H_i, $i \in I$, są podgrupami grupy G oraz $I \neq \emptyset$, to $\bigcap H_i$ jest podgrupą grupy G.*

Dowód. Proste ćwiczenie na definicję podgrupy. □

Wniosek 1.5.2. *Jeśli X jest podzbiorem grupy G, to istnieje najmniejsza (w sensie zawierania zbiorów) podgrupa H grupy G zawierająca zbiór X.*

Dowód. Niech H_i, $i \in I$, będą wszystkimi podgrupami grupy G zawierającymi zbiór X. Zauważmy, że $I \neq \emptyset$, gdyż G jest podgrupą grupy G zawierająca zbiór X. Z poprzedniego stwierdzenia wynika zatem, że $H = \bigcap_{i \in I} H_i$ jest podgrupą grupy G. Oczywiście $X \subseteq H$. Ponadto, jeśli K jest podgrupą grupy G zawierającą zbiór X, to $K = H_i$ dla pewnego i. Zatem $H \subseteq K$, a więc H jest najmniejszą podgrupą grupy G zawierającą zbiór X. □

Najmniejszą podgrupę grupy G zawierającą zbiór X będziemy oznaczać $\langle X \rangle$ i nazywać *podgrupą generowaną przez X*. Jeśli $X = \{x_1, \ldots, x_n\}$, to będziemy też pisać $\langle x_1, \ldots, x_n \rangle$, zamiast $\langle \{x_1, \ldots, x_n\} \rangle$. *Rzędem elementu $a \in G$* nazwiemy rząd grupy $\langle a \rangle$. Rząd elementu a będziemy oznaczać przez $|a|$. Gdy istnieje element $a \in G$ taki, że $G = \langle a \rangle$, to grupę G nazwiemy *cykliczną*. W tej sytuacji element a nazywamy *generatorem grupy G* i mówimy, że *grupa G jest generowana przez element a*.

Przykłady. (1) $\mathbb{Z} = \langle 1 \rangle$.

(2) Jeśli $m > 0$, to $m\mathbb{Z} = \langle m \rangle$.

(3) Jeśli $m > 0$, to $\mathbb{Z}_m = \langle 1 \rangle$.

Lemat 1.5.3. *Niech $f : G \to H$ będzie homomorfizmem grup. Jeśli X jest podzbiorem grupy G, to $\langle f(X) \rangle = f(\langle X \rangle)$.*

Dowód. Oczywiście $X \subseteq \langle X \rangle$, więc $f(X) \subseteq f(\langle X \rangle)$. Ponieważ $f(\langle X \rangle)$ jest podgrupą grupy H na mocy Lematu 1.4.2, więc także $\langle f(X) \rangle \subseteq f(\langle X \rangle)$. Dla dowodu przeciwnego zawierania oznaczmy przez K podgrupę $f^{-1}(\langle f(X) \rangle)$ grupy G (jest to podgrupa na mocy Lematu 1.4.2). Oczywiście $X \subseteq K$, zatem $\langle X \rangle \subseteq K$. Stąd $f(\langle X \rangle) \subseteq f(K) \subseteq \langle f(X) \rangle$, co kończy dowód. □

Niech Y będzie podzbiorem grupy G. Dla liczby naturalnej $n \geq 0$ definiujemy zbiór Y^n w indukcyjny sposób następująco:

$$Y^n = \begin{cases} \{1\} & n = 0, \\ Y^{n-1}Y & n > 0, \end{cases}$$

(tzn. dla $n > 0$, $Y^n = \underbrace{Y \cdots Y}_{n \text{ razy}}$).

Stwierdzenie 1.5.4. *Jeśli X jest podzbiorem grupy G, to $\langle X \rangle = \bigcup_{n \geq 0}(X \cup X^{-1})^n$ (tzn. $\langle X \rangle = \{x_1 \dots x_n \mid x_i \in X$ lub $x_i^{-1} \in X$, $i = 1, \dots, n$, $n \geq 0\}$).*

Dowód. Niech $H = \bigcup_{n \geq 0} Y^n$, gdzie $Y = X \cup X^{-1}$. Ponieważ $X \subseteq \langle X \rangle$ oraz $\langle X \rangle$ jest podgrupą grupy G, więc $Y \subseteq \langle X \rangle$, skąd $Y^n \subseteq \langle X \rangle$, zatem $H \subseteq \langle X \rangle$.

Pokażemy teraz, że H jest podgrupą grupy G. Ponieważ $Y^0 = \{1\}$, więc $1 \in H$. Ponadto $HH = (\bigcup_{n \geq 0} Y^n)(\bigcup_{n \geq 0} Y^n) = \bigcup_{m,n \geq 0} Y^n Y^m = \bigcup_{m,n \geq 0} Y^{n+m} = \bigcup_{k \geq 0} Y^k = H$.

Aby udowodnić, że $H^{-1} \subseteq H$ pokażemy najpierw, że $(Y^n)^{-1} = Y^n$. Dla $n = 0$ teza jest oczywista. Dla $n = 1$ mamy $(Y^1)^{-1} = (X \cup X^{-1})^{-1} = X^{-1} \cup X = Y$. Gdy $n > 1$ oraz wiemy już, że $(Y^{n-1})^{-1} = Y^{n-1}$, to otrzymujemy, że $(Y^n)^{-1} = (Y^{n-1}Y)^{-1} = Y^{-1}(Y^{n-1})^{-1} = YY^{n-1} = Y^n$. Stąd $H^{-1} = (\bigcup_{n \geq 0} Y^n)^{-1} = \bigcup_{n \geq 0} (Y^n)^{-1} = \bigcup_{n \geq 0} Y^n = H$, a więc H istotnie jest podgrupą. Ponieważ $X \subseteq H$, więc $\langle X \rangle \subseteq H$, a to oznacza, że $\langle X \rangle = H$. □

Lemat 1.5.5. *Jeśli $X = \{a\}$, to $\bigcup_{0 \leq m \leq n}(X \cup X^{-1})^m = \{a^k \mid |k| \leq n\}$.*

Dowód. Proste zadanie na indukcję matematyczną. □

Wniosek 1.5.6. *Jeśli G jest grupą cykliczną generowaną przez element a, to $G = \{a^k \mid k \in \mathbb{Z}\}$.*

Dowód. Natychmiastowa konsekwencja dwóch poprzednich faktów. □

Stwierdzenie 1.5.7. *Jeśli G jest grupą oraz $a \in G$, to funkcja $f : \mathbb{Z} \to G$ dana wzorem $f(k) = a^k$ dla $k \in \mathbb{Z}$ jest homomorfizmem grup takim, że* $\operatorname{Im} f = \langle a \rangle$.

Dowód. Fakt, że f jest homomorfizmem wynika z punktu (1) Stwierdzenia 1.1.3. Część tezy poświęcona obrazowi jest natomiast konsekwencją powyższego wniosku. □

Stwierdzenie 1.5.8. *Jeśli H jest podgrupą grupy $\mathbb{Z}$ oraz $H \neq \{0\}$, to istnieje $m > 0$ takie, że $H = m\mathbb{Z}$.*

Dowód. Ponieważ $H \neq \{0\}$, więc istnieje $k \neq 0$, takie, że $k \in H$. Wtedy $|k| \in H$, gdyż $|k| = \pm k$. Niech $m = \min\{n \in H \mid n > 0\}$. Pokażemy, że $H = m\mathbb{Z}$. Oczywiście $m\mathbb{Z} \subseteq H$. Niech $l \in H$. Z twierdzenia o dzieleniu z resztą wiemy, że $l = qm + r$ dla $q \in \mathbb{Z}$ oraz $0 \leq r < m$. Ponieważ $r = l - qm$, więc $r \in H$, stąd $r = 0$, zatem $l = qm$ i $H \subseteq m\mathbb{Z}$. □

Twierdzenie 1.5.9. *Niech G będzie grupą cykliczną generowaną przez element a.*

(1) *Jeśli rząd grupy G jest nieskończony, to odwzorowanie $\mathbb{Z} \ni k \mapsto a^k \in G$ jest izomorfizmem.*

(2) *Jeśli $|G| = m$, to odwzorowanie $\mathbb{Z}_m \ni k \mapsto a^k \in G$ jest izomorfizmem.*

Dowód. Niech $f : \mathbb{Z} \to G$ będzie funkcją daną wzorem $f(k) = a^k$ dla $k \in \mathbb{Z}$. Ze Stwierdzenia 1.5.7 wynika, że f jest homomorfizmem grup oraz $\operatorname{Im} f = G$. Wiemy, że $\operatorname{Ker} f$ jest podgrupą grupy $\mathbb{Z}$. Na mocy poprzedniego stwierdzenia wiemy zatem, że gdy $\operatorname{Ker} f = 0$ lub istnieje $m > 0$ takie, że $\operatorname{Ker} f = m\mathbb{Z}$. Gdy $\operatorname{Ker} f = 0$, to f jest izomorfizmem. Gdy $\operatorname{Ker} f = m\mathbb{Z}$, to z Pierwszego Twierdzenia o Izomorfizmie wynika, że odwzorowanie $g : \mathbb{Z}/m\mathbb{Z} \to G$ dane wzorem $g(k + m\mathbb{Z}) = a^k$ dla $k \in \mathbb{Z}$ jest izomorfizmem. Przypomnijmy, że $h : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}_m$ dane wzorem $h(k) =$ reszta z dzielenia k przez m jest izomorfizmem. Stąd $gh^{-1} : \mathbb{Z}_m \to G$ jest izomorfizmem. Zauważmy, że $h^{-1}(k) = k + m\mathbb{Z}$ dla $k \in \mathbb{Z}_m$, skąd $gh^{-1}(k) = a^k$. Powyższe rozważania kończą dowód. Istotnie, z porównania ilości elementów w dziedzinie i przeciwdziedzinie wynika, że jeśli rząd grupy G jest nieskończony, to mamy do czynienia z przypadkiem $\operatorname{Ker} f = 0$, zaś gdy $|G| = m$, to $\operatorname{Ker} f = m\mathbb{Z}$. □

Wniosek 1.5.10. *Niech G będzie grupą oraz $a \in G$.*

(1) *Jeśli rząd elementu a jest nieskończony, to $a^k = 1$ wtedy i tylko wtedy, gdy $k = 0$ oraz elementy a^k, $k \in \mathbb{Z}$, są parami różne.*

(2) *Niech $|a| = m$.*

   (a) *m jest najmniejszą liczbą naturalną $n > 0$ taką, że $a^n = 1$.*

   (b) *$a^k = 1$ wtedy i tylko wtedy, gdy m dzieli k.*

(c) $a^k = a^l$ *wtedy i tylko wtedy, gdy* $k \equiv l \pmod{m}$.

