Grzegorz Bobiński

Algebra I

Wydział Matematyki i Informatyki
Uniwersytet Mikołaja Kopernika w Toruniu
2022

Algebra I

Spis treści

Algebra I

1. Struktury algebraiczne i ich homomorfizmy

1.1. Działania w zbiorach i ich własności

Definicja.

Działaniem w zbiorze X nazywamy każdą funkcję postaci $X \times X \to X$.

Oznaczenie.

Działania będziemy zwykle oznaczać symbolami takimi jak $*$, $+$ lub $\cdot$. Jeśli $*$ jest działaniem w zbiorze X, to wynik działania $*$ na elementach $x, y \in X$ oznaczamy przez $x*y$ (zamiast $*(x,y)$). Jeśli działanie oznaczamy symbolem $+$, to nazywamy je dodawaniem. Gdy działanie oznaczamy symbolem $\cdot$, to nazywamy je mnożeniem i piszemy często xy zamiast $x \cdot y$.

Przykład.

Poniższa tabela zawiera niektóre wcześniej poznane przykłady działań. Dla podzbioru X zbioru $\mathbb{R}$ przez X_+ oznaczamy zbiór liczb dodatnich należących do X. Podobnie, przez X_- oznaczamy zbiór liczby ujemnych należących do X. Dalej, dla dodatniej liczby całkowitej n przez $\mathbb{Z}_n$ oznaczamy zbiór reszt z dzielenia przez n, a przez $+_n$ i $\cdot_n$ działania dodawania i mnożenia modulo n w tym zbiorze.

Działanie	Zbiór
$+$	$\mathbb{N}$, $\mathbb{N}_+$, $\mathbb{Z}$, $\mathbb{Z}_+$, $\mathbb{Z}_-$, $\mathbb{Q}$, $\mathbb{Q}_+$, $\mathbb{Q}_-$, $\mathbb{R}$, $\mathbb{R}_+$, $\mathbb{R}_-$, $\ldots$
$-$	$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\ldots$
$\cdot$	$\mathbb{N}$, $\mathbb{N}_+$, $\mathbb{Z}$, $\mathbb{Z}_+$, $\mathbb{Q}$, $\mathbb{Q}_+$, $\mathbb{R}$, $\mathbb{R}_+$, $\ldots$
$:$	$\mathbb{Q}_+$, $\mathbb{R}_+$, $\ldots$
$+_n$, $\cdot_n$	$\mathbb{Z}_n$, $n \in \mathbb{N}_+$
$+$, $-$	$\mathbb{M}_{m,n}(\mathbb{R})$, $m, n \in \mathbb{N}_+$
$\cdot$	$\mathbb{M}_n(\mathbb{R})$, $n \in \mathbb{N}_+$
$\cdot$	zbiór $n \times n$ macierzy odwracalnych, $n \in \mathbb{N}_+$
$\circ$	zbiór funkcji (odwracalnych) $X \to X$ dla pewnego zbioru X

Definicja.

Działanie $*$ w zbiorze X nazywamy łącznym, jeśli

$$(x * y) * z = x * (y * z)$$

dla dowolnych elementów x, y i z zbioru X.

Zbiór X wraz łącznym działaniem $*$ nazywamy półgrupą.

Ćwiczenie.

Sprawdzić, które z poznanych działań są łączne.

Uwaga.

Jeśli $*$ jest działaniem łącznym w zbiorze X oraz $x_1, \ldots, x_n$ są elementami

zbioru X, to wynik działania

$$x_1 * \cdots * x_n$$

nie zależy od kolejności wykonywania działań.

Dowód.
Indukcja (ćwiczenie). □

Definicja.
Działanie $*$ w zbiorze X nazywamy przemiennym, jeśli

$$x * y = y * x$$

dla dowolnych elementów x i y zbioru X.

Półgrupę, w której działanie jest przemienne, nazywamy półgrupą przemienną.

Ćwiczenie.
Sprawdzić, które z poznanych działań są przemienne.

Uwaga.
Jeśli zbiór X z działaniem $*$ jest półgrupą przemienną oraz $x_1, \ldots, x_n$ są elementami zbioru X, to

$$x_1 * \cdots * x_n = x_{\sigma(1)} * \cdots * x_{\sigma(n)}$$

dla dowolnej permutacji σ zbioru $\{1, \ldots, n\}$.

Dowód.
Ćwiczenie – należy wykorzystać fakt, że każdą permutację można przedstawić jako iloczyn transpozycji postaci $(i, i+1)$. □

Definicja.
Niech $*$ będzie działaniem w zbiorze X. Mówimy, że element e zbioru X jest elementem neutralnym dla działania $*$, jeśli

$$x * e = x = e * x$$

dla dowolnego elementu x zbioru X.

Półgrupę (przemienną), która posiada element neutralny, nazywamy monoidem (przemiennym).

Ćwiczenie.
Sprawdzić, które z poznanych działań posiadają element neutralny.

Uwaga.

Jeśli $*$ jest działaniem w zbiorze X oraz e_1 i e_2 są elementami neutralnymi dla działania $*$, to $e_1 = e_2$.

Dowód.

Ponieważ e_1 jest elementem neutralnym, więc $e_1 * e_2 = e_2$. Podobnie, ponieważ e_2 jest elementem neutralnym, więc $e_1 * e_2 = e_1$, co kończy dowód. □

Oznaczenie.

Jeśli działanie oznaczamy symbolem $+$ i posiada ono element neutralny, to oznaczamy go symbolem 0 i nazywamy zerem. Podobnie, jeśli działanie oznaczamy symbolem $\cdot$ i posiada ono element neutralny, to oznaczamy go symbolem 1 i nazywamy jedynką.

Definicja.

Niech $*$ będzie działaniem w zbiorze X posiadającym element neutralny e. Jeśli x jest elementem zbioru X, to mówimy, że element y zbioru X jest elementem odwrotnym (względem działania $*$) do elementu x, jeśli

$$x * y = e = y * x.$$

Element, który posiada element odwrotny, nazywamy elementem odwracalnym (względem działania $*$).

Monoid, w którym każdy element jest odwracalny, nazywamy grupą.

Grupę, w której działanie jest przemienne, nazywamy grupą abelową.

Ćwiczenie.

Sprawdzić, dla których poznanych działań wszystkie elementy są odwracalne.

Terminologia.

Działanie w (abstrakcyjnej) grupie (monoidzie, półgrupie) będziemy zwykle domyślnie oznaczać symbolem $\cdot$. Dlatego zwykle będziemy identyfikować grupę (monoid, półgrupę) ze zbiorem, na którym jest zdefiniowana struktura grupy (monoidu, półgrupy).

Uwaga.

Niech X będzie monoidem oraz x elementem zbioru X. Jeśli y_1 i y_2 są elementami odwrotnymi do elementu x, to $y_1 = y_2$.

Dowód.

Ponieważ y_1 jest elementem odwrotnym do elementu x oraz 1 jest elementem neutralnym, więc

$$y_1 x y_2 = (y_1 x) y_2 = 1 \cdot y_2 = y_2.$$

Analogicznie, $y_1 x y_2 = y_1$, co kończy dowód. □

Oznaczenie.

Niech x będzie elementem zbioru X. Jeśli działanie w zbiorze X oznaczamy symbolem $+$, to element odwrotny do elementu x oznaczamy $-x$ i nazywamy go ELEMENTEM PRZECIWNYM. Podobnie, jeśli działanie oznaczamy symbolem $\cdot$, to element odwrotny oznaczamy x^{-1}.

Przykłady.

(1) Zbiór liczb całkowitych (wymiernych, rzeczywistych, zespolonych) z działaniem dodawania jest grupą, którą oznaczamy $\mathbb{Z}$ ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, odpowiednio).

(2) Zbiór niezerowych liczb wymiernych (rzeczywistych, zespolonych) z działaniem mnożenia jest grupą, którą oznaczamy $\mathbb{Q}^\times$ ($\mathbb{R}^\times$, $\mathbb{C}^\times$, odpowiednio).

(3) Jeśli n jest dodatnią liczbą całkowitą, to zbiór reszt z dzielenia przez n z działaniem dodawania modulo n jest grupą, którą oznaczamy $\mathbb{Z}_n$.

(4) Jeśli n jest dodatnią liczbą całkowitą, to zbiór reszt z dzielenia przez n, które są względnie pierwsze z n, z działaniem dodawania modulo n jest grupą, którą oznaczamy $\mathbb{Z}_n^\times$.

(5) Jeśli n jest dodatnią liczbą całkowitą, to zbiór pierwiastków zespolonych n-tego stopnia z 1 z działanie mnożenia liczb zespolonych jest grupą, którą oznaczamy $\mathbb{T}_n$.

(6) Jeśli X jest zbiorem, to zbiór funkcji odwracalnych $X \to X$ ze składaniem funkcji jest grupą, którą oznaczamy symbolem S_X. Gdy $X = \{1, \ldots, n\}$ dla dodatniej liczby całkowitej n, to piszemy S_n zamiast S_X. Grupy S_n nazywamy GRUPAMI SYMETRYCZNYMI.

(7) Jeśli n jest dodatnią liczbą, to zbiór $n \times n$ macierzy odwracalnych o współczynnikach wymiernych (rzeczywistych, zespolonych) z działaniem mnożenia macierzy jest grupą, którą oznaczamy $\mathrm{GL}_n(\mathbb{Q})$ ($\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{C})$, odpowiednio).

Lemat 1.1.

Niech G będzie grupą.

(1) $1^{-1} = 1$.

(2) Jeśli $g \in G$, to $(g^{-1})^{-1} = g$.

(3) Jeśli $g, h \in G$, to $(gh)^{-1} = h^{-1}g^{-1}$.

(4) Przyporządkowanie

$$G \ni g \mapsto g^{-1} \in G$$

jest bijekcją.

Dowód.

(1) Teza wynika z równości $1 \cdot 1 = 1$, która jest konsekwencją faktu, że 1 jest elementem neutralnym. Inaczej, mamy ciąg równości

$$1^{-1} = 1 \cdot 1^{-1} = (1 \cdot 1) \cdot 1^{-1} = 1 \cdot (1 \cdot 1^{-1}) = 1 \cdot 1 = 1.$$

(2) Teza wynika z równości

$$g \cdot g^{-1} = 1 = g^{-1} \cdot g,$$

które wynikają z faktu, że g jest elementem odwrotnym do elementu g. Inaczej, mamy ciąg równości

$$(g^{-1})^{-1} = (g^{-1})^{-1} \cdot (g^{-1} \cdot g) = ((g^{-1})^{-1} \cdot g^{-1}) \cdot g = 1 \cdot g = g.$$

(3) Ponieważ $gg^{-1} = 1 = hh^{-1}$ oraz 1 jest elementem neutralnym, więc otrzymujemy ciąg równości

$$g \cdot h \cdot h^{-1} \cdot g^{-1} = g \cdot (h \cdot h^{-1}) \cdot g^{-1} = g \cdot 1 \cdot g^{-1} = g \cdot g^{-1} = 1.$$

Analogicznie pokazujemy, że $h^{-1} \cdot g^{-1} \cdot g \cdot h = 1$, co kończy dowód. Inaczej, mamy ciąg równości

$$\begin{aligned}(gh)^{-1} &= (gh)^{-1} \cdot 1 = (gh)^{-1} \cdot g \cdot g^{-1} = (gh)^{-1} \cdot g \cdot 1 \cdot g^{-1} \\ &= (gh)^{-1} \cdot g \cdot h \cdot h^{-1} \cdot g^{-1} = ((gh)^{-1} \cdot (g \cdot h)) \cdot h^{-1} \cdot g^{-1} \\ &= 1 \cdot h^{-1} \cdot g^{-1} = h^{-1} \cdot g^{-1}.\end{aligned}$$

(4) Teza jest konsekwencją punktu (2). Dokładniej, jeśli $\sigma\colon G \to G$ jest funkcją daną wzorem

$$\sigma(g) := g^{-1} \qquad (g \in G),$$

to z punktu (2) wynika, że $\sigma \circ \sigma = \mathrm{Id}_G$. □

Definicja.

Niech x będzie elementem półgrupy X.

Jeśli $n \in \mathbb{N}_+$, to definiujemy

$$x^n := \begin{cases} x & \text{jeśli } n = 1, \\ x^{n-1}x & \text{jeśli } n > 1. \end{cases}$$

Jeśli dodatkowo X jest monoidem, to definiujemy

$$x^0 := 1.$$

Wreszcie, jeśli X jest grupą oraz $n \in \mathbb{Z}_-$, to definiujemy

$$x^n := (x^{-1})^{-n}.$$

Oznaczenie.
Jeśli działanie oznaczamy symbolem $+$, to piszemy nx zamiast x^n.

Lemat 1.2.
(1) Jeśli X jest monoidem (grupą) i $n \in \mathbb{N}$ ($n \in \mathbb{Z}$), to

$$1^n = 1.$$

(2) Jeśli x jest elementem półgrupy (monoidu, grupy) X oraz $n, m \in \mathbb{N}_+$ ($n, m \in \mathbb{N}$, $n, m \in \mathbb{Z}$), to

$$x^{n+m} = x^n x^m \qquad \text{oraz} \qquad (x^n)^m = x^{nm}.$$

Dowód.
Ćwiczenie. □

Definicja.
Niech X będzie zbiorem z działaniami $*$ i $\#$. Mówimy, że działanie $*$ jest rozdzielne względem działania $\#$, jeśli

$$x * (y \# z) = (x * y) \# (x * z)$$

i

$$(x \# y) * z = (x * z) \# (y * z)$$

dla dowolnych elementów x, y i z zbioru X.

Definicja.
Pierścieniem nazywamy zbiór R wraz z dwoma działaniami $+$ i $\cdot$ takimi, że:
(1) zbiór R wraz z działaniem $+$ tworzy grupę abelową;
(2) zbiór R wraz z działaniem $\cdot$ tworzy monoid przemienny;
(3) działanie $\cdot$ jest rozdzielne względem działania $+$.

Jeśli dodatkowo w pierścieniu R mamy $0 \neq 1$ oraz zbiór $R \setminus \{0\}$ wraz z działaniem $\cdot$ tworzy grupę (abelową), to zbiór R z działaniami $+$ i $\cdot$ nazywamy ciałem.

Uwaga.
Działania w (abstrakcyjnym) pierścieniu będziemy zwykle oznaczać symbolami $+$ i $\cdot$ oraz nazywać dodawaniem i mnożeniem, odpowiednio. Dlatego zwykle będziemy identyfikować pierścień ze zbiorem, na którym jest zdefiniowana struktura pierścieniu.

Ponadto, jeśli R jest pierścieniem, to zakładamy, że działanie mnożenia w pierścieniu ma wyższy priorytet niż działanie dodawania. Zatem, na przykład, jeśli r, s i t są elementami pierścienia R, to

$$rs + t := (r \cdot s) + t.$$

Definicja.

Jeśli R jest pierścieniem, to zbiór R wraz z działaniem $+$ będziemy nazywać grupą addytywną pierścienia R. Podobnie, zbiór R wraz z działaniem $\cdot$ będzie nazywać monoidem multiplikatywnym pierścienia R.

Terminologia.

Sformułowanie „X jest strukturą algebraiczną" oznacza, że X jest pierścieniem, grupą, monoidem lub półgrupą.

Przykłady.

(1) Zbiór liczb całkowitych (wymiernych, rzeczywistych, zespolonych) z działaniami dodawania i mnożenia jest pierścieniem, który oznaczamy $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$, odpowiednio.

(2) Jeśli n jest dodatnią liczbą całkowitą, to zbiór reszt z dzielenia przez n z działaniami dodawania i mnożenia modulo n jest pierścieniem, który oznaczamy $\mathbb{Z}_n$.

(3) Jeśli R jest pierścieniem, to zbiór wielomianów o współczynnikach w pierścieniu R z działaniami dodawania i mnożenia wielomianów jest pierścieniem, który oznaczamy $R[X]$.

(4) Jeśli R jest pierścieniem, to zbiór szeregów formalnych o współczynnikach w pierścieniu R z działaniami dodawania i mnożenia szeregów formalnych jest pierścieniem, który oznaczamy $R[[X]]$.

(5) Jeśli $R_1, \ldots, R_n$ są pierścieniami, to zbiór $R_1 \times \cdots \times R_n$ z dodawaniem i mnożeniem po współrzędnych jest pierścieniem. W szczególności, jeśli R jest pierścieniem oraz n jest dodatnią liczbą całkowitą, to zbiór R^n ciągów długości n o współczynnikach w zbiorze R z dodawaniem i mnożeniem po współrzędnych jest pierścieniem.

Przykłady.

(1) Jeśli R jest pierścieniem, to zbiór $R^\times$ elementów odwracalnych w pierścieniu R z działaniem mnożenia jest grupą, którą nazywamy grupą multiplikatywną pierścienia R.

(2) Jeśli n jest dodatnią liczbą całkowitą oraz F jest ciałem, to zbiór $\mathrm{GL}_n(F)$ $n \times n$-macierzy odwracalnych o współczynnikach w ciele F jest grupą.

Lemat 1.3.

Jeśli R jest pierścieniem, to $0 \cdot r = 0 = r \cdot 0$ dla każdego elementu r pierścienia R. Ponadto, jeśli r i s są elementami pierścienia R, to

$$-r \cdot s = (-r) \cdot s = r \cdot (-s).$$

Dowód.

Mamy ciąg równości

$$0 \cdot r = 0 \cdot r + 0 \cdot r - 0 \cdot r = (0 + 0) \cdot r - 0 \cdot r = 0 \cdot r - 0 \cdot r = 0.$$

Ponadto

$$(-r) \cdot s = (-r) \cdot s + r \cdot s - r \cdot s = ((-r) + r) \cdot s - r \cdot s = 0 \cdot s - r \cdot s = 0 - r \cdot s = -r \cdot s.$$

co kończy dowód. □

1.2. Homomorfizmy

Definicja.

Niech X i Y będą półgrupami z działaniami $*$ i $\star$ odpowiednio. Homomorfizmem nazywamy każdą funkcję $\varphi\colon X \to Y$ taką, że

$$\varphi(x_1 * x_2) = \varphi(x_1) \star \varphi(x_2)$$

dla dowolnych elementów x_1 i x_2 zbioru X.

Sformułowanie: „$\varphi\colon X \to Y$ jest homomorfizmem półgrup (monoidów, grup)" oznacza, że X i Y są półgrupami (monoidami, grupami, odpowiednio) oraz φ jest homomorfizmem półgrup.

Jeśli R i S są pierścieniami, to funkcję $\varphi\colon R \to S$ nazywamy homomorfizmem pierścieni, jeśli φ jest homomorfizmem grup addytywnych oraz monoidów multiplikatywnych pierścieni R i S.

Stwierdzenie 1.4.

(1) Jeśli X jest strukturą algebraiczną, to Id_X jest homomorfizmem.

(2) Jeśli $\varphi\colon X \to Y$ i $\psi\colon Y \to Z$ są homomorfizmami, to $\psi \circ \varphi$ też jest homomorfizmem.

Dowód.

Ćwiczenie. □

Przykłady.

(1) Jeśli n jest dodatnią liczbą całkowitą, to funkcja $\mathbb{Z} \to \mathbb{Z}_n$, która przyporządkowuje liczbie całkowitej jej resztę z dzielenia przez n, jest homomorfizmem grup i pierścieni.