(d) $\langle a \rangle = \{1 = a^0, a = a^1, a^2, \ldots, a^{m-1}\}$.

Dowód. Przypuśćmy najpierw, że rząd elementu a jest nieskończony. Wtedy funkcja $\mathbb{Z} \ni k \mapsto a^k \in \langle a \rangle$ jest izomorfizmem. Stąd wynika teza. Podobnie postępujemy w przypadku, gdy rząd elementu $|a| = m$, z tą różnicą, że tym razem wykorzystujemy izomorfizm $\mathbb{Z}_m \ni k \mapsto a^k \in \langle a \rangle$. □

1.6 Działanie grupy na zbiorze

Definicja. *Działaniem grupy G na zbiorze X* nazywamy każdą funkcję $G \times X \to X$, $(a, x) \mapsto ax$, taką, że

$$1x = x \text{ i } (ab)x = a(bx)$$

dla dowolnych $a, b \in G$ oraz $x \in X$. Mówimy też, że w powyższej sytuacji *grupa G działa na zbiorze X*.

Przykłady. (1) Jeśli X jest zbiorem, to grupa $S(X)$ działa na zbiorze X zgodnie ze wzorem

$$(f, x) \mapsto f(x) \text{ dla } f \in S(X) \text{ i } x \in X.$$

Powyższy wzór zadaje też działanie dowolnej podgrupy grupy $S(X)$.

(2) Niech G będzie grupą. Podgrupa H grupy G działa na G zgodnie ze wzorem

$$(a, b) \mapsto ab \text{ dla } a \in H \text{ i } b \in G.$$

Powyższe działanie grupy H nazywamy *działaniem przez* (lewe) *przesunięcia*.

(3) Niech G będzie grupą. Podgrupa H grupy G działa na G zgodnie ze wzorem

$$(a, b) \mapsto aba^{-1} \text{ dla } a \in H \text{ i } b \in G.$$

Działanie powyższe nazywamy *działaniem przez sprzężenia*.

Stwierdzenie 1.6.1. (1) *Jeśli $\delta : G \times X \to X$ jest działaniem grupy G zbiorze X, to funkcja $f_\delta : G \to S(X)$ dana wzorem*

$$(f_\delta(a))(x) = \delta(a, x) \text{ dla } a \in G \text{ i } x \in X$$

jest homomorfizmem.

(2) *Jeśli X jest zbiorem oraz $f : G \to S(X)$ jest homomorfizmem grup, to funkcja $\delta_f : G \times X \to X$ dana wzorem*

$$\delta_f(a, x) = (f(a))(x) \text{ dla } a \in G \text{ i } x \in X$$

jest działaniem grupy G na zbiorze G.

(3) *Jeśli δ jest działaniem grupy G zbiorze X, to $\delta_{f_\delta} = \delta$.*

(4) *Jeśli X jest zbiorem oraz $f : G \to S(X)$ jest homomorfizmem grup, to $f_{\delta_f} = f$.*

Dowód. Ćwiczenie. □

Wniosek 1.6.2 (Cayley). *Jeśli G jest grupą, to istnieje monomorfizm grup $G \to S(G)$.*

Dowód. Niech $\delta : G \times G \to G$ będzie działaniem grupy G na G przez przesunięcia. Wtedy $f_\delta : G \to S(G)$ jest homomorfizmem grup. Musimy sprawdzić, że $\operatorname{Ker} f_\delta = \{1\}$. Zauważmy, że $f_\delta(a) = 1_G$ wtedy i tylko wtedy, gdy $ab = b$ dla dowolnego $b \in G$. W szczególności $a = a \cdot 1 = 1$, co kończy dowód. □

Stwierdzenie 1.6.3. *Jeśli δ jest działaniem grupy G na G przez sprzężenia, to $\operatorname{Im} f_\delta \subseteq \operatorname{Aut}(G)$.*

Dowód. Należy sprawdzić, że dla każdego $a \in G$ funkcja $g_a = f_\delta(a)$ jest homomorfizmem grupy G, co wynika natychmiast z bezpośrednich rachunków. □

Automorfizmy grupy G postaci $f_\delta(a)$ dla $a \in G$, gdzie δ jest działaniem grupy G na G przez sprzężenia, nazywamy *automorfizmami wewnętrznymi*. Zbiór wszystkich automorfizmów wewnętrznych grupy G tworzy grupę (gdyż jest równy $\operatorname{Im} f_\delta$), którą nazywamy *grupą automorfizmów wewnętrznych grupy G* i oznaczamy $\operatorname{Inn}(G)$.

Centrum grupy G nazywamy zbiór wszystkich elementów $a \in G$ takich, że $ab = ba$ dla dowolnego $b \in G$. Centrum grupy G oznaczamy $C(G)$.

Przykłady. (1) $C(G) = G$ wtedy i tylko wtedy, gdy G jest grupą abelową.

(2) Jeśli K jest ciałem oraz $C(\mathrm{GL}_n(K))$ składa się z wszystkich macierzy diagonalnych.

Stwierdzenie 1.6.4. *Jeśli δ jest działaniem grupy G na G przez sprzężenia, to $\operatorname{Ker} f_\delta = C(G)$. W szczególności, $C(G)$ jest dzielnikiem normalnym grupy G oraz $\operatorname{Inn}(G) \simeq G/C(G)$.*

Dowód. Bezpośredni rachunek. □

Zauważmy, że $C(G)$ jest zawsze grupą abelową.

Wniosek 1.6.5. *Jeśli H jest podgrupą grupy G oraz $a \in G$, to aHa^{-1} jest podgrupą grupy G izomorficzną z H.*

Dowód. Ze Stwierdzenia 1.6.3 wynika, że funkcja $g : G \to G$ dana wzorem $g(b) = aba^{-1}$, $b \in G$, jest automorfizmem grupy G. Stąd funkcja $gi : H \to G$, gdzie $i : H \to G$ jest naturalnym włożeniem, jest monomorfizmem. Ponieważ $\mathrm{Im}(gi) = aHa^{-1}$, więc teza wynika ze Stwierdzenia 1.4.3 oraz Pierwszego Twierdzenia o Izomorfizmie. □

Jeśli H i K są podgrupami grupy G oraz istnieje element $a \in G$ taki, że $K = aHa^{-1}$, to grupy H i K nazywamy *sprzężonymi* (zauważmy, że w tej sytuacji $H = a^{-1}Ka = a^{-1}K(a^{-1})^{-1}$). Możemy powiedzieć, że podgrupa G jest dzielnikiem normalnym wtedy i tylko wtedy, gdy $H = K$ dla dowolnej podgrupy K sprzężonej z H.

Jeśli grupa G działa na zbiorze X to dla dowolnego $x \in X$ przez G_x będziemy oznaczać zbiór $a \in G$ takich, że $ax = x$. Ponadto przez Gx oznaczać będziemy zbiór wszystkich elementów postaci $\{ax \mid a \in G\}$. Zbiór Gx będziemy nazywać *orbitą elementu x*.

Stwierdzenie 1.6.6. *Załóżmy, że grupa G działa na zbiorze X.*

(1) *Relacja $\sim$ na zbiorze X dana wzorem*

$$x \sim y \text{ wtedy i tylko wtedy, gdy } y = ax \text{ dla } a \in G$$

jest relacją równoważności.

(2) *Klasą abstrakcji elementu $x \in X$ w powyższej relacji jest Gx.*

(3) *Dla każdego $x \in X$ zbiór G_x jest podgrupą grupy G.*

(4) *Jeśli $x \in X$ oraz $g \in G$, to $G_{ax} = aG_xa^{-1}$.*

Dowód. Bezpośrednie rachunki. □

Dla $x \in x$ grupę G_x nazywamy *grupą izotropii* lub *stabilizatorem elementu x*.

Twierdzenie 1.6.7. *Jeśli grupa G działa na zbiorze X oraz $x \in X$, to funkcja $G/G_x \in aG_x \mapsto ax \in Gx$ jest bijekcją.*

Dowód. Bezpośredni rachunek. □

1.7 Twierdzenia Sylowa

Niech G będzie grupą, która działa na zbiorze X. Przez X^G będziemy oznaczać zbiór wszystkich $x \in X$ dla których $Gx = \{x\}$.

Lemat 1.7.1. *Jeśli p jest liczbą pierwszą oraz G jest grupą rzędu p^n, $n \geq 1$, która działa na zbiorze X, to $|X^G| \equiv |X| \pmod{p}$.*

Dowód. Ze Stwierdzenia 1.6.6 wynika, że istnieją elementy $x_1, \ldots, x_k \in X$ takie, że $X = |X^G| \cup Gx_1 \cup \cdots \cup Gx_k$, $Gx_i \cap Gx_j = \emptyset$, $i \neq j$, oraz $|Gx_i| > 1$, $i = 1, \ldots, n$. Z Twierdzenia 1.6.7 wiemy, że $|Gx_i| = |G_{x_i}|$, natomiast z Twierdzenia Lagrange'a wynika, że $|G_{x_i}|$ dzieli $|G| = p^n$. Ponieważ $|G_{x_i}| > 1$ oraz p jest liczbą pierwszą, więc wnioskujemy stąd, że p dzieli $|G_{x_i}|$, $i = 1, \ldots, n$, co kończy dowód. □

Twierdzenie 1.7.2 (Cauchy). *Jeśli p jest liczbą pierwszą oraz G jest grupą skończoną, której rząd jest podzielny przez p, to w grupie G istnieje element, którego rząd jest równy p.*

Dowód. Niech X będzie zbiorem wszystkich ciągów $(a_1, \ldots, a_p)$, $a_i \in G$, $i = 1, \ldots, p$, oraz $a_1 \cdots a_p = 1$. Zauważmy, że $|X| = |G|^{p-1}$, zatem p dzieli $|X|$. Rozważmy działanie grupy $\mathbb{Z}_p$ na zbiorze X dane wzorem

$$k(a_1, \ldots, a_p) \mapsto (a_{k+1}, \ldots, a_p, a_1, \ldots, a_k)$$

(należy sprawdzić poprawność definicji). Zauważmy, że $X^{\mathbb{Z}_p} = \{(a, \ldots, a) \mid a^p = 1\}$. Z poprzedniego lematu wynika, że p dzieli $|X^{\mathbb{Z}_p}|$. Ponieważ mamy $(1, \ldots, 1) \in X^{\mathbb{Z}_p}$, więc $|X^{\mathbb{Z}_p}| \geq p > 1$. W szczególności istnieje $a \neq 1$ takie, że $a^p = 1$. Ponieważ p jest liczbą pierwszą, więc z Wniosku 1.5.10 wynika, że $|a| = p$. □

Niech p będzie liczbą pierwszą. Grupę G nazwiemy *p-grupą*, jeśli rząd każdego elementu grupy G jest potęgą liczby p. Jeśli podgrupa H grupy G jest p-grupą, to H nazywamy *p-podgrupą*.