(2) Funkcja $\mathbb{R} \to \mathbb{R}^\times$, która przyporządkowuje liczbie rzeczywistej x liczbę e^x, jest homomorfizmem grup.

(3) Jeśli n jest dodatnią liczbą całkowitą, to funkcja $S_n \to \mathbb{T}_2$, która przyporządkowuje permutacji σ jej znak $\operatorname{sign}\sigma$, jest homomorfizmem grup.

(4) Jeśli F jest ciałem oraz n jest dodatnią liczbą całkowitą, to funkcja $\mathbb{M}_n(F) \to F$, która przyporządkowuje macierzy jej ślad, jest homomorfizmem grup.

(5) Jeśli F jest ciałem oraz n jest dodatnią liczbą całkowitą, to funkcja $\mathrm{GL}_n(F) \to F^\times$, która przyporządkowuje macierzy jej wyznacznik, jest homomorfizmem grup.

(6) Jeśli R jest pierścieniem oraz r jest elementem pierścienia R, to funkcja $R[X] \to R$, która przyporządkowuje wielomianowi f wartość $f(r)$, jest homomorfizmem pierścieni.

(7) Jeśli R jest pierścieniem, n dodatnią liczbą całkowitą oraz $i \in \{1, \ldots, n\}$, to funkcja $\iota_i \colon R \to R^n$, która przyporządkowuje elementowi $r \in R$ ciąg $(0, \ldots, 0, r, 0, \ldots, 0)$, gdzie r znajduje się na i-tym miejscu, jest homomorfizmem pierścieni. Zauważmy, że $\iota_i(1)$ nie jest elementem neutralnym pierścienia R, jeśli $n > 1$.

Stwierdzenie 1.5.
Jeśli $\varphi \colon G \to H$ jest homomorfizmem grup, to

$$\varphi(1) = 1$$

oraz

$$\varphi(g^{-1}) = (\varphi(g))^{-1}$$

dla dowolnego elementu g grupy G.

Dowód.
Mamy ciąg równości

$$\begin{aligned}\varphi(1) = \varphi(1) \cdot 1 = \varphi(1) \cdot \varphi(1) \cdot (\varphi(1))^{-1} \\ = \varphi(1 \cdot 1) \cdot (\varphi(1))^{-1} = \varphi(1) \cdot (\varphi(1))^{-1} = 1.\end{aligned}$$

Ustalmy teraz element g grupy G. Wtedy

$$\begin{aligned}\varphi(g^{-1}) = \varphi(g^{-1}) \cdot 1 = \varphi(g^{-1}) \cdot \varphi(g) \cdot (\varphi(g))^{-1} \\ = \varphi(g^{-1} \cdot g) \cdot (\varphi(g))^{-1} = \varphi(1) \cdot (\varphi(g))^{-1} = 1 \cdot (\varphi(g))^{-1} = (\varphi(g))^{-1},\end{aligned}$$

co kończy dowód. □

Ćwiczenie.
Podać przykład homomorfizmu monoidów $\varphi\colon X \to Y$ takiego, że $\varphi(1) \neq 1$.

Uwaga.
Z powyższego dowodu wynika, że jeśli $\varphi\colon X \to Y$ jest homomorfizmem monoidów i Y jest grupą, to $\varphi(1) = 1$.

Uwaga.
Niech R i S będzie funkcją pomiędzy pierścieniami R i S. Wiemy, że $\varphi\colon R \to S$ jest homomorfizmem pierścieni, jeśli jest homomorfizmem grup addytywnych oraz monoidów multiplikatywnych pierścieni R i S. W szczególności, jeśli $\varphi\colon R \to S$ jest homomorfizmem pierścieni, to $\varphi(0) = 0$ i $\varphi(-r) = -\varphi(r)$ dla każdego elementu r pierścienia R. Nie musi natomiast zachodzić równość $\varphi(1) = 1$. Jeśli jednak S jest ciałem i $\varphi(1) \neq 0$, to $\varphi(1) = 1$.

Ćwiczenie.
Podać przykład homomorfizmu pierścieni $\varphi\colon R \to S$ takiego, że $\varphi(1) \neq 1$.

Definicja.
Homomorfizm $\varphi\colon X \to Y$ nazywamy izomorfizmem, jeśli istnieje homomorfizm $\psi\colon Y \to X$ taki, że

$$\psi \circ \varphi = \mathrm{Id}_X \qquad \text{i} \qquad \varphi \circ \psi = \mathrm{Id}_Y\,.$$

Jeśli φ jest izomorfizmem i $X = Y$, to φ nazywamy automorfizmem struktury X.

Jeśli istnieje izomorfizm $X \to Y$, to mówimy, że struktury algebraiczne X i Y są izomorficzne i piszemy $X \simeq Y$.

Przykłady.

(1) Grupy $\mathbb{Z}_n$ i $\mathbb{T}_n$ są izomorficzne – odpowiedni izomorfizm dany jest wzorem

$$\mathbb{Z}_n \ni k \mapsto \varepsilon_n^k \in \mathbb{T}_n,$$

gdzie ε_n jest pierwiastkiem pierwotnym n-tego stopnia z 1.

(2) Grupy $\mathbb{R}$ i $\mathbb{R}_+ := ((0,\infty),\cdot)$ są izomorficzne – odpowiedni izomorfizm dany jest wzorem

$$\mathbb{R} \ni x \mapsto e^x \in \mathbb{R}_+,$$

a izomorfizm odwrotny

$$\mathbb{R}_+ \ni y \mapsto \ln y \in \mathbb{R}.$$

Definicja.

Homomorfizm $\varphi\colon X \to Y$ nazywam monomorfizmem, jeśli φ jest injekcją.

Homomorfizm φ nazywamy epimorfizmem, jeśli φ jest surjekcją.

Stwierdzenie 1.6.

Homomorfizm $\varphi\colon X \to Y$ jest izomorfizmem wtedy i tylko wtedy, gdy φ jest monomorfizmem i epimorfizmem.

Dowód.

Jest oczywiste, że jeśli φ jest izomorfizmem, to φ jest monomorfizmem i epimorfizmem. Załóżmy zatem, że φ jest monomorfizmem i epimorfizmem. Wtedy istnieje funkcja $\psi\colon Y \to X$ taka, że

$$\psi \circ \varphi = \mathrm{Id}_X \qquad \text{i} \qquad \varphi \circ \psi = \mathrm{Id}_Y .$$

Musimy pokazać, ψ jest homomorfizmem. W tym celu ustalmy odpowiadające sobie działania $*$ i $\star$ w zbiorach X i Y, odpowiednio, oraz elementy y_1 i y_2 zbioru Y. Niech

$$x_1 := \psi(y_1) \qquad \text{i} \qquad x_2 := \psi(y_2).$$

Wtedy również

$$\varphi(x_1) = y_1 \qquad \text{i} \qquad \varphi(x_2) = y_2.$$

Stąd

$$\psi(y_1 \star y_2) = \psi(\varphi(x_1) \star \varphi(x_2)) = \psi(\varphi(x_1 * x_2)) = x_1 * x_2 = \psi(y_1) * \psi(y_2). \quad \square$$

1.3. Podstruktury

Definicja.

Podzbiór Y półgrupy X nazywamy podpółgrupą, jeśli $y_1 \cdot y_2 \in Y$ dla dowolnych elementów y_1 i y_2 zbioru Y.

Uwaga.

Jeśli Y jest podpółgrupą półgrupy X, to funkcja $\cdot|^{Y}_{Y\times Y}\colon Y \times Y \to Y$ jest działaniem w zbiorze Y, które również oznaczamy symbolem $\cdot$. Wtedy zbiór Y z działaniem $\cdot$ jest półgrupą

Definicja.

Zbiór Y nazywamy podmonoidem/podgrupą monoidu/grupy X, jeśli Y jest podpółgrupą półgrupy X oraz zbiór Y wraz z działaniem $\cdot$ jest monoidem/grupą. Podobnie, zbiór S nazywamy podpierścieniem pierścienia R, jeśli S jest podgrupą grupy addytywnej pierścienia R oraz S jest podmonoidem monoidu multiplikatywnego pierścienia R.

Uwaga.

Zbiór S jest podpierścieniem pierścienia R wtedy i tylko wtedy, gdy S jest podpółgrupą grupy addytywnej pierścienia R, S jest podpółgrupą monoidu multiplikatywnego pierścienia R oraz zbiór S wraz z działaniami $+$ i $\cdot$ jest pierścieniem.

Terminologia.

Sfromułowanie „Y jest podstrukturą struktury X" oznacza, że X jest pierścieniem, grupą, monoidem, półgrupą, a Y jest podpierścieniem, podgrupą, podmonoidem, podpółgrupą, odpowiednio. Jeśli Y jest podstrukturą stuktury X, to piszemy $Y \leq X$.

Uwaga.

Jeśli $Y \leq X$ i $Z \leq Y$ (tego samego typu), to $Z \leq X$.

Przykład.

Jeśli X jest strukturą algebraiczną, to $X \leq X$.

Stwierdzenie 1.7.

Niech Y będzie podstrukturą struktury algebraicznej X. Wtedy odwzorowanie $\mu\colon Y \to X$ dane wzorem $\mu(y) := y$, $y \in Y$, jest monomorfizmem, który nazywamy naturalnym włożeniem.

Dowód.

Ćwiczenie.

Stwierdzenie 1.8.

(1) Podzbiór Y monoidu X jest podmonoidem wtedy i tylko wtedy, gdy spełnione są warunki:
   (a) jeśli $y_1, y_2 \in Y$, to $y_1 \cdot y_2 \in Y$;
   (b) istnieje element e zbioru Y taki, że $e \cdot y = y = y \cdot e$ dla każdego elementu y zbioru Y.