Wniosek 1.7.3. *Jeśli p jest liczbą pierwszą oraz G jest grupą skończoną, to G jest p-grupą wtedy i tylko wtedy, gdy $|G|$ jest potęgą liczby p.*

Dowód. Oczywiście, jeśli $|G|$ jest potęgą liczby p, to z Twierdzenia Lagrange'a wynika, że rząd każdego elementu grupy G jest potęgą liczby p. Przypuśćmy teraz, że G jest p-grupą oraz niech liczba pierwsza q dzieli $|G|$. Wtedy z poprzedniego twierdzenia wynika, że istnieje element grupy G, którego rząd jest równy q. Stąd natychmiast otrzymujemy, że $q = p$, co kończy dowód. □

Niech H będzie podgrupą grupy G. Przez $N_G(H)$ oznaczać będziemy zbiór wszystkich $a \in G$ dla których $aHa^{-1} = H$. Zbiór $N_G(H)$ nazywamy *normalizatorem podgrupy H w grupie G*. Normalizator podgrupy H w grupie G jest podgrupą grupy G oraz H jest dzielnikiem normalnym grupy $N_G(H)$.

Lemat 1.7.4. *Jeśli p jest liczbą pierwszą oraz H jest p-podgrupą grupy skończonej G, to $[N_G(H) : H] \equiv [G : H] \pmod{p}$.*

Dowód. Grupa H działa na zbiorze G/H przez (lewe) przesunięcia zgodnie ze wzorem

$$a(bH) \mapsto abH \text{ dla } a \in H \text{ i } b \in G.$$

(Trzeba sprawdzić, że gdy $b \sim_H c$, to $ab \sim_H ac$ dla $a \in H$ oraz $b, c \in G$.) Zauważmy, że $bH \in (G/H)^H$ wtedy i tylko wtedy, gdy $b \in N_G(H)$. Stąd $|(G/H)^H| = [N_G(H) : H]$, co kończy dowód wobec Lematu 1.7.1. □

Wniosek 1.7.5. *Jeśli p jest liczbą pierwszą oraz H jest p-podgrupą grupy skończonej G taką, że p dzieli $[G : H]$, to $N_G(H) \neq H$. W szczególności istnieje p-podgrupa K grupy G taka, że H jest dzielnikiem normalnym grupy K oraz $[K : H] = p$.*

Dowód. Ponieważ $[N_G(H) : H] \equiv [G : H] \pmod{p}$, więc p dzieli $[N_G(H) : H]$. Stąd wynika teza pierwszej części, gdyż $[N_G(H) : H] \geq 1$.

Dla dowodu drugiej części wniosku zauważmy, że z Twierdzenia Cauchy'ego istnieje podgrupa L rzędu p w grupie $N_G(H)/H$. Niech $K = f^{-1}(L)$, gdzie $f : N_G(H) \to H$ jest naturalnym rzutowaniem. Wtedy K jest podgrupą grupy $N_G(H)$ na mocy Lematu 1.4.2, a więc także grupy G. Ponadto $[K : H] = |L| = p$, zatem K jest p-grupą. Ponadto H jest dzielnikiem normalnym grupy K, gdyż $K \subseteq N_G(H)$. □

Twierdzenie 1.7.6 (Pierwsze Twierdzenie Sylowa). *Niech p będzie liczbą pierwszą oraz G będzie grupą rzędu $p^n m$, gdzie $n \geq 0$ oraz $(p, m) = 1$. Wtedy dla każdego $i = 0, \ldots, n$ istnieje podgrupa grupy G rzędu p^i oraz dla każdego $i = 0, \ldots, n-1$ każda podgrupa grupy G rzędu p^i jest dzielnikiem normalnym pewnej podgrupy grupy G rzędu p^{i+1}.*

Dowód. Jest to natychmiastowa konsekwencja poprzedniego wniosku wykorzystująca indukcję ze względu na i. □

Jeśli p jest liczbą pierwszą, to podgrupę P grupy G nazywamy *p-podgrupą Sylowa*, jeśli P jest maksymalną (w sensie zawierania) p-podgrupą. Łatwo zauważyć, że każda p-podgrupa H grupy skończonej G jest zawarta w pewnej p-podgrupie Sylowa. Dowód tego samego faktu dla grup nieskończonych wymaga wykorzystania lematu Kuratowskiego–Zorna. W szczególności w każdej grupie G istnieje p-podgrupa Sylowa. Mamy też następujące konsekwencje Pierwszego Twierdzenia Sylowa.

Wniosek 1.7.7. *Niech p będzie liczbą pierwszą oraz G będzie grupą rzędu $p^n m$, gdzie $n \geq 0$ oraz $(p, m) = 1$.*

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

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

Dowód. Oczywiste. □

Z drugiego punktu powyższego wniosku wynika między innymi, że jeśli p jest liczbą pierwszą i w skończonej grupie G istnieje dokładnie jedna p-podgrupa Sylowa P, to P jest dzielnikiem normalnym grupy G.

Twierdzenie 1.7.8 (Drugie Twierdzenie Sylowa). *Niech p będzie liczbą pierwszą. Dowolne dwie p-podgrupy Sylowa grupy skończonej G są ze sobą sprzężone.*

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

$$a(bP) \mapsto abP \text{ dla } a \in Q \text{ i } b \in G.$$

Wiemy, że $|(G/P)^Q| \equiv [G : Q] \pmod{p}$ na mocy Lematu 1.7.1. Ponieważ P jest p-podgrupą Sylowa, więc p nie dzieli $[G : Q]$, stąd $(G/P)^Q \neq \emptyset$. Zauważmy, że $aP \in (G/P)^Q$ wtedy i tylko wtedy, gdy $Q \subseteq aPa^{-1}$. Ponieważ $|Q| = |P| = |aPa^{-1}|$, więc $Q = aPa^{-1}$. □

Twierdzenie 1.7.9 (Trzecie Twierdzenie Sylowa). *Niech p będzie liczbą pierwszą oraz N będzie ilością p-podgrup Sylowa grupy skończonej G. Wtedy N dzieli $|G|$ oraz $N \equiv 1 \pmod{p}$.*

Dowód. Niech P będzie p-podgrupą Sylowa grupy G. Z Drugiego Twierdzenia Sylowa wynika, że N jest równe ilości podgrup sprzężonych z P. Zauważmy, że $aPa^{-1} = bPb^{-1}$ wtedy i tylko wtedy, gdy $aN_G(P) = bN_G(P)$, zatem $N = [G : N_G(P)]$ skąd wynika, że N dzieli $|G|$.

Niech X będzie zbiorem wszystkich p-podgrup Sylowa grupy G. Grupa P działa na X przez sprzężenia, tzn.

$$(a, Q) \mapsto aQa^{-1}.$$

Zauważmy, że jeśli $Q \in X^P$, to $P \subseteq N_G(Q)$. Zatem P jest p-podgrupa Sylowa grupy $N_G(Q)$, więc istnieje $a \in N_G(Q)$ taki, że $aQa^{-1} = P$. Ale $aQa^{-1} = Q$, zatem $Q = P$, więc $X^P = \{P\}$, co kończy dowód twierdzenia wobec Lematu 1.7.1. □

1.8 Grupy rozwiązalne

Niech G będzie grupą oraz $a, b \in G$. Element $aba^{-1}b^{-1}$ nazywamy *komutatorem elmentów a i b* i oznaczamy $[a, b]$. Podgrupę generowaną przez wszystkie komutatory elementów grupy G nazywamy *komutantem grupy G* i oznaczamy $[G, G]$. Zauważmy, że $[G, G] = \{1\}$ wtedy i tylko wtedy, gdy grupa G jest abelowa.

Lemat 1.8.1. *Jeśli $f : G \to H$ jest epimorfizmem grup, to mamy $[H, H] = f([G, G])$.*

Dowód. Niech X będzie zbiorem wszystkich komutatorów elementów grupy G, zaś Y zbiorem wszystkich komutatorów elementów grupy H. Pokażemy, że $f(X) = Y$. Jeśli $a, b \in G$, to $f([a, b]) = [f(a), f(b)]$, a więc $f(X) \subseteq Y$. Z drugiej strony, gdy $c, d \in H$, to istnieją $a, b \in G$ takie, że $f(a) = c$ i $f(d) = b$. Wtedy $[c, d] = f([a, b])$, a więc $Y \subseteq f(X)$. Korzystając z Lematu 1.5.3 otrzymujemy zatem, że $[H, H] = \langle Y \rangle = \langle f(X) \rangle = f(\langle X \rangle) = f([G, G])$. □

Twierdzenie 1.8.2. *Jeśli G jest grupą, to komutant grupy G jest dzielnikiem normalnym oraz $G/[G, G]$ jest grupą abelową. Ponadto, jeśli N jest dzielnikiem normalnym grupy G takim, że grupa G/N jest abelowa, to mamy $[G, G] \subseteq N$.*

Dowód. Niech $a \in G$ oraz $f : G \to G$ będzie automorfizmem danym wzorem $f(b) = a^{-1}ba$, $b \in G$. Z poprzedniego lematu otrzymujemy, że $[G, G] = f([G, G]) = a^{-1}[G, G]a$. Stąd $a[G, G]a^{-1} = aa^{-1}[G, G]aa^{-1} = [G, G]$, co wobec dowolności a kończy dowód faktu, że $[G, G]$ jest dzielnikiem normalnym. Jeśli $a, b \in G$, to otrzymujemy ciąg równości $(a[G, G])(b[G, G]) = ab[G, G] = (ab[G, G])([b^{-1}, a^{-1}][G, G]) = ab[b^{-1}, a^{-1}][G, G] = ba[G, G] = (b[G, G])(a[G, G])$, a więc $G/[G, G]$ jest grupą abelową.

Przypuśćmy teraz, że N jest takim dzielnikiem normalnym grupy G, że G/N jest grupą abelową. Jeśli $a, b \in G$, to $(b^{-1}N)(a^{-1}N) = (a^{-1}N)(b^{-1}N)$. Stąd $b^{-1}a^{-1} \sim_N a^{-1}b^{-1}$, a więc $aba^{-1}b^{-1} \in N$, tzn. $[a, b] \in N$. Zatem wszystkie komutatory elementów $X \subseteq N$, skąd $G \subseteq N$. □

Ćwiczenie 1.8.1. Udowodnić, że jeśli H jest podgrupą grupy G taką, że $[G, G] \subseteq H$, to H jest dzielnikiem normalnym grupy G.

Niech G będzie grupą. Definiujemy ciąg podgrup $G^{(m)}$, $m \in \mathbb{N}$, grupy G następująco:

$$G^{(m)} = \begin{cases} G & m = 0, \\ [G^{(m-1)}, G^{(m-1)}] & m > 0. \end{cases}$$

Z powyższego twierdzenia wynika, że dla każdego $m \geq 1$ grupa $G^{(m)}$ jest dzielnikiem normalnym grupy $G^{(m-1)}$ oraz $G^{(m-1)}/G^{(m)}$ jest grupą abelową. Grupę G nazywamy *rozwiązalną*, jeśli $G^{(n)} = \{1\}$ dla pewnego $n \geq 0$.

Twierdzenie 1.8.3. (1) *Jeśli grupa G jest rozwiązalna oraz H jest podgrupą grupy G, to H jest grupą rozwiązalną.*

(2) *Jeśli grupa G jest rozwiązalna oraz $f : G \to H$ jest epimorfizmem grup, to grupa H jest rozwiązalna.*

(3) *Jeśli N jest dzielnikiem normalnym grupy G oraz grupy N i G/N są rozwiązalne, to grupa G jest rozwiązalna.*

Dowód. (1) Łatwo pokazać indukcyjnie, że $H^{(m)} \subseteq G^{(m)}$ dla dowolnego $m \geq 0$, skąd natychmiast wynika teza.

(2) Z Lematu 1.8.1 wynika, że $H^{(m)} = f(G^{(m)})$ dla dowolnego $m \geq 0$, skąd natychmiast otrzymujemy tezę.

(3) Niech $f : G \to G/N$ będzie naturalnym rzutowaniem. Ponieważ grupa G/N jest rozwiązalna, więc istnieje $n \geq 0$ takie, że $(G/N)^{(n)} = \{1\}$. Ponadto $(G/N)^{(n)} = f(G^{(n)})$ na mocy Lematu 1.8.1, więc $G^{(n)} \subseteq \operatorname{Ker} f = N$. Z rozwiązalności grupy N i punktu (1) wynika, że grupa $G^{(n)}$ jest rozwiazalna, zatem istnieje $k \geq 0$ takie, że $(G^{(n)})^{(k)} = \{1\}$. Ale $(G^{(n)})^{(k)} = G^{(n+k)}$, co kończy dowód. □

Twierdzenie 1.8.4. *Grupa G jest rozwiązalna wtedy i tylko wtedy, gdy istnieje ciąg podgrup G_m, $m = 0, \ldots, n$, grupy G taki, że $G_0 = G$, $G_n = \{1\}$, G_m jest dzielnikiem normalnym grupy G_{m-1} oraz G_{m-1}/G_m jest grupą abelową, $m = 1, \ldots, n$.*

Dowód. Trzeba pokazać, że jeśli w grupie G istnieje ciąg podgrup o powyższych własnościach, to grupa G jest rozwiązalna. W tym celu udowodnimy, że $G^{(m)} \subseteq G_m$ dla $m = 0, \ldots, n$. Wtedy bowiem $G^{(n)} \subseteq \{1\}$, a więc $G^{(n)} = \{1\}$. Dla $m = 0$ teza jest oczywista. Gdy $m > 0$ oraz wiemy, że $G^{(m-1)} \subseteq G_{m-1}$, to ponieważ grupa G_{m-1}/G_m jest abelowa, więc z Twierdzenia 1.8.2 wynika, że $G_m \supseteq [G_{m-1}, G_{m-1}]$. Ponadto $[G_{m-1}, G_{m-1}] \supseteq [G^{(m-1)}, G^{(m-1)}]$, gdyż $G_{m-1} \supseteq G^{(m-1)}$. To kończy dowód, gdyż $[G^{(m-1)}, G^{(m-1)}] = G^{(m)}$. □

1.9 Grupy symetryczne

Przez cały paragraf n będzie ustaloną liczbą całkowitą nie mniejszą niż 2 oraz $I_n = \{1, \ldots, n\}$.

Funkcje odwracalne $\sigma : I_n \to I_n$ nazywać będziemy *permutacjami*. Jeśli i_1, $\ldots$, i_r są parami różnymi elementami zbioru I_n, to przez $(i_1, \ldots, i_r)$ będziemy oznaczać permutację $\sigma : I_n \to I_n$ zdefiniowaną wzorem

$$\sigma(i) = \begin{cases} i_{k+1} & i = i_k,\ k = 1, \ldots, r-1, \\ i_1 & i = i_r, \\ i & \text{w przeciwnym wypadku.} \end{cases}$$

Permutacje powyższej postaci będziemy nazywać *cyklami*, a liczbę r będziemy *długością cyklu* σ. Cykle długości 2 będziemy nazywać *transpozycjami*.

Stwierdzenie 1.9.1. *Każda permutację zbioru I_n można zapisać jako iloczyn cykli.*

Dowód. Dla permutacji σ przez N_σ oznaczać będziemy ilość indeksów i takich, że $\sigma(i) \neq i$. Dowód stwierdzenia będzie indukcyjny ze względu na N_σ. Gdy $N_\sigma = 0$, to $\sigma = 1_{I_n}$ i teza jest oczywista. Załóżmy zatem, że σ jest permutacją zbioru I_n taką, że $N_\sigma > 0$, oraz każdą permutację σ' zbioru I_n taką, że $N_{\sigma'} < N_\sigma$ można zapisać jako iloczyn cykli.

Ustalmy indeks $i \in I_n$ taki, że $\sigma(i) \neq i$. Niech M będzie najmniejszą liczbą całkowitą dodatnią m taką, że $\sigma^m(i) = i$. Taka liczba istnieje, gdyż zbiór I_n jest skończony. Istotnie, ze skończoności zbioru I_n wynika, że istnieją liczby całkowite k i l takie, że $l > k$ oraz $\sigma^l(i) = \sigma^k(i)$. Wtedy $\sigma^{l-k}(i) = i$ oraz $l - k > 0$. Ponadto $\sigma^k(i) \neq \sigma^l(i)$ dla $0 \leq k < l \leq M - 1$. Niech $\tau = (\sigma^{M-1}(i), \sigma^{M-2}(i), \ldots, \sigma(i), i)$ i $\sigma' = \tau\sigma$. Wtedy

$$\sigma'(j) = \begin{cases} j & j = \sigma^k(i),\ k = 0, \ldots, M-1, \\ \sigma(j) & j \neq \sigma^k(i),\ k = 0, \ldots, M-1, \end{cases}$$

zatem $N_{\sigma'} < N_\sigma$. Korzystając z założenia indukcyjnego oraz równości $\sigma = \tau^{-1}\sigma'$ oraz $\tau^{-1} = (i, \sigma(i), \ldots, \sigma^{M-1}(i))$ otrzymujemy tezę twierdzenia. □

Lemat 1.9.2. *Cykl długości r jest iloczynem $r - 1$ transpozycji.*

Dowód. Mamy wzór $(i_1, \ldots, i_r) = (i_1, i_{r-1}) \cdots (i_1, i_2)$, co kończy dowód. □

Wniosek 1.9.3. *Każda permutacja jest iloczynem pewnej ilości transpozycji.*

Permutację nazywamy *parzystą*, jeśli może być przedstawiona w postaci iloczynu parzystej ilości transpozycji, permutację nazywamy *nieparzystą*, jeśli może być przedstawiona w postaci iloczynu nieparzystej ilości transpozycji.

Twierdzenie 1.9.4. *Permutacja nie może być jednocześnie parzysta i nieparzysta.*

Dowód. Rozważmy funkcję $\Delta : S_n \to \mathbb{Z}$ daną wzorem

$$\Delta(\sigma) = \prod_{1 \leq i < j \leq n} (\sigma(i) - \sigma(j)).$$

Łatwo można pokazać, że jeśli τ jest transpozycją, to $\Delta(\sigma\tau) = -\Delta(\sigma)$. Stąd wynika, że gdyby σ było permutacją, która jest jednocześnie parzysta i nieparzysta, to $\Delta(\sigma) = \Delta(1_{I_n}) = -\Delta(\sigma)$, a więc $\Delta(\sigma) = 0$, co jest niemożliwe. □

Z powyższego twierdzenia wynika, że z każdą permutacją $\sigma \in S_n$ możemy związać jej *znak* $\operatorname{sgn}\sigma$ zgodnie z regułą

$$\operatorname{sgn}\sigma = \begin{cases} 1 & \sigma \text{ jest permutacją parzystą,} \\ -1 & \sigma \text{ jest permutacją nieparzystą.} \end{cases}$$

Przez A_n oznaczać będziemy zbiór permutacji parzystych. Zauważmy, że A_n jest grupą, którą nazywamy *grupą alternującą*.

Stwierdzenie 1.9.5. *Funkcja* $\operatorname{sgn} : S_n \to \mathbb{C}_2$ *jest epimorfizmem grup.*

Dowód. Ćwiczenie. □

Wniosek 1.9.6. $[S_n : A_n] = 2$ *oraz* A_n *jest dzielnikiem normalnym grupy* S_n*.*

Dowód. Natychmiastowa konsekwencja poprzedniego stwierdzenia oraz faktu, że $\operatorname{Ker}\operatorname{sgn} = A_n$. □

Grupę G nazywamy *prostą*, jeśli nie ma nietrywialnych dzielników normalnych. Podamy teraz bez dowodu następujące twierdzenie.