(2) Podzbiór H grupy G jest podgrupą wtedy i tylko wtedy, gdy spełnione są warunki:
   (a) jeśli $h_1, h_2 \in H$, to $h_1 \cdot h_2 \in H$;
   (b) $1 \in H$;
   (c) jeśli $h \in H$, to $h^{-1} \in H$.

(3) Podzbiór S pierścienia R jest podpierścieniem wtedy i tylko wtedy, gdy spełnione są warunki:
   (a) jeśli $s_1, s_2 \in S$, to $s_1 + s_2 \in S$;
   (b) $0 \in S$;
   (c) jeśli $s \in S$, to $s^{-1} \in S$;

(d) jeśli $s_1, s_2 \in S$, to $s_1 \cdot s_2 \in S$;

(e) istnieje element e zbioru S taki, że $e \cdot s = s = s \cdot e$ dla każdego elementu s zbioru S.

Dowód.

Punkt (1) jest oczywisty. Dla dowodu punktu (2) musimy pokazać, że jeśli H jest podgrupą grupy G, to $1 \in H$ oraz $h^{-1} \in H$ dla każdego elementu h zbioru H. Ponieważ H jest podmonoidem grupy G, więc na mocy punktu (1) istnieje element e zbioru H taki, że $e \cdot e = e$. Wtedy

$$1 = e \cdot e^{-1} = e \cdot e \cdot e^{-1} = e \cdot 1 = e,$$

a więc $1 \in H$. W szczególności, 1 jest elementem neutralnym grupy H. Ustalmy teraz element $h \in H$. Wtedy istnieje element l zbioru H taki, że $h \cdot l = 1$. Stąd

$$h^{-1} = h^{-1} \cdot 1 = h^{-1} \cdot h \cdot l = 1 \cdot l = l,$$

a więc $h^{-1} \in H$.

Punkt (3) wynika natychmiast z punktów (2) i (1). □

Uwaga.

Z powyższego dowodu wynika, że jeśli G jest grupą, a Y jest podmonoidem grupy G, to $1 \in Y$.

Przykłady.

(1) Jeśli G jest grupą, to zbiory $\{1\}$ i G są podgrupami grupy G, które nazywamy PODGRUPAMI TRYWIALNYMI.

(2) Jeśli n jest liczbą całkowitą, to zbiór $n\mathbb{Z}$ liczb całkowitych podzielnych przez n jest podgrupą grupy $\mathbb{Z}$.

(3) Jeśli F jest jednym ze zbiorów $\mathbb{Q}$ i $\mathbb{R}$, to zbiór F_+ jest podgrupą grupy $F^\times$.

(4) Zbiór $\mathbb{T}$ liczb zespolonych o module 1 jest podgrupa grupą grupy $\mathbb{C}^\times$.

(5) Jeśli n jest dodatnią liczbą całkowitą, to zbiór A_n permutacji parzystych zbioru $\{1, \ldots, n\}$ jest podgrupą grupy S_n, którą nazywamy GRUPĄ ALTERNUJĄCĄ.

(6) Jeśli V jest przestrzenią liniową, to zbiór $\mathrm{GL}(V)$ odwracalnych endomorfizmów przestrzeni V jest podgrupą grupy S_V.

(7) Jeśli G jest grupą, to zbiór $\mathrm{Aut}(G)$ automorfizmów grupy G jest podgrupą grupy S_G.

(8) Jeśli F jest ciałem i n jest dodatnią liczbą całkowitą, to zbiór $\mathrm{SL}_n(F)$ macierzy o wyznaczniku równym 1 jest podgrupą grupy $\mathrm{GL}_n(F)$.

Przykłady.

(1) Jeśli R jest pierścieniem, to zbiory $\{0\}$ i R są podpierścieniami pierścienia R, które nazywamy PODPIERŚCIENIAMI TRYWIALNYMI.

(2) Mamy następujący ciąg podpierścieni $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

(3) Jeśli S jest podpierścieniem pierścienia R, to pierścień $S[X]$ jest podpierścieniem pierścienia $R[X]$.

(4) Jeśli R jest pierścieniem, to $R[X]$ jest podpierścieniem pierścienia $R[[X]]$.

(5) Jeśli n jest dodatnią liczbą całkowitą i R jest pierścieniem, to zbiór $R[X^n]$ wielomianów, w których wszystkie nietrywialne wyrazy mają stopień podzielny przez n, jest podpierścieniem pierścienia $R[X]$.

(6) Zbiór $\{0, 2, 4\}$ jest pierścieniem pierścienia $\mathbb{Z}_6$ – elementem neutralnym dla mnożenia jest 4.

(7) Zbiór funkcji ciągłych $[0, 1] \to \mathbb{R}$ jest podpierścieniem pierścienia $R^{[0,1]}$.

Stwierdzenie 1.9.

Podzbiór H grupy G jest podgrupą grupy G wtedy i tylko wtedy, gdy $H \neq \varnothing$ oraz $h_1 \cdot h_2^{-1} \in H$ dla dowolnych elementów h_1 i h_2 podzbioru H.

Dowód.

Załóżmy najpierw, że podzbiór H jest podgrupą grupy G. Wtedy $1 \in H$, więc $H \neq \varnothing$. Jeśli $h_1, h_2 \in H$, to $h_2^{-1} \in H$, więc $h_1 \cdot h_2^{-1} \in H$.

Załóżmy teraz, że spełniony jest warunek przedstawiony w stwierdzeniu. Wybierzmy element $h_0 \in H$. Wtedy $1 = h_0 \cdot h_0^{-1} \in H$. Ponadto, jeśli $h \in H$, to $h^{-1} = 1 \cdot h^{-1} \in H$. Wreszcie, jeśli $h_1, h_2 \in H$, to $h_2^{-1} \in H$, więc $h_1 \cdot h_2 = h_1 \cdot (h_2^{-1})^{-1} \in H$. □

Definicja.

Jeśli $\varphi\colon X \to Y$ jest homomorfizmem struktur algebraicznych, to definiujemy zbiór $\operatorname{Im}\varphi \subseteq Y$ wzorem

$$\operatorname{Im}\varphi := \{\varphi(x) : x \in X\}.$$

Zbiór $\operatorname{Im}\varphi$ nazywamy OBRAZEM homomorfizmu φ.

Stwierdzenie 1.10.

Jeśli $\varphi\colon X \to Y$ jest homomorfizmem struktur algebraicznych oraz $X' \leq X$, to $\varphi(X') \leq Y$.

W szczególności, $\operatorname{Im}\varphi \leq Y$.

Dowód.

Udowodnimy to stwierdzenie w przypadku pierścieni, korzystając ze Stwierdzenia 1.8(3). Dowody w pozostałych przypadkach są szczególnymi przypadkami dowodu w przypadku pierścieni.

Załóżmy najpierw, że $y_1, y_2 \in \varphi(X')$. Z definicji istnieją wtedy $x_1, x_2 \in X$ takie, że $\varphi(x_1) = y_1$ i $\varphi(x_2) = y_2$. Ponieważ $X' \leq X$, więc $x_1 + x_2, x_1 \cdot x_2 \in X'$. Wtedy

$$y_1 + y_2 = \varphi(x_1) + \varphi(x_2) = \varphi(x_1 + x_2) \in \varphi(X')$$

oraz

$$y_1 \cdot y_2 = \varphi(x_1) \cdot \varphi(x_2) = \varphi(x_1 \cdot x_2) \in \varphi(X').$$

Następnie, ze Stwierdzenia 1.5 wynika, że $\varphi(0) = 0$, więc $0 \in \varphi(X')$. Podobnie, jeśli $y \in Y$, to istnieje $x \in X'$ taki, że $y = \varphi(x)$. Ponieważ $-x \in X'$ oraz, na mocy Stwierdzenia 1.5, $\varphi(-x) = -\varphi(x)$, więc

$$-y = -\varphi(x) = \varphi(-x) \in \varphi(X').$$

Na zakończenie dowodu należy zauważyć, że jeśli e jest elementem neutralnym dla mnożenia w zbiorze X', to element $\varphi(e)$ jest elementem neutralnym dla mnożenia w zbiorze $\varphi(X')$. □

Definicja.

Jeśli $\varphi\colon G \to H$ jest homomorfizmem grup, to definiujemy zbiór $\operatorname{Ker}\varphi \subseteq G$ wzorem

$$\operatorname{Ker}\varphi := \{g \in G : \varphi(g) = 1\}.$$

Zbiór $\operatorname{Ker}\varphi$ nazywamy jądrem homomorfizmu φ.

Uwaga.

Jeśli $\varphi\colon R \to S$ jest homomorfizmem pierścieni, to φ jest również homomorfizmem grup addytywnych pierścieni R i S. Zatem zbiór $\operatorname{Ker}\varphi$ jest również zdefiniowany dla homomorfizmów pierścieni. W tym przypadku

$$\operatorname{Ker}\varphi = \{r \in R : \varphi(r) = 0\}.$$

Stwierdzenie 1.11.

Jeśli $\varphi\colon G \to H$ jest homomorfizmem grup i H' jest podgrupą grupy H, to zbiór $\varphi^{-1}(H')$ jest podgrupą grupy G.

W szczególności, zbiór $\operatorname{Ker}\varphi$ jest podgrupą grupy G.

Dowód.

Skorzystamy ze Stwierdzenia 1.8(2).

Załóżmy najpierw, że $g_1, g_2 \in \varphi^{-1}(H')$. Wtedy $\varphi(g_1), \varphi(g_2) \in H'$, więc $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2) \in H'$, więc $g_1 \cdot g_2 \in \varphi^{-1}(H')$.