Twierdzenie 1.9.7. *Grupa* A_n *jest prosta dla* $n \geq 5$*.*

Wniosek 1.9.8. *Grupa* S_n *nie jest rozwiązalna dla* $n \geq 5$*.*

Dowód. Gdyby grupa S_n była rozwiązalna, to na mocy Twierdzenia 1.8.3 także grupa A_n byłaby rozwiązalna. Ta jednak nie jest abelowa oraz nie ma nietrywialnych dzielników normalnych, więc $[A_n, A_n] = A_n$, zatem $A_n^{(m)} = A_n$ dla $m \geq 0$, co prowadzi do sprzeczności. □

2 Pierścienie

2.1 Podstawowe definicje

Definicja. *Pierścieniem* (*przemiennym z jedynką*) nazywamy zbiór R wraz z dwoma działaniami $+, \cdot : R \times R \to R$ takimi, że R wraz z działaniem $+$ jest grupą abelową oraz

(1) działanie $\cdot$ jest łączne;

(2) *działanie* $\cdot$ *jest rozłączne względem działania* $+$, tzn. $a(b+c) = ab+ac$ i $(b+c)a = ba+ca$ dla dowolnych $a, b, c \in R$;

(3) dla działania $\cdot$ istnieje element neutralny (pierścień z jedynką);

(4) działanie $\cdot$ jest przemienne (pierścień przemienny).

Zbiór R wraz z działaniem $+$ nazywamy *grupą addytywną pierścienia* R. Element neutralny dla $+$ będziemy oznaczać przez 0, element neutralny dla $\cdot$, który jest wyznaczony jednoznacznie, będziemy oznaczać przez 1.

Przykłady. (1) Każde ciało K jest pierścieniem, który będziemy oznaczać przez K.

(2) Zbiór liczb całkowitych z działaniami dodawania i mnożenia jest pierścieniem, który będziemy oznaczać $\mathbb{Z}$.

(3) Jeśli $m > 0$, to zbiór reszt z dzielenia przez m z działaniami dodawania i mnożenia modulo m jest pierścieniem, który będziemy oznaczać $\mathbb{Z}_m$.

(4) Jeśli R jest pierścieniem oraz X jest zbiorem, to zbiór wszystkich funkcji $f : X \to R$ z działaniami dodawania i mnożenia funkcji jest pierścieniem.

Definicja. Podpierścieniem pierścienia R nazywamy taki podzbiór $S \subseteq R$, że S jest podgrupą grupy addytywnej pierścienia R oraz

(1) jeśli $a, b \in S$, to $ab \in S$;

(2) $1 \in S$.

Przykłady. (1) Jeśli K jest podciałem ciała L, to K jest podpierścieniem pierścienia L.

(2) Pierścień $\mathbb{Z}$ jest podpierścieniem pierścienia $\mathbb{Q}$.

Definicja. Relację $\sim$ w R nazywamy *kongruencją*, jeśli $\sim$ jest kongruencją w grupie addytywnej pierścienia R oraz jeśli $a \sim b$ oraz $c \sim d$, to $ac \sim bd$.

Stwierdzenie 2.1.1. *Jeśli $\sim$ jest kongruencją w pierścieniu R, to definicje*

$$[a]_\sim + [b]_\sim = [a+b]_\sim,$$
$$[a]_\sim \cdot [b]_\sim = [a+b]_\sim,$$

są poprawne i definiują w $R/\sim$ strukturę pierścienia.

Dowód. Natychmiastowa konsekwencja definicji. □

Pierścień $R/\sim$ nazywamy *pierścieniem ilorazowym*.

Definicja. Podzbiór $I \subseteq R$ nazywamy *ideałem*, jeśli I jest podgrupą grupy addytywnej pierścienia R oraz jeśli $a \in I$ i $r \in R$, to $ra \in R$. Jeśli I jest ideałem pierścienia R, to piszemy $I \trianglelefteq R$. Zapis $I \triangleleft R$ oznacza, że $I \trianglelefteq R$ oraz $I \neq R$.

Jeśli $\sim$ jest kongruencją w pierścieniu R, to przez $I_\sim$ będziemy oznaczać $[0]_\sim$. Podobnie, gdy I jest ideałem w pierścieniu R, to przez $\sim_I$ oznaczać będziemy relację w R zadaną przez warunek

$$a \sim_I b \text{ wtedy i tylko wtedy, gdy } a - b \in I.$$

Stwierdzenie 2.1.2. *Niech R będzie pierścieniem.*

(1) *Jeśli $\sim$ jest kongruencją w pierścieniu R, to $I_\sim$ jest ideałem oraz $\sim_{I_\sim} = \sim$.*

(2) *Jeśli I jest ideałem w pierścieniu R, to $\sim_I$ jest kongruencją oraz $I_{\sim_I} = I$. Ponadto $[a]_{\sim_I} = a + I$.*

Dowód. Ćwiczenie. □

Niech $R/I = R/\sim_I$. Jeśli $a \sim_I b$, to piszemy też $a \equiv b \pmod{I}$.

Wniosek 2.1.3. *Jeśli I jest ideałem w pierścieniu R, to definicje*

$$(a+I) + (b+I) = (a+b) + I,$$
$$(a+I) \cdot (b+I) = ab + I,$$

są poprawne i definiują w R/I strukturę pierścienia.

Pierścień R/I nazywamy *pierścieniem ilorazowym*. Jeśli I jest ideałem pierścienia R, to dla ideału $J \subseteq R$ takiego, że $I \subseteq J$, przez J/I oznaczać będziemy zbiór $\{a + I \mid a \in J\} \subseteq R/I$.

Definicja. Niech R i S będą pierścieniami. Funkcję $f : R \to S$ nazywamy *homomorfizmem pierścieni*, jeśli f jest homomorfizmem grup addytywnych pierścieni R i S, $f(1) = 1$ oraz $f(ab) = f(a)f(b)$ dla dowolnych $a, b \in R$. Podobnie jak dla grup wprowadzamy pojęcie *monomorfizmu*, *epimorfizmu*, *izomorfizmu*, *endomorfizmu*, *automorfizmu*, *jądra* i *obrazu homomorfizmu* oraz *izomorficzności pierścieni*. Podobnie jak dla grup też możemy mówić o *naturalnym włożeniu* podpierścienia w pierścień, *naturalnym rzutowaniu* pierścienia na pierścień ilorazowy.

Lemat 2.1.4. *Niech $f : R \to S$ będzie homomorfizmem pierścieni.*

(1) *Jeśli T jest podpierścieniem pierścienia R, to $f(T)$ jest podpierścieniem pierścienia S.*

(2) *Jeśli T jest podpierścieniem pierścienia S, to $f^{-1}(T)$ jest podpierścieniem pierścienia R.*

(3) *Jeśli I jest ideałem pierścienia R oraz f jest epimorfizmem, to $f(I)$ jest ideałem pierścienia S.*

(4) *Jeśli I jest ideałem pierścienia S, to $f^{-1}(I)$ jest ideałem pierścienia R.*

Dowód. Ćwiczenie. □

Stwierdzenie 2.1.5. *Niech $f : R \to S$ będzie homomorfizmem pierścieni.*

(1) $\operatorname{Ker} f$ *jest ideałem pierścienia R.*

(2) $\operatorname{Im} f$ *jest podpierścieniem pierścienia S.*

(3) *f jest monomorfizmem wtedy i tylko wtedy, gdy* $\operatorname{Ker} f = \{1\}$.

(4) *f jest epimorfizmem wtedy i tylko wtedy, gdy* $\operatorname{Im} f = S$.

(5) *f jest izomorfizmem wtedy i tylko wtedy, gdy* $\operatorname{Ker} f = \{1\}$ *oraz* $\operatorname{Im} f = S$.

(6) *Jeśli f jest izomorfizmem, to funkcja odwrotna do f też jest homomorfizmem.*

Dowód. Ćwiczenie. □

Wniosek 2.1.6. *Jeśli $f : R \to S$ jest monomorfizmem pierścieni, to funkcja $g : R \to \operatorname{Im} f$ dana wzorem $g(a) = f(a)$ jest izomorfizmem.*

Dowód. Ćwiczenie. □

Twierdzenie 2.1.7. *Niech $f : R \to S$ będzie homomorfizmem pierścieni oraz I ideałem pierścienia R takim, że $I \subseteq \operatorname{Ker} f$. Wtedy odwzorowanie $g : R/I \to S$ dane wzorem $g(a + I) = f(a)$ jest poprawnie określone oraz jest homomorfizmem,* $\operatorname{Ker} g = \operatorname{Ker} f/I$ *i* $\operatorname{Im} g = \operatorname{Im} f$.

Dowód. Ćwiczenie. □

Wniosek 2.1.8 (Pierwsze Twierdzenie o Izomorfizmie). *Jeśli $f : R \to S$ jest homomorfizmem pierścieni, to funkcja $R/\operatorname{Ker} f \in a+\operatorname{Ker} f \mapsto f(a) \in \operatorname{Im} f$ jest izomorfizmem pierścieni.*

Dowód. Ćwiczenie. □

Lemat 2.1.9. *Niech R będzie pierścieniem, niech S będzie podpierścieniem pierścienia R oraz niech I będzie ideałem pierścienia R.*

(1) *$S \cap I$ jest ideałem pierścienia S.*

(2) *$S + I$ jest podpierścieniem pierścienia R.*

Dowód. Ćwiczenie. □

Wniosek 2.1.10 (Drugie Twierdzenie o Izomorfizmie). *Jeśli R jest pierścieniem, S jest podpierścieniem pierścienia R oraz I jest ideałem pierścienia R, to funkcja $S/(S \cap I) \ni a + (S \cap I) \mapsto a + I \in (S + I)/I$ jest izomorfizmem pierścieni.*

Dowód. Ćwiczenie. □

Wniosek 2.1.11 (Trzecie Twierdzenie o Izomofizmie). *Jeśli I i J są ideałami pierścienia R takimi, że $I \subseteq J$, to J/I jest ideałem pierścienia R/I oraz funkcja $(R/I)/(J/I) \ni (a+I)+(J/I) \mapsto a+J \in R/J$ jest izomorfizmem.*

Dowód. Ćwiczenie. □

2.2 Ideały

Element $a \neq 0$ pierścienia R nazywamy *dzielnikiem zera*, jeśli istnieje element $b \in R$ taki, że $b \neq 0$ oraz $ab = 0$. Pierścień R, w którym nie ma dzielników zera, nazywamy *dziedziną*. Element $a \in R$ nazywamy *odwracalnym*, jeśli istnieje element $b \in R$ taki, że $ab = 1$. Zauważmy, że jeśli element jest odwracalny, to nie jest dzielnikiem zera. Pierścień, w którym $0 \neq 1$ oraz każdy element różny od 0 jest odwracalny, nazywamy *ciałem*.

Stwierdzenie 2.2.1. *Jeśli element a pierścienia R nie jest dzielnikiem zera, to z równości $ab = ac$ wynika, że $b = c$.*

Dowód. Zauważmy, że przy naszych założeniach mamy $a(b-c)=0$, zatem $b-c=0$, skąd $b=c$. □

Ideał I pierścienia R nazywamy *pierwszym*, jeśli dla dowolnych elementów $a,b\in R$ z faktu, że $ab\in I$ wynika, że $a\in I$ lub $b\in I$. Ideał I pierścienia R nazywamy *maksymalnym*, jeśli $I\neq R$ oraz dla dowolnego ideału J pierścienia R z faktu, że $I\subseteq J$ wynika, że $J=I$ lub $J=R$.

Stwierdzenie 2.2.2. *Niech I będzie ideałem pierścienia R takim, że $I\neq R$.*

(1) *Ideał I jest pierwszy wtedy i tylko wtedy, gdy pierścień R/I jest dziedziną.*

(2) *Ideał I jest maksymalny wtedy i tylko wtedy, gdy pierścień R/I jest ciałem.*

(3) *Każdy ideał maksymalny jest pierwszy.*

Dowód. (1) Ćwiczenie.

(2) Załóżmy najpierw, że I jest ideałem maksymalnym. Chcemy pokazać, że R/I jest ciałem. Ponieważ $I\neq R$, więc $1\notin I$, zatem $1+I\neq 0+I$. Niech $a\in R$ i $a\notin I$. Szukamy $b\in I$ takiego, że $ab+I=1+I$. Niech $J=\{ab+c\mid b\in R,\, c\in I\}$. Wtedy $J\trianglelefteq R$. Ponadto $I\subseteq J$ oraz $I\neq J$. Stąd $J=R$. W szczególności istnieją $b\in R$ oraz $c\in I$ takie, że $1=ab+c$. Wtedy $ab+I=1+I$.

Załóżmy teraz, że R/I jest ciałem. Ponieważ wtedy $0+I\neq 1\neq I$, więc $1\notin I$, skąd $I\neq R$. Niech $J\trianglelefteq R$, $I\subseteq J$ oraz $I\neq J$. Wybierzmy $a\in J\setminus I$. Z założenia istnieje $b\in R$ takie, że $ab+I=1+I$. Stąd $1=ab+c$ dla pewnego $c\in I$, a więc $1\in J$, skąd $J=R$.

(3) Ćwiczenie. □

Stwierdzenie 2.2.3. *Jeśli I_α, $\alpha\in A$, $A\neq\emptyset$, są ideałami pierścienia R, to $\bigcap_{\alpha\in A} I_\alpha$ jest ideałem pierścienia R.*

Dowód. Ćwiczenie. □

Wniosek 2.2.4. *Jeśli X jest podzbiorem pierścienia R, to istnieje najmniejszy ideał pierścienia R zawierający zbiór X.*

Dowód. Ćwiczenie. □

Jeśli X jest podzbiorem pierścienia R, to najmniejszy ideał pierścienia R zawierający zbiór X będziemy oznaczać (X). Jeśli $I=(X)$, to mówimy, że *ideał I jest generowany przez zbiór X*. Gdy $X=\{x_1,\ldots,x_n\}$, to zamiast (X) piszemy $(x_1,\ldots,x_n)$. Ideał I pierścienia R nazywamy *głównym*, gdy istnieje

element $a \in R$ taki, że $I = (a)$. Pierścień R, w którym każdy ideał jest główny, nazywamy *pierścieniem ideałów głównych*. Gdy dodatkowo R jest dziedziną, to mówimy o *dziedzinie ideałów głównych*.

Jeśli R jest pierścieniem oraz $X, Y \subseteq R$, to oznaczamy $XY = \{xy \mid x \in X, y \in Y\}$. Gdy $a \in R$ oraz $X \subseteq R$, to $aX = \{a\}X$ oraz $Xa = X\{a\}$.

Twierdzenie 2.2.5. *Niech R będzie pierścieniem oraz $x_1, \ldots, x_n \in R$. Wtedy $(x_1, \ldots, x_n) = Rx_1 + \cdots + Rx_n$.*

Dowód. Niech $I = (X)$ oraz $J = Rx_1 + \cdots + Rx_n$. Z definicji ideału natychmiast wynika, że $J \subseteq I$. Oczywiście $X \subseteq J$. Dla dowodu wystarczy pokazać zatem, że J jest ideałem, co jest prostym ćwiczeniem. □

Twierdzenie 2.2.6 (Chińskie Twierdzenie o Resztach). *Niech $I_1, \ldots, I_n$ będą ideałami pierścienia R takimi, że $I_i + I_j = R$ dla $i \neq j$. Jeśli $a_1, \ldots, a_n \in R$, to istnieje $a \in R$ taki, że $a \equiv a_i \pmod{I_i}$, $i = 1, \ldots, n$. Ponadto, gdy $a, b \in R$ oraz $a \equiv b \pmod{I_i}$, $i = 1, \ldots, n$, to $a \equiv b \pmod{I_1 \cap \cdots \cap I_n}$.*

Dowód. Zauważmy, że dla każdego $i = 1, \ldots, n$ mamy $(I_i + I_1) \cdots (I_i + I_{i-1})(I_i + I_{i+1}) \cdots (I_i + I_n) \subseteq I_i + I_1 \cdots I_{i-1} I_{i+1} \cdots I_n \subseteq I_i + I_1 \cap \cdots \cap I_{i-1} \cap I_{i+1} \cap \cdots \cap I_n$. Stąd $R = I_i + I_1 \cap \cdots \cap I_{i-1} \cap I_{i+1} \cap \cdots \cap I_n$. Zatem dla każdego $i = 1, \ldots, n$ istnieją elementy $b_i \in I_i$ oraz $c_i \in I_1 \cap \cdots \cap I_{i-1} \cap I_{i+1} \cap \cdots \cap I_n$ takie, że $1 = b_i + c_i$. Niech $a = a_1c_1 + \cdots + a_nc_n$. Wtedy a ma żądane własności. Druga część twierdzenia jest oczywista. □

Wniosek 2.2.7. *Niech $m_1, \ldots, m_n$ będą dodatnimi liczbami całkowitymi takimi, że $(m_i, m_j) = 1$, $i \neq j$. Jeśli $a_1, \ldots, a_n$ są liczbami całkowitymi, to istnieje liczba całkowita a taka, że $a \equiv a_i \pmod{m_i}$, $i = 1, \ldots, m$. Ponadto, jeśli a i b są liczbami całkowitymi takimi, że $a \equiv b \pmod{m_i}$, $i = 1, \ldots, n$, to $a \equiv b \pmod{m_1 \cdots m_n}$.*

Dowód. Ćwiczenie. □

Niech $R_1, \ldots, R_n$ będą pierścieniami. Przez $R_1 \times \cdots \times R_n$ będziemy oznaczać pierścień zdefiniowany w zbiorze $\{(a_1, \ldots, a_n) \mid a_i \in R_i\}$ wzorami

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$
$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1b_1, \ldots, a_nb_n).$$

Pierścień $R_1 \times \cdots \times R_n$ nazywamy *produktem pierścieni $R_1, \ldots, R_n$*.

Wniosek 2.2.8. *Niech $I_1, \ldots, I_n$ będą ideałami pierścienia R takimi, że $I_i + I_j = R$ dla $i \neq j$. Odwzorowanie*

$$R/(I_1 \cap \cdots \cap I_n) \ni a + I_1 \cap \cdots \cap I_n \mapsto (a + I_1, \ldots, a + I_n) \in R/I_1 \times \cdots \times R/I_n$$

jest poprawnie określone i jest izomorfizmem pierścieni.

Dowód. Ćwiczenie. □

2.3 Faktoryzacja

Niech R będzie dziedziną całkowitości i $a, b \in R$. Mówimy, że *element a dzieli element b*, jeśli istnieje element $c \in R$ taki, że $b = ac$. Piszemy wtedy $a|b$. Elementy a i b nazywamy stowarzyszonymi, jeśli $a|b$ i $b|a$. Jeśli elementy a i b są stowarzyszone, to piszemy $a \approx b$.

Twierdzenie 2.3.1. *Niech R będzie dziedziną całkowitości i $a, b \in R$.*

(1) *$a|b$ wtedy i tylko wtedy, gdy $(b) \subseteq (a)$ (równoważnie $b \in (a)$).*

(2) *$a \approx b$ wtedy i tylko wtedy, gdy $(a) = (b)$.*

(3) *a jest elementem odwracalnym wtedy i tylko wtedy, gdy $a|b$ dla wszystkich $b \in R$.*

(4) *a jest elementem odwracalnym wtedy i tylko wtedy, gdy $(a) = R$.*

(5) *$\approx$ jest relacją równoważności.*

(6) *$a \approx b$ wtedy i tylko wtedy, gdy istnieje element odwracalny $c \in R$ taki, że $a = cb$.*

Dowód. Ćwiczenie. □

Niech R będzie dziedziną całkowitości. Element $a \in R$ nazywamy *nierozkładalnym* jeśli $a \neq 0$, a nie jest elementem odwracalnym oraz jeśli $b|a$, to b jest elementem odwracalnym lub $b \approx a$. Element $a \in R$ nazywamy *pierwszym* jeśli $a \neq 0$, a nie jest elementem odwracalnym oraz jeśli $a|bc$, to $a|b$ lub $a|c$.

Twierdzenie 2.3.2. *Niech R będzie dziedziną całkowitości i $a \in R$, $a \neq 0$.*

(1) *a jest pierwszy wtedy i tylko wtedy, gdy (a) jest ideałem pierwszym.*

(2) *a jest nierozkładalny wtedy i tylko wtedy, gdy (a) jest maksymalny w zbiorze wszystkich właściwych ideałów głównych pierścienia R.*

(3) *Każdy element pierwszy jest nierozkładalny.*

(4) *Jeśli a jest dziedziną ideałów głównych, to każdy element nierozkładalny jest pierwszy.*

(5) *Element stowarzyszony z elementem nierozkładalnym jest nierozkładalny.*

(6) *Element stowarzyszony z elementem pierwszym jest pierwszy.*

Dowód. (1) Ćwiczenie.

(2) Przypuśćmy, że element a jest nierozkładalny. Wtedy $(a) \neq R$ na mocy Twierdzenia 2.3.1, gdyż element a nie jest odwracalny. Ponadto, jeśli $(a) \subseteq (b)$, to $b|a$, więc b jest odwracalny i $(b) = R$, lub $b \approx a$ i $(b) = (a)$.