Wiemy, że $\varphi(1) = 1$ na mocy Stwierdzenia 1.5 oraz $1 \in H'$, więc $1 \in \varphi^{-1}(H')$.

Na zakończenie załóżmy, że $g \in \varphi^{-1}(H')$. Wtedy $\varphi(g) \in H'$, więc również $(\varphi(g))^{-1} \in H'$. Ze Stwierdzenia 1.5 wiemy jednak, że $(\varphi(g))^{-1} = \varphi(g^{-1})$, co kończy dowód. □

Przykład.

Niech $\varphi\colon \mathbb{Z} \to \mathbb{Z}_6$ będzie homomorfizmem danym wzorem $\varphi(k) := k \bmod 6$, $k \in \mathbb{Z}$. Wtedy zbiór $\varphi^{-1}(\{0, 2, 4\}) = \{0, \pm 2, \pm 4, \ldots\}$ nie jest podpierścieniem pierścienia $\mathbb{Z}$, mimo iż zbiór $\{0, 2, 4\}$ jest podpierścieniem pierścienia $\mathbb{Z}_6$.

Stwierdzenie 1.12.

Niech $\varphi\colon G \to H$ będzie homomorfizmem grup.

(1) φ jest monomorfizmem wtedy i tylko wtedy, gdy $\operatorname{Ker}\varphi = \{1\}$.

(2) φ jest epimorfizmem wtedy i tylko wtedy, gdy $\operatorname{Im}\varphi = H$.

(3) φ jest izomorfizmem wtedy i tylko wtedy, gdy $\operatorname{Ker}\varphi = \{1\}$ i $\operatorname{Im}\varphi = H$.

Uwaga.

Zauważmy, że jeśli φ jest homomorfizmem grup, to $\operatorname{Ker}\varphi = \{1\}$ wtedy i tylko wtedy, gdy $|\operatorname{Ker}\varphi| = 1$.

Dowód.

Punkt (3) wynika natychmiast z punktów (1) i (2) oraz Stwierdzenia 1.6. Punkt (2) jest oczywisty. Dla dowodu punktu (1) wystarczy pokazać, że jeśli $\operatorname{Ker}\varphi = \{1\}$, to funkcja φ jest różnowartościowa. Załóżmy zatem, że $\varphi(g_1) = \varphi(g_2)$. Wtedy $\varphi(g_1 \cdot g_2^{-1}) = 1$, tzn. $g_1 \cdot g_2^{-1} \in \operatorname{Ker}\varphi$. Stąd $g_1 \cdot g_2^{-1} = 1$, a więc $g_1 = g_2$. □

Lemat 1.13.

Niech G będzie grupą. Jeśli H_i, $i \in I$, są podgrupami grupy G, to zbiór $\bigcap_{i \in I} H_i$ jest podgrupą grupy G.

Dowód.

Ćwiczenie. □

Przykład.

Niech R będzie pierścieniem $\mathbb{Z}_2 \times \mathbb{Z}_4$ (z działaniami po współrzędnych). Wtedy zbiory $R_1 := \{(0,0), (0,1), (0,2), (0,3)\}$ i $S_2 := \{(0,0), (1,1), (0,2), (1,3)\}$ są podpierścieniami pierścienia R, ale zbiór $R_1 \cap R_2 = \{(0,0), (0,2)\}$ nie jest

podpierścieniem pierścienia R.

Stwierdzenie 1.14.
Jeśli X jest podzbiorem grupy G, to istnieje najmniejsza (w sensie inkluzji) podgrupa grupy G zawierająca zbiór X. Tę grupę nazywamy PODGRUPĄ GENEROWANĄ przez zbiór X oraz oznaczamy $\langle X \rangle$.

Dowód.
Niech H_i, $i \in I$, będą wszystkimi podgrupami grupy G zawierającymi zbiór X. Wtedy $\bigcap_{i \in I} H_i$ jest szukaną podgrupą. □

Oznaczenie.
Jeśli $X = \{g_1, \ldots, g_n\}$ jest podzbiorem grupy G, to piszemy $\langle g_1, \ldots, g_n \rangle$ zamiast $\langle \{g_1, \ldots, g_n\} \rangle$.

Stwierdzenie 1.15.
Jeśli X jest podzbiorem grupy G, to

$$\langle X \rangle = \{g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n} : n \in \mathbb{N},\, g_1, \ldots, g_n \in X,\, \varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}\}.$$

Dowód.
Łatwo zauważyć, że jeśli H jest podgrupą grupy G zawierającą podzbiór X, to każdy element powyższej postaci należy do H. Z drugiej strony, zbiór opisany w stwierdzeniu oczywiście jest podgrupą grupy H (np. $(g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n})^{-1} = g_n^{-\varepsilon_n} \cdots g_1^{-\varepsilon_1}$), co kończy dowód. □

Wniosek 1.16.
Jeśli g jest elementem grupy G, to

$$\langle g \rangle = \{g^m : m \in \mathbb{Z}\}.$$

Dowód.
Wystarczy zauważyć, że $g^{\varepsilon_1} \cdots g^{\varepsilon_n} = g^{\varepsilon_1 + \cdots + \varepsilon_n}$. □

Wniosek 1.17.
Jeśli G jest grupą abelową oraz $g_1, \ldots, g_n \in G$, to

$$\langle g_1, \ldots, g_n \rangle = \{g_1^{m_1} \cdots g_n^{m_n} : n \in \mathbb{N},\, m_1, \ldots, m_n \in \mathbb{Z}\}.$$

Dowód.
Ćwiczenie. □

1.4. Struktury ilorazowe

Definicja.
Relacją kongurencji (kongruencją) w półgrupie (monoidzie, grupie)

X nazywamy każdą relację równoważności $\sim$ w zbiorze X taką, że jeśli x_1, x_2, y_1 i y_2 są elementami zbioru X oraz $x_1 \sim x_2$ i $y_1 \sim y_2$, to $x_1 \cdot y_1 \sim x_2 \cdot y_2$.

Jeśli R jest pierścieniem, to relacja $\sim$ w zbiorze R jest KONGURENCJĄ w pierścieniu R, jeśli $\sim$ jest kongurencją w grupie addytywnej i monoidzie multiplikatywnym pierścienia R.

Przykłady.

(1) Jeśli n jest dodatnią liczbą całkowitą, to relacja przystawania modulo n jest relacją kongruencji w grupie/pierścieniu $\mathbb{Z}$.

(2) Jeśli r jest elementem pierścienia R, to relacja $\sim$ w pierścieniu wielomianów $R[X]$ zdefiniowana wzorem $f \sim g$ wtedy i tylko wtedy, gdy $f(r) = g(r)$, jest relacją kongruencji.

(3) Niech $\varphi\colon X \to Y$ będzie homomorfizmem struktur algebraicznych. Definiujemy relację $\sim_\varphi$ w zbiorze X wzorem $x_1 \sim_\varphi x_2$ wtedy i tylko wtedy, gdy $\varphi(x_1) = \varphi(x_2)$. Wtedy relacja $\sim_\varphi$ jest relacją kongruencji. Zauważmy, że obie powyższe relacje są szczególnymi przykładami relacji tego typu. Innymi przykładami relacji otrzymanych w ten sposób są następujące relacje:
   (a) Jeśli F jest ciałem i n jest dodatnią liczbą całkowitą, to relacja $\sim$ w grupie $\mathrm{GL}_n(F)$ zdefiniowana wzorem: $A \sim B$ wtedy i tylko wtedy, gdy $\det A = \det B$, jest kongruencją.
   (b) Jeśli n jest dodatnią liczbą całkowitą, to relacja $\sim$ w grupie S_n zdefiniowana wzorem: $\sigma \sim \tau$ wtedy i tylko wtedy, gdy $\operatorname{sign}\sigma = \operatorname{sign}\tau$, jest kongruencją.

Lemat 1.18.

Niech $\sim$ będzie relacją kongruencji w grupie G. Jeśli g i h są elementami grupy G oraz $g \sim h$, to $g^{-1} \sim h^{-1}$.

Dowód.

Mamy następujący ciąg równoważności i równości

$$g^{-1} = g^{-1} \cdot 1 = g^{-1} \cdot h \cdot h^{-1} \sim g^{-1} \cdot g \cdot h^{-1} = 1 \cdot h^{-1} = h^{-1},$$

co kończy dowód. □

Stwierdzenie 1.19.

Jeśli $\sim$ jest relacją kongruencji w półgrupie X i w zbiorze ilorazowym $X/\!\sim$ definiujemy działanie $\cdot$ wzorem

$$[x_1]_\sim \cdot [x_2]_\sim := [x_1 \cdot x_2]_\sim \qquad (x_1, x_2 \in X),$$

Wtedy powyższa definicja jest poprawna.

Dowód.
Ćwiczenie. □

Uwaga.
Powyższe stwierdzenie można stosować oczywiście również w przypadku monoidów i grup. W konsekwencji, możemy je także stosować w przypadku pierścieni.

Przykład.
Jeśli n jest dodatnią liczbą całkowitą i $\equiv_n$ jest relacją przystawania modulo n, to zbiór $\mathbb{Z}/\equiv_n$ z działaniami otrzymanymi ze zwykłych działań dodawania i mnożenia w sposób opisany w Stwierdzeniu 1.19 można utożsamić ze zbiorem reszt z dzielenia przez n z działaniami dodawania i mnożenia modulo n.

Stwierdzenie 1.20.
Jeśli $\sim$ jest relacją kongruencji w pierścieniu (grupie, monoidzie, półgrupie) X, to zbiór $X/\sim$ z działaniami opisanymi w Stwierdzeniu 1.19 jest pierścieniem (grupą, monoidem, półgrupą), który(ą) nazywamy pierścieniem (grupą, monoidem, półgrupą) ilorazowym(ą).