Załóżmy teraz, że ideał (a) jest maksymalny w zbiorze wszystkich właściwych ideałów głównych. Jeśli $b|a$, to $(a) \subseteq (b)$, a więc $(b) = (a)$ i $b \approx a$ lub $(b) = R$ i element b jest odwracalny.

(3) Przypuśćmy, że element a jest pierwszy oraz $b|a$. Wtedy $a = bc$ dla pewnego $c \in R$. W szczególności $a|bc$, skąd $a|b$ lub $a|c$. W pierwszym przypadku $a \approx b$. W drugim $c = ad$ dla pewnego $d \in R$. Stąd $a = bda$. Ponieważ R jest dziedziną całkowitości i $a \neq 0$, więc $bd = 1$ na mocy Stwierdzenie 2.2.1, skąd element b jest odwracalny.

(4) Przypuśćmy, że element a jest nierozkładalny. Na mocy punktu (2) ideał (a) jest maksymalny w zbiorze wszystkich właściwych ideałów głównych. Ponieważ R jest dziedziną ideałów głównych, więc (a) jest ideałem maksymalnym, a więc pierwszym na mocy Stwierdzenia 2.2.2, co kończy dowód wobec punktu (1).

(5), (6) Jest to natychmiastowa konsekwencja punktów (1) i (2) wykorzystująca własność, że jeśli $a \approx b$, to $(a) = (b)$. □

Dziedzinę całkowitości R nazywamy *dziedziną z jednoznacznością rozkładu*, jeśli:

(1) dla każdego niezerowego i nieodwracalnego elementu $a \in R$ istnieją nierozkładalne elementy $c_1, \ldots, c_n$ takie, że $a = c_1 \cdots c_n$,

(2) jeśli $c_1, \ldots, c_n, d_1, \ldots, d_m$ są elementami nierozkładalnymi oraz $c_1 \cdots c_n = d_1 \cdots d_m$, to $n = m$ oraz istnieje permutacja σ zbioru $\{1, \ldots, n\}$ taka, że $c_i \approx d_{\sigma(i)}$ dla każdego $i = 1, \ldots, n$.

Lemat 2.3.3. *Niech R będzie dziedziną ideałów głównych. Jeśli $a_1, a_2, \ldots$ są elementami pierścienia R takimi, że $(a_i) \subseteq (a_{i+1})$ dla każdego i, to istnieje liczba całkowita $n \geq 1$ taka, że $(a_i) = (a_n)$ dla $i \geq n$.*

Dowód. Niech $I = \bigcup_{i=1}^{\infty}(a_i)$. Łatwo pokazać, że I jest ideałem. Ponieważ R jest dziedziną ideałów głównych, więc istnieje element $a \in R$ taki, że $I = (a)$. Istnieje liczba całkowita $n \geq 1$ taka, że $a \in (a_n)$. Dla $i \geq n$ mamy wtedy ciąg inkluzji $I = (a) \subseteq (a_n) \subseteq (a_i) \subseteq I$, co kończy dowód. □

Twierdzenie 2.3.4. *Każda dziedzina ideałów głównych jest dziedziną z jednoznacznością rozkładu.*

Dowód. Niech R będzie dziedziną ideałów głównych. Pokażemy najpierw, że każdy niezerowy i nieodwracalny element $a \in R$ ma przedstawienie w postaci iloczynu elementów nierozkładalnych. Niech S będzie zbiorem tych niezerowych i nieodwracalnych elementów pierścienia R, dla których takie przedstawienie nie istnieje. Zauważmy najpierw, że jeśli dla niezerowych i nieodwracalnych elementów b i c mamy $b, c \notin S$, to $bc \notin S$. Ponadto, jeśli $a \in S$, to istnieje element $d_a \in S$ taki, że $(a) \subseteq (d_a)$ oraz $(a) \neq (d_a)$. Istotnie, element a jest rozkładalny, zatem istnieją elementy $b, c \in R$ takie, że $a = bc$ oraz $a \not\approx b$ i $a \not\approx c$. Oczywiście $b \neq 0$ i $c \neq 0$. Ponadto elementy b i c są nieodwracalne. Z powyższej uwagi wynika też, że $b \notin S$ lub $c \notin S$, więc możemy wziąć $d_a = b$ w pierwszym przypadku i $d_a = c$ w drugim przypadku. Z powyższej obserwacji wynika zatem, że jeśli $S \neq \emptyset$, to istnieje ciąg a_1, a_2, ... elementów zbioru S taki, że $(a_i) \subseteq (a_{i+1})$ oraz $(a_i) \neq (a_{i+1})$ dla $i \geq 1$. To przeczy poprzedniemu lematowi, a więc mamy równość $S = \emptyset$, co kończy dowód pierwszej części twierdzenia.

Drugą część twierdzenia udowodnimy przez indukcję ze względu na n. Przypuśćmy najpierw, że $c = d_1 \cdots d_m$, $m \geq 1$, gdzie c, d_1, ..., d_m są nierozkładalne. Ponieważ R jest dziedziną ideałów głównych, więc na mocy Twierdzenia 2.3.2 element c jest pierwszy. Stąd istnieje $i \in \{1, \ldots, m\}$ takie, że $c|d_i$, a więc $c \approx d_i$, gdyż element d_i jest nierozkładalny. Wtedy $c = ud_i$ dla pewnego elementu odwracalnego u, skąd $d_1 \cdots d_{i-1} d_{i+1} \cdots d_m = u$, co jest możliwe tylko dla $m - 1 = 0$, gdyż elementy d_1, ..., d_m są nieodwracalne.

Załóżmy teraz, że $n > 1$ oraz przypuśćmy, że elementy c_1, ..., c_n, d_1, ..., d_m są nierozkładalne i $c_1 \cdots c_n = d_1 \cdots d_m$. Podobnie jak poprzednio istnieje $i \in \{1, \ldots, m\}$ takie, że $c_n = ud_i$ dla pewnego elementu odwracalnego u. Bez straty ogólności możemy założyć, że $i = m$. Wtedy elementy uc_1, c_2, ..., c_{n-1}, d_1, ..., d_{m-1} są nierozkładalne oraz $(uc_1)c_2 \cdots c_{n-1} = d_1 \cdots d_{m-1}$. Z założenia indukcyjnego wynika, że $n - 1 = m - 1$ oraz istnieje permutacja τ zbioru $\{1, \ldots, n-1\}$ taka, że $u \approx d_{\tau(1)}$ oraz $c_i \approx d_{\tau(i)}$, $i = 2, \ldots, n-1$. Wtedy permutacja σ zbioru $\{1, \ldots, n\}$ dana wzorem $\sigma(i) = \tau(i)$ dla $i \in \{1, \ldots, n-1\}$ oraz $\sigma(n) = m$ jest szukaną permutacją. □

Dziedzinę całkowitości R nazywamy *dziedziną Euklidesa* jeśli istnieje funkcja $\varphi : R \to \mathbb{N}$ taka, że:

(1) $\varphi(a) = -\infty$ wtedy i tylko wtedy, gdy $a = 0$;

(2) jeśli $a, b \in R$, to $\varphi(ab) = \varphi(a)\varphi(b)$;

(3) jeśli $a, b \in R$ oraz $b \neq 0$, to istnieją elementy $q, r \in R$ takie, że $a = qb+r$ oraz $\varphi(r) < \varphi(b)$.

Twierdzenie 2.3.5. *Jeśli R jest dziedziną Euklidesa, to R jest dziedziną ideałów głównych.*

Dowód. Niech I będzie ideałem w R. Możemy założyć, że $I \neq \{0\}$. Niech $a \in I$ będzie takim elementem, że $\varphi(a) = \min\{\varphi(b) \mid b \in I, b \neq 0\}$. Jeśli $b \in I$, to istnieją elementy $q, r \in R$ takie, że $b = qa + r$ oraz $\varphi(r) < \varphi(a)$. Z wyboru elementy a wynika, że $r = 0$, a więc $b \in Ra = (a)$. Stąd $I = (a)$, co kończy dowód. □

Natychmiastową konsekwencją powyższego twierdzenia oraz Twierdzenia 2.3.4 jest następujący fakt.

Wniosek 2.3.6. *Jeśli R jest dziedziną Euklidesa, to R jest dziedziną z jednoznacznością rozkładu.*

Niech R będzie dziedziną całkowitości. Element d nazywamy *największym wspólnym dzielnikiem* elementów $a_1, \ldots, a_k \in R$, jeśli $d|a_i$, $i = 1, \ldots, k$ oraz, gdy $c|a_i$, $i = 1, \ldots, k$, to $c|d$. W powyższej sytuacji piszemy $d = (a_1, \ldots, a_k)$. Jeśli $1 = (a_1, \ldots, a_k)$, to mówimy, że elementy $a_1, \ldots, a_k$ są *względnie pierwsze*. Jeśli największy wspólny dzielnik dwóch elementów istnieje, to jest wyznaczony jednoznacznie z dokładnością do stowarzyszenia.

Twierdzenie 2.3.7. *Jeśli R jest dziedziną z jednoznacznością rozkładu, to dla dowolnych elementów $a_1, \ldots, a_k \in R$ istnieje ich największy wspólny dzielnik.*

Dowód. Bez straty ogólności możemy założyć, że $a_i \neq 0$, $i = 1, \ldots, k$. Dowód opiera się na obserwacji, że jeśli $a_i = u_i c_1^{l_{i,1}} \cdots c_n^{l_{i,n}}$, gdzie elementy $u_1, \ldots, u_k$ są odwracalne, $c_1, \ldots, c_n$ są nierozkładalne oraz $l_{i,1}, \ldots, l_{i,n} \geq 0$, $i = 1, \ldots, k$, to $c_1^{\min(l_{1,1},\ldots,l_{k,1})} \cdots c_n^{\min(l_{1,n},\ldots,l_{k,n})} = (a_1, \ldots, a_k)$. □

2.4 Pierścienie wielomianów

Niech R będzie pierścieniem oraz $n \geq 1$ liczbą całkowitą. *Pierścieniem wielomianów od n-zmiennych o współczynnikach w R* nazywamy zbiór wszystkich

funkcji $f : \mathbb{N}^n \to R$ takich, że $f(u) \neq 0$ dla skończenie wielu u z działaniami zdefiniowanymi wzorami

$$(f+g)(u) = f(u) + g(u),$$
$$(f \cdot g)(u) = \sum_{v+w=u} f(v)g(w).$$

Elementem neutralnym dla dodawania jest funkcja $0 : \mathbb{N}^n \to R$ dana wzorem $0(u) = u$ dla każdego 0, zaś elementem neutralnym dla mnożenia funkcja $1 : \mathbb{N}^n \to R$ dana wzorem

$$1(u) = \begin{cases} 1 & u = (0, \ldots, 0), \\ 0 & u \neq (0, \ldots, 0). \end{cases}$$

Dla $i = 1, \ldots, n$ niech $x_i : \mathbb{N}^n \to R$ będzie funkcją daną wzorem

$$x_i(u) = \begin{cases} 1 & u = (0, \ldots, 0, \underbrace{1}_{i\text{-te miejsce}}, 0, \ldots, 0), \\ 0 & u \neq (0, \ldots, 0, \underbrace{1}_{i\text{-te miejsce}}, 0, \ldots, 0). \end{cases}$$

W powyższej sytuacji pierścień wielomianów od n-zmiennych o współczynnikach w R oznaczamy przez $R[x_1, \ldots, x_n]$ i mówimy o pierścieniu wielomianów od zmiennych x_1, …, x_n. W szczególności pierścień wielomianów od zmiennej x, to zbiór wszystkich ciągów $(a_0, a_1, \ldots)$ takich, że $a_i = 0$ dla $i \gg 0$, z działaniami danymi wzorami

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots),$$
$$(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = (a_0 \cdot b_0, a_1 b_0 + a_0 b_1, \ldots, \sum_{k+l=m} a_k b_l, \ldots).$$

Mamy $0 = (0, 0, \ldots)$, $1 = (1, 0, 0, \ldots)$ oraz $x = (0, 1, 0, 0, \ldots)$.

Jeśli $f \in R[x_1, \ldots, x_n]$, to

$$f = \sum_{u=(u_1,\ldots,u_n)\in\mathbb{N}^n} f(u) x_1^{u_1} \cdots x_n^{u_n}.$$

Elementy $f(u)$ nazywamy *współczynnikami wielomianu* f, zaś współczynnik $f((0, \ldots, 0))$ *wyrazem wolnym*. Wielomiany postaci $a x_1^{v_1} \cdots x_n^{v_n}$, gdzie $a \in R$ i $v \in \mathbb{N}^n$ (tzn. funkcje $f : \mathbb{N}^n \to R$ takie, że $f(u) = \begin{cases} a & u = v \\ 0 & u \neq v \end{cases}$) nazywamy *jednomianami*, zaś jednomiany $a x_1^0 \cdots x_n^0 = a$ *wielomianami stałymi*. *Stopniem wielomianu* f nazywamy $\max\{|u| \mid u \in \mathbb{N}^n, f(u) \neq 0\}$, gdzie

$|(u_1, \ldots, u_n)| = u_1 + \cdots + u_n$ oraz $\max \emptyset = -\infty$. Stopień wielomianu f oznaczamy $\deg f$. Dla $f \in R[x]$ otrzymujemy

$$f = \sum_{k=0}^{\infty} a_k x^k = \sum_{k=0}^{m} a_k x^k,$$

gdzie $m \geq \deg f$. Jeśli $a_m \neq 0$, to $m = \deg f$ oraz a_m nazywamy *współczynnikiem wiodącym*. Gdy $a_m = 1$, to mówimy, że wielomian f jest *unormowany*.

Stwierdzenie 2.4.1. *Niech R będzie dziedziną oraz $f, g \in R[x_1, \ldots, x_n]$. Wtedy $\deg(f+g) \leq \max(\deg f, \deg g)$ oraz $\deg(fg) = \deg f + \deg g$.*

Mamy monomorfizm pierścieni $\phi : R \to R[x_1, \ldots, x_n]$ dany wzorem

$$(\varphi(r))(u) = \begin{cases} r & u = (0, \ldots, 0), \\ 0 & u \neq (0, \ldots, 0), \end{cases}$$

dla $r \in R$ i $u \in \mathbb{N}^n$, dzięki któremu możemy traktować R jako podpierścień pierścienia $R[x_1, \ldots, x_n]$. Pierścień wielomianów jest scharakteryzowany przez następującą własność. Niech $\varphi : R \to S$ będzie homomorfizmem pierścieni oraz $s_1, \ldots, s_n \in S$. Istnieje dokładnie jeden homomorfizm $\psi : R[x_1, \ldots, x_n] \to S$ taki, że $\psi(r) = \varphi(r)$ dla $r \in R$ oraz $\varphi(x_i) = s_i$, $i = 1, \ldots, n$. Homomorfizm φ dany jest wzorem

$$\varphi(f) = \sum_{u=(u_1,\ldots,u_n)\in\mathbb{N}^n} \varphi(f(u)) s_1^{u_1} \cdots s_n^{u_n}.$$

Gdy R jest podpierścieniem pierścienia S oraz φ jest naturalnym włożeniem, to element $\varphi(f)$ oznaczamy też $f(s_1, \ldots, s_n)$ i mówimy o *podstawieniu elementów $s_1, \ldots, s_n$ do wielomianu f*.

Gdy $i_1 < \cdots < i_k$, to pierścień $R[x_{i_1}, \ldots, x_{i_k}]$ utożsamiamy z odpowiednim podpierścieniem pierścienia $R[x_1, \ldots, x_n]$. Dla dowolnego pierścienia R oraz rozkładu ($I = \{i_1, \ldots, i_k\}, J = \{j_1, \ldots, j_l\}$ zbioru $\{1, \ldots, n\}$ (tzn. $I \cup J = \{1, \ldots, n\}$ i $I \cap J = \emptyset$) mamy też naturalny izomorfizm

$$R[x_1, \ldots, x_k][x_{k+1}, \ldots, x_n] \simeq R[x_1, \ldots, x_n].$$

Stwierdzenie 2.4.2. *Jeśli R jest dziedziną całkowitości, to $R[x_1, \ldots, x_n]$ też jest dziedziną całkowitości.*

Dowód. Ćwiczenie. □

Twierdzenie 2.4.3 (Algorytm Dzielenia). *Niech R będzie dziedziną całkowitości oraz $f, g \in R[x]$ takie, że $g \neq 0$ oraz współczynnik wiodący wielomianu g jest elementem odwracalnym w R. Wtedy istnieją jedyne wielomiany q i r takie, że $f = qg + r$ oraz $\deg r < \deg g$.*

Dowód. Dowód istnienia będzie indukcyjny ze względu na $\deg f$. Gdy $\deg f < \deg g$, to teza zachodzi dla $q = 0$ i $r = f$.

Załóżmy teraz, że $\deg f \geq \deg g$ oraz niech a oraz b będą wiodącymi współczynnikami wielomianów f i g odpowiednio. Ponieważ b jest elementem odwracalnym, więc istnieje $c \in R$ taki, że $a = bc$. Niech $h = f - cx^k g$, gdzie $k = \deg g - \deg f$. Wtedy $\deg h < \deg f$, więc z założenia indukcyjnego istnieją wielomiany p i r takie, że $h = pg + r$ oraz $\deg r < \deg g$. Dla $q = cx^k + p$ mamy $f = qg + r$.

Dla dowodu jednoznaczności załóżmy, że $q_1 g + r_1 = q_2 g + r_2$ oraz $\deg r_1, \deg r_2 < \deg g$. Wtedy $(q_1 - q_2)g = r_2 - r_1$. Zauważmy, że jeśli $q_1 \neq q_2$, to $\deg((q_1 - q_2)g) = \deg(q_1 - q_2) + \deg g \geq \deg g$, zaś $\deg(r_2 - r_1) \leq \max(\deg r_2, \deg r_1)) < \deg g$. Stąd $q_1 = q_2$, a więc także $r_1 = r_2$. □

Wniosek 2.4.4. *Jeśli F jest ciałem, to pierścień wielomianów $F[x]$ jest dziedziną Euklidesa.*

Dowód. Ponieważ F jest ciałem, a więc dziedziną, więc $F[x]$ jest dziedziną na mocy Stwierdzenia 2.4.2. Można sprawdzić wykorzystując powyższe twierdzenie, że funkcja $\varphi : F[x] \to \mathbb{N}$ dana wzorem $\varphi(f) = 2^{\deg f}$ ma żądane własności. □

Wniosek 2.4.5. *Jeśli F jest ciałem, to pierścień wielomianów $F[x]$ jest dziedziną z jednoznacznością rozkładu.*

Mamy też następujący bardziej ogólny fakt, który podamy bez dowodu.

Twierdzenie 2.4.6. *Jeśli R jest dziedziną z jednoznacznością rozkładu, to pierścień wielomianów $R[x_1, \ldots, x_n]$ jest dziedziną z jednoznacznością rozkładu.*

Niech R będzie dziedziną. Niech X będzie zbiorem par (a, b), $a, b \in R$ takich, że $b \neq 0$. W zbiorze X definiujemy relację równoważności $\sim$ wzorem $(a, b) \sim (c, d)$ wtedy i tylko wtedy, gdy $ad = bc$. Łatwo sprawdzić, że relacja $\sim$ jest relacją równoważności. Niech $F = X/\sim$. W zbiorze F wprowadzamy działania $+$ i $\cdot$ wzorami

$$[(a, b)]_\sim + [(c, d)]_\sim = [(ad + bc, bd)]_\sim,$$
$$[(a, b)]_\sim \cdot [(c, d)]_\sim = [(ac, bd)]_\sim.$$

Łatwo pokazać, że zbiór F wraz z powyższymi działaniami jest ciałem, które nazywamy *ciałem ułamków dziedziny R*.

Niech R będzie dziedziną z jednoznacznością rozkładu oraz $f \in R[x]$. Wielomian f nazywamy *prymitywnym*, jeśli współczynniki wielomianu f są względnie pierwsze.

Mamy następujące kryterium na nierozkładalność wielomianów, które podamy bez dowodu.

Twierdzenie 2.4.7 (Kryterium Eisensteina). *Niech R będzie dziedziną z jednoznacznością rozkładu z ciałem ułamków F oraz $f = \sum_{i=0}^{n} a_i x^i \in R[x]$, $n \geq 1$. Jeśli istnieje element nierozkładalny $p \in R$ taki, że*

$$p|a_i,\ i = 0, \ldots, n-1,\ p \not| a_n,\ p^2 \not| a_0,$$

to wielomian f jest nierozkładalny w $F[x]$. Ponadto, gdy wielomian f jest prymitywny, to w powyższej sytuacji wielomian f jest nierozkładalny w $R[x]$.