Dowód.
Łatwo sprawdzić, że jeśli działanie w zbiorze X jest łączne/przemienne, to odpowiednie działanie w zbiorze $X/\sim$ jest łączne/przemienne. Podobnie rozdzielność w X indukuje odpowiednią rozdzielność w $X/\sim$. Podobnie, klasa abstrakcji elementu neutralnego dla działania w zbiorze X jest elementem neutralnymi dla odpowiedniego działania w zbiorze $X/\sim$. Wreszcie, elementem odwrotnym (przeciwnym) do klasy abstrakcji elementu $x \in X$ jest klasa abstrakcji elementu odwrotnego (przeciwnego) do x. □

Stwierdzenie 1.21.
Jeśli $\sim$ jest relacją kongruencji w strukturze algebraicznej X, to odwzorowanie $\pi\colon X \to X/\sim$, dane wzorem $\pi(x) := [x]_\sim$, $x \in X$, jest epimorfizmem, który nazywamy naturalnym rzutowaniem.

Dowód.
Ćwiczenie. □

Uwaga.
Jeśli $\sim$ jest relacją kongruencji w strukturze algebraicznej X, to $\sim=\sim_\pi$, gdzie $\pi\colon X \to X/\sim$ jest naturalnym rzutowaniem.

Definicja.
Jeśli $\sim$ jest relacją kongruencji w grupie G, to definiujemy zbiór $N_\sim$ wzorem

$$N_\sim := [1]_\sim.$$

Uwaga.

Jeśli R jest pierścieniem, to R jest grupą ze względu na działanie dodawania. Stąd, jeśli $\sim$ jest relacją kongruencji w pierścieniu R, to

$$N_\sim = [0]_\sim.$$

Przykłady.

(1) Jeśli n jest dodatnią liczbą całkowitą i $\equiv_n$ jest relacją przystawania modulo n, to $N_{\equiv_n}$ jest zbiorem liczb podzielnych przez n.

(2) Jeśli $\varphi\colon X \to Y$ jest homomorfizmem grup (lub pierścieni), to $N_{\sim_\varphi} = \operatorname{Ker}\varphi$.

Definicja.

Podzbiór N grupy G nazywamy dzielnikiem normalnym, jeśli N jest podgrupą grupy G oraz $g \cdot h \cdot g^{-1} \in N$ dla dowolnych elementów $h \in N$ i $g \in G$. Jeśli podzbiór N jest dzielnikiem normalnym grupy G, to piszemy $N \trianglelefteq G$.

Uwaga.

Jeśli grupa G jest abelowa, to każda podgrupa jest dzielnikiem normalnym.

Przykład.

Podzbiór

$$\left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix} \right\}$$

jest podgrupą grupy S_3, która nie jest dzielnikiem normalnym.

Definicja.

Podzbiór I pierścienia R nazywamy ideałem, jeśli I jest podgrupą grupy addytywnej pierścienia R oraz $r \cdot a \in I$ (i $a \cdot r \in I$) dla dowolnych elementów r pierścienia R i a ideału I. Jeśli podzbiór I jest ideałem pierścienia R, to piszemy $I \trianglelefteq R$.

Przykłady.

(1) W każdej grupie G (pierścieniu R) zbiory $\{1\}$ i G ($\{0\}$ i R) są dzielnikami normalnymi (ideałami).

(2) Jeśli n jest dodatnią liczbą całkowitą to podgrupa A_n jest dzielnikiem normalnym grupy S_n.

(3) Jeśli n jest dodatnią liczbą całkowitą, to zbiór $n\mathbb{Z}$ jest ideałem pierścienia $\mathbb{Z}$. Dodatkowo, jeśli $n > 1$, to $n\mathbb{Z}$ nie jest podpierścieniem pierścienia R.

(4) Jeśli R jest pierścieniem i $r \in R$, to zbiór wielomianów $f \in R[X]$ takich, że $f(r) = 0$, jest ideałem pierścienia R.

Lemat 1.22.

(1) Jeśli $\sim$ jest relacją kongruencji w grupie G, to zbiór $N_\sim$ jest dzielnikiem normalnym grupy G.

(2) Jeśli $\sim$ jest relacją kongruencji w pierścieniu R, to zbiór $N_\sim$ jest ideałem pierścienia R.

Dowód.

(1) Jeśli $g_1, g_2 \in N_\sim$, to $g_1 \sim 1$ i $g_2 \sim 1$, skąd $g_1 \cdot g_2 \sim 1 \cdot 1 = 1$. Oczywiście, $1 \in N_\sim = [1]_\sim$. Wreszcie, jeśli $g \sim 1$, to, korzystając z Lematu 1.18, mamy $g^{-1} \sim 1^{-1} = 1$, zatem $N_\sim$ jest podgrupą grupy G. Ponadto, jeśli $g \in G$ i $h \in N$, to $g \cdot h \cdot g^{-1} \sim g \cdot 1 \cdot g^{-1} = 1$, co kończy dowód tego punktu.

(2) Z punktu (1) wiemy już, że $N_\sim$ jest podgrupą grupy addytywnej pierścienia R. Aby zakończyć dowód, załóżmy, że $r \in R$ i $a \in I$. Wtedy $r \cdot a \sim r \cdot 0 = 0$. □

Definicja.

Jeśli H jest podgrupą grupy G, to definiujemy relację $\sim_H$ w zbiorze G wzorem $g_1 \sim_H g_2$ wtedy i tylko wtedy, gdy $g_1^{-1} \cdot g_2 \in H$.

Uwaga.

Jeśli H jest podgrupą grupy addytywnej pierścienia R (np. ideałem), to $r_1 \sim_H r_2$ wtedy i tylko wtedy, gdy $r_2 - r_1 \in H$.

Lemat 1.23.

(1) Jeśli H jest podgrupą grupy G, to relacja $\sim_H$ jest relacją równoważności w zbiorze G.

(2) Jeśli N jest dzielnikiem normalnym grupy G, to relacja $\sim_N$ jest relacją kongruencji w grupie G.

(3) Jeśli I jest ideałem pierścienia R, to relacja $\sim_I$ jest relacją kongruencji w pierścieniu R.

Dowód.

(1) Ćwiczenie.

(2) Jeśli $g_1 \sim_N g_2$ i $h_1 \sim_N h_2$, to

$$(g_1 \cdot h_1)^{-1} \cdot g_2 \cdot h_2 = h_1^{-1} \cdot g_1^{-1} \cdot g_2 \cdot h_2 = h_1^{-1} \cdot g_1^{-1} \cdot g_2 \cdot h_1 \cdot h_1^{-1} \cdot h_2.$$

Z założenia, $g_1^{-1} \cdot g_2, h_1^{-1} \cdot h_2 \in N$. Ponieważ N jest dzielnikiem normalnym, więc $h_1^{-1} \cdot (g_1^{-1} \cdot g_2) \cdot h_1 \in N$. Ostatecznie, $(g_1 \cdot h_1)^{-1} \cdot g_2 \cdot h_2 \in N$.

(3) Jeśli $r_1 \sim_I r_2$ i $s_1 \sim_I s_2$, to

$$r_2 \cdot s_2 - r_1 \cdot s_1 = r_2 \cdot (s_2 - s_1) + s_1 \cdot (r_2 - r_1),$$

skąd łatwo widać, że $r_2 \cdot s_2 - r_1 \cdot s_1 \in I$. □

Oznaczenie.

Jeśli H jest podgrupą grupy G, to piszemy G/H zamiast $G/{\sim_H}$. Podobnie, jeśli I jest ideałem w pierścieniu R, to piszemy R/I zamiast $R/{\sim_I}$.

Przykład.

Jeśli G jest grupą, to $|G/G| = 1$ i $G/\{1\} \simeq G$. Podobne, jeśli R jest pierścieniem, to $R/\{0\} \simeq R$.

Stwierdzenie 1.24.

(1) Jeśli $\sim$ jest relacją kongruencji w grupie G, to $\sim_{N_\sim} = \sim$.

(2) Jeśli N jest dzielnikiem normalnym w grupie G, to $N_{\sim_N} = N$.

Uwaga.

Z powyższego stwierdzenia otrzymujemy również odpowiednią wersję dla pierścieni.

Dowód.

(1) Jeśli $g_1, g_2 \in G$ i $g_1 \sim_{N_\sim} g_2$, to $g_1^{-1} \cdot g_2 \in N_\sim = [1]_\sim$, a więc $g_1^{-1} \cdot g_2 \sim 1$, skąd $g_2 \sim g_1$. Analogicznie, jeśli $g_1 \sim g_2$, to $1 \sim g_1^{-1} \cdot g_2$, więc $g_1^{-1} \cdot g_2 \in N_\sim$, skąd $g_1 \sim_{N_\sim} g_2$.

(2) Postępujemy podobnie jak w punkcie (1). □

Stwierdzenie 1.25.

Jeśli $\varphi\colon X \to Y$ jest homomorfizmem grup (pierścieni) i N jest dzielnikiem normalnym grupy (ideałem pierścienia) Y, to zbiór $\varphi^{-1}(N)$ jest dzielnikiem normalnym grupy (ideałem pierścienia) X.

W szczególności, zbiór $\operatorname{Ker}\varphi$ jest dzielnikiem normalnym grupy (ideałem pierścienia) X.

Dowód.

Wiemy już ze Stwierdzenia 1.11, że zbiór $\varphi^{-1}(N)$ jest podgrupą grupy X. Aby pokazać, że zbiór $\varphi^{-1}(N)$ jest dzielnikiem normalnym grupy X, ustalmy elementy $x \in X$ i $g \in \varphi^{-1}(N)$. Wtedy $\varphi(g) \in N$, więc

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

gdyż zbiór N jest dzielnikiem normalnym grupy Y. Stąd $x \cdot g \cdot x^{-1} \in \varphi^{-1}(N)$.

Wersję dla pierścieni dowodzimy podobnie. □

Stwierdzenie 1.26.

Jeśli $\varphi\colon X \to Y$ jest epimorfizmem grup (pierścieni) i N jest dzielnikiem normalnym grupy (ideałem pierścienia) X, to zbiór $\varphi(N)$ jest dzielnikiem normalnym grupy (ideałem pierścienia) Y.

Dowód.

Wiemy już ze Stwierdzenia 1.10, że zbiór $\varphi(N)$ jest podgrupą grupy Y. Aby pokazać, że zbiór $\varphi(N)$ jest dzielnikiem normalnym grupy Y, ustalmy elementy $y \in Y$ i $h \in \varphi(N)$. Wtedy istnieje element $g \in N$ taki, że $h = \varphi(g)$. Ponieważ φ jest epimorfizmem, więc istnieje element $x \in X$ taki, że $\varphi(x) = y$. Wtedy $x \cdot g \cdot x^{-1} \in N$, gdyż N jest dzielnikiem normalnym grupy. Stąd

$$y \cdot h \cdot y^{-1} = \varphi(x) \cdot \varphi(g) \cdot (\varphi(x))^{-1} = \varphi(x \cdot g \cdot x^{-1}) \in \varphi(N).$$

Wersję dla pierścieni dowodzimy podobnie. □

Przykład.

Jeśli H jest podgrupą grupy G, która nie jest dzielnikiem normalnym, to H jest dzielnikiem normalnym grupy H, ale $\mu(H) = H$ nie jest dzielnikiem normalnym grupy G, gdzie $\mu\colon H \to G$ jest naturalnym włożeniem.

1.5. Twierdzenie Lagrange'a

Definicja.

Jeśli H jest podgrupą grupy G, to definiujemy relację $\sim'_H$ wzorem: $g_1 \sim'_H g_2$ wtedy i tylko wtedy, gdy $g_2 \cdot g_1^{-1} \in H$.

Uwaga.

Jeśli H jest dzielnikiem normalnym grupy G, to relacje $\sim_H$ i $\sim'_H$ się pokrywają.

Lemat 1.27.

Jeśli H jest podgrupą grupy G, to relacja $\sim'_H$ jest relacją równoważności.

Dowód.

Ćwiczenie. □

Oznaczenie.

Jeśli H jest podgrupą grupy G, to piszemy $H\backslash G$ zamiast $G/\sim'_H$.

Oznaczenie.

Jeśli g jest elementem grupy G oraz X podzbiorem grupy G, to definiujemy zbiory gX i Xg wzorami

$$gX := \{g \cdot h : h \in X\} \qquad \text{i} \qquad Xg := \{h \cdot g : h \in X\}.$$

Definicja.

Jeśli g jest elementem grupy G oraz H jest podgrupą grupy G, to zbiory gH i Hg nazywamy warstwami lewo- i prawostronną elementu g względem podgrupy H.

Lemat 1.28.
Jeśli H jest podgrupą grupy G, to

$$[g]_{\sim_H} = gH \qquad \text{oraz} \qquad [g]_{\sim'_H} = Hg$$

dla każdego elementu g grupy G.

Dowód.
Jeśli $g' \in [g]_{\sim_H}$, to $g^{-1} \cdot g' \in H$, a więc $g' = g \cdot (g^{-1} \cdot g') \in gH$. Podobnie, jeśli $g' \in gH$, to $g' = g \cdot h$ dla pewnego elementu $h \in H$, a więc $g^{-1} \cdot g' = h \in H$, skąd $g \sim_H g'$. □

Uwaga.
Z Lematu 1.28 wynika, że jeśli I jest ideałem w pierścieniu R oraz $r \in R$, to

$$[r]_{\sim_I} = r + I.$$

Lemat 1.29.
Jeśli H jest podgrupą grupy G, to zbiory G/H i $H\backslash G$ są równoliczne.

Dowód.
Definiujemy funkcję $\Phi\colon G/H \to H\backslash G$ wzorem

$$\Phi([g]_{\sim_H}) := [g^{-1}]_{\sim'_H} \qquad (g \in G).$$

Zauważmy, że ta funkcja jest poprawnie określona. Istotnie, jeśli $[g_1]_{\sim_H} = [g_2]_{\sim_H}$, to $g_1^{-1} \cdot g_2 \in H$, więc

$$g_2^{-1} \cdot (g_1^{-1})^{-1} = (g_1^{-1} \cdot g_2)^{-1} \in H,$$

skąd $[g_1^{-1}]_{\sim'_H} = [g_2^{-1}]_{\sim'_H}$.
Podobnie pokazujemy, że funkcja $\Psi\colon H\backslash G \to G/H$, dana wzorem

$$\Psi([g]_{\sim'_H}) := [g^{-1}]_{\sim_H} \qquad (g \in G),$$

jest poprawnie określona. Ponadto łatwo widać, że $\Phi \circ \Psi = \mathrm{Id}_{H\backslash G}$ i $\Psi \circ \Phi = \mathrm{Id}_{G/H}$, co kończy dowód. □

Definicja.
Jeśli H jest podgrupą grupy G, to liczbę elementów zbioru G/H (równoważnie, zbioru $H\backslash G$) nazywamy INDEKSEM podgrupy H w grupie G i oznaczamy $[G : H]$.

Twierdzenie 1.30 (Lagrange).
Jeśli H jest podgrupą grupy G, to

$$|G| = |H| \cdot [G : H].$$

Dowód.

Wiadomo, że jeśli $\sim$ jest relacją równoważności w zbiorze X oraz istnieje liczba kardynalna $\mathfrak{a}$ taka, że $|Y| = \mathfrak{a}$ dla każdej klasy abstrakcji $Y \in X/\sim$, to $|X| = \mathfrak{a} \cdot |X/\sim|$. Tezę twierdzenia otrzymamy, stosując powyższą obserwację dla $X = G$ i $\sim = \sim_H$, jeśli pokażemy, że $|Y| = |H|$ dla każdego zbioru $Y \in G/H$. Jeśli jednak $Y \in G/H$, to $Y = [g]_{\sim_H}$ dla pewnego $g \in G$. Wtedy $Y = gH$ na mocy Lematu 1.28. Definiujemy funkcję $\Phi\colon H \to gH$ wzorem $\Phi(h) := gh$, $h \in H$. Z definicji zbioru gH funkcja Φ jest dobrze określona oraz jest surjekcją. Ponadto, jeśli $h_1, h_2 \in H$ i $\Phi(h_1) = \Phi(h_2)$, to

$$h_1 = g^{-1} \cdot g \cdot h_1 = g^{-1} \cdot \Phi(h_1) = g^{-1} \cdot \Phi(h_2) = g^{-1} \cdot g \cdot h_2 = h_2,$$

co kończy dowód. □

Definicja.

Rzędem grupy nazywamy liczbę jej elementów.

Wniosek 1.31.

Jeśli H jest podgrupą grupy skończonej G, to rząd grupy H dzieli rząd grupy G. □

Definicja.

Rzędem elementu g grupy G nazywamy rząd podgrupy $\langle g \rangle$ generowanej przez element G. Rząd elementu g oznaczamy symbolem $\operatorname{ord}(g)$.

Stwierdzenie 1.32.

Jeśli g jest elementem grupy G, to

$$\operatorname{ord}(g) = \min\{n \in \mathbb{N}_+ : g^n = 1\}.$$

W szczególności, jeśli $\operatorname{ord}(g) < \infty$, to

$$\langle g \rangle = \{g^k : k \in \{0, 1, \ldots, \operatorname{ord}(g) - 1\}\}.$$

Uwaga.

W powyższym stwierdzeniu zakładamy, że $\min \varnothing := \infty$.

Dowód.

Niech

$$m := \min\{n \in \mathbb{N}_+ : g^n = 1\}.$$

Pokażmy najpierw, że elementy g^k, $0 \leq k < m$, są parami różne. Istotnie, przypuśćmy, że $g^k = g^l$ dla pewnych liczb całkowitych k i l takich, że $0 \leq k < l < m$. Wtedy

$$g^{l-k} = g^l \cdot (g^k)^{-1} = 1$$

oraz $l - k \in \mathbb{N}_+$ i $l - k < m$, co jest niemożliwe wobec definicji liczby m.

Z powyższej obserwacji oraz Wniosku 1.16 natychmiast wynika, jeśli $m = \infty$, to $\operatorname{ord}(g) = \infty$. Załóżmy zatem, że $m < \infty$. Aby dokończyć dowód, wystarczy, wobec Wniosku 1.16, pokazać, że dla każdej liczby całkowitej n istnieje liczba całkowita k taka, że $0 \leq k < m$ i $g^n = g^k$. Wiemy jednak, że istnieją liczby całkowite q i k takie, że $n = q \cdot m + k$ i $0 \leq k < m$. Wtedy

$$g^n = (g^m)^q \cdot g^k = 1^q \cdot g^k = 1 \cdot g^k = g^k,$$

co kończy dowód. □

1.6. Twierdzenia o izomorfizmie

Uwaga.

Jeśli N jest dzielnikiem normalnym grupy G i H jest podgrupą grupy G zawierającą zbiór N, to N jest dzielnikiem normalnym grupy H. Ponadto, grupa ilorazowa H/N jest podgrupą grupy G/N. Jeśli dodatkowo H jest dzielnikiem normalnym grupy G, to H/N jest dzielnikiem normalnym grupy G/N.

Podobnie, jeśli I i J są ideałem pierścienia R takimi, że $I \subseteq J$, to podgrupa J/I grupy addytywnej pierścienia R/I jest ideałem pierścienia R/I.

Lemat 1.33.

Niech $\varphi\colon X \to Y$ będzie homomorfizmem grup (pierścieni). Jeśli N jest dzielnikiem normalnym grupy (ideałem pierścienia) X takim, że $N \subseteq \operatorname{Ker}\varphi$, to istnieje jedyny homomorfizm $\varphi'\colon X/N \to Y$ taki, że $\varphi = \varphi' \circ \pi$, gdzie $\pi\colon X \to X/N$ jest naturalnym rzutowaniem. Homomorfizm φ' dany jest wzorem

$$\varphi'([x]_{\sim_N}) := \varphi(x) \qquad (x \in X).$$

Ponadto

$$\operatorname{Ker}\varphi' = (\operatorname{Ker}\varphi)/N \qquad \text{i} \qquad \operatorname{Im}\varphi' = \operatorname{Im}\varphi.$$

Dowód.

Udowodnimy lemat w wersji dla grup.

Pokażemy najpierw, że funkcja φ' zdefiniowana powyższym wzorem jest poprawnie określona. Przypuśćmy zatem, że $[x]_{\sim_N} = [y]_{\sim_N}$ dla pewnych elementów x i y grupy X. Wtedy $x^{-1} \cdot y \in N \subseteq \operatorname{Ker}\varphi$, skąd

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

Łatwo widać, że φ' jest istotnie homomorfizmem, $\varphi = \varphi' \circ \pi$ oraz $\operatorname{Im}\varphi' = \operatorname{Im}\varphi$. Ponadto, jeśli $\varphi'([x]_{\sim_N}) = 1$, to $x \in \operatorname{Ker}\varphi$, zatem $\operatorname{Ker}\varphi' = (\operatorname{Ker}\varphi)/N$.

Aby pokazać jedyność homomorfizmu φ', przypuśćmy, że $\psi\colon X/N \to Y$ jest homomorfizmem takim, że $\varphi = \psi \circ \pi$. Wtedy dla każdego elementu $x \in X$ mamy

$$\psi([x]_{\sim_N}) = \psi(\pi(x)) = \varphi(x) = \varphi'([x]_{\sim_N}),$$

co kończy dowód. □

Twierdzenie 1.34 (Pierwsze Twierdzenie o Izomorfizmie).
Jeśli $\varphi\colon X \to Y$ jest homomorfizmem grup (pierścieni), to funkcja

$$\psi\colon X/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi, [x]_{\sim_{\operatorname{Ker}\varphi}} \mapsto \varphi(x),$$

jest izomorfizmem.

Dowód.
Z Lematu 1.33 wiemy, że ψ jest homomorfizmem takim, że

$$\operatorname{Ker}\psi = \operatorname{Ker}\varphi/\operatorname{Ker}\varphi \qquad \text{oraz} \qquad \operatorname{Im}\psi = \operatorname{Im}\varphi.$$

Stąd oraz ze Stwierdzenia 1.12(3) wynika teza. □

Przykłady.

(1) Jeśli n jest dodatnią liczbą całkowitą, to

$$\mathbb{Z} \to \mathbb{Z}_n,\ k \mapsto k \bmod n,$$

indukuje jest izomorfizm $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ (grup i pierścieni).

(2) Funkcja

$$\mathbb{R} \to \mathbb{T},\ x \mapsto \cos(2\pi x) + i\sin(2\pi x),$$

indukuje izomorfizm $\mathbb{R}/\mathbb{Z} \simeq \mathbb{T}$.

(3) Jeśli F jest ciałem, to funkcja

$$\mathrm{GL}_n(F) \to F^\times,\ A \mapsto \det A,$$

indukuje izomorfizm $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \simeq F^\times$.

Twierdzenie 1.35 (Trzecie Twierdzenie o Izomorfizmie (wersja dla grup)).
Niech M i N będą dzielnikami normalnymi grupy G takimi, że $M \subseteq N$. Wtedy

$$(G/M)/(N/M) \simeq G/N.$$

Uwaga.
Mamy analogiczne twierdzenie o izomorfizmie dla pierścieni, w którym dzielniki normalne należy zastąpić ideałami.

Dowód.
Niech $\pi\colon G \to G/N$ będzie naturalnym rzutowaniem. Wtedy $\operatorname{Im}\pi = G/N$ oraz $\operatorname{Ker}\pi = N$. Z Lematu 1.33 istnieje homomorfizm $\pi'\colon G/M \to G/N$ taki, że $\operatorname{Ker}\pi' = N/M$ i $\operatorname{Im}\pi' = G/N$. Zatem teza wynika z Twierdzenia 1.34. □

Przykład.
Niech m i n będą dodatnimi liczbami całkowitymi. Wtedy mamy izomorfizm

$$\mathbb{Z}_{mn}/\{0, m, \ldots, mn - m\} \simeq (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}) \simeq \mathbb{Z}/m\mathbb{Z}.$$

Oznaczenie.
Jeśli X i Y są podzbiorami grupy G, to definiujemy zbiór XY wzorem

$$XY = \{x \cdot y : x \in X \text{ i } y \in Y\}.$$

Uwaga.
Jeśli X jest podzbiorem, a N dzielnikiem normalnym grupy G, to $XN = NX$.

Dowód.
Pokażemy inkluzję $XN \subseteq NX$. Dowód przeciwnej inkluzji jest analogiczny. Zauważmy jednak, że jeśli $x \in X$ i $n \in N$, to $x \cdot n = x \cdot n \cdot x^{-1} \cdot x$ oraz $x \cdot n \cdot x^{-1} \in N$. □

Lemat 1.36.
Jeśli H jest podgrupą, a N dzielnikiem normalnym grupy G, to $H \cap N$ jest dzielnikiem normalnym grupy H oraz HN jest podgrupą grupy G.

Dowód.
Ćwiczenie. □

Twierdzenie 1.37 (Drugie Twierdzenie o Izomorfizmie (wersja dla grup)).
Jeśli H jest podgrupą, a N dzielnikiem normalnym grupy G, to

$$(HN/N) \simeq (H/H \cap N).$$

Dowód.
Niech $\varphi\colon H \to G/N$ będzie złożeniem naturalnego zanurzenia $H \to G$ oraz naturalnego rzutowania $G \to G/N$. Wtedy $\operatorname{Ker}\varphi = H \cap N$. Ponadto $\operatorname{Im}\varphi = HN/N$. Istotnie, inkluzja $\operatorname{Im}\varphi \subseteq HN/N$ jest oczywista. Ponadto, jeśli $h \in H$ i $g \in N$, to $(h \cdot g)N = hN = \varphi(h)$. Stąd teza wynika z Twierdzenia 1.34. □

Twierdzenie 1.38 (Drugie Twierdzenie o Izomorfizmie (wersja dla pierścieni)).
Jeśli S jest podpierścieniem, a I ideałem pierścienia R, to

$$(S + I)/I \simeq S/(S \cap I).$$

Dowód.
Ćwiczenie. □

Uwaga.
Odpowiednikiem Drugiego Twierdzenia o Izomorfizmie dla skończenie wymiarowych przestrzeni liniowych jest wzór

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W).$$

Przykład.
Grupę G nazywamy rozwiązalną, jeśli istnieje ciąg

$$\{1\} = H_0 \subseteq H_1 \subseteq \ldots \subseteq H_n = G$$

podgrup grupy G taki, że dla każdego $i = 1, \ldots, n$ grupa H_{i-1} jest dzielnikiem normalnym grupy H_i takim, że grupa H_i/H_{i-1} jest abelowa. Pokażemy, że jeśli H jest podgrupą grupy rozwiązalnej G, to grupa H jest rozwiązalna.

Istotnie, jeśli mamy ciąg podgrup jak wyżej, to definiujemy ciąg

$$H'_0 \subseteq H'_1 \subseteq \ldots \subseteq H'_n$$

podgrup grupy H wzorami: $H'_i := H_i \cap H$, $i = 1, \ldots, n$. Wtedy oczywiście $H'_0 = \{1\}$ oraz $H'_n = H$. Łatwo też pokazać, że jeśli $i \in \{1, \ldots, n\}$, to grupa H'_{i-1} jest dzielnikiem normalnym grupy H'_i. Ponadto

$$H'_{i-i} = H'_{i-1} \cap H'_i = (H_{i-1} \cap H) \cap H'_i = H_{i-1} \cap (H \cap H'_i) = H_{i-1} \cap H'_i,$$

więc

$$H'_i/H'_{i-1} = H'_i/(H'_i \cap H_{i-1}) \simeq (H'_i H_{i-1})/H_{i-1} \leq H_i/H_{i-1},$$

zatem jest grupą abelową dla każdego $i = 1, \ldots, n$.

2. Teoria podzielności w pierścieniach

2.1. Ideały

Lemat 2.1.

Jeśli I_j, $j \in J$, są ideałami pierścienia R, to zbiór $\bigcap_{j\in J} I_j$ jest ideałem pierścienia R.

Dowód.

Ćwiczenie. □

Stwierdzenie 2.2.

Jeśli X jest podzbiorem pierścienia R, to istnieje najmniejszy ideał pierścienia R zawierający zbiór X. Ten ideał nazywamy IDEAŁEM GENEROWANYM przez zbiór X oraz oznaczamy (X).

Dowód.

Ćwiczenie. □

Oznaczenie.

Jeśli $X = \{r_1, \ldots, r_n\}$ jest podzbiorem pierścienia R, to piszemy $(r_1, \ldots, r_n)$ zamiast $(\{r_1, \ldots, r_n\})$.

Stwierdzenie 2.3.

Jeśli $r_1, \ldots, r_n$ są elementami pierścienia R, to

$$(r_1, \ldots, r_n) = \{s_1 \cdot r_1 + \cdots + s_n \cdot r_n : s_1, \ldots, s_n \in R\}.$$

W szczególności, jeśli $r \in R$, to

$$(r) = \{s \cdot r : s \in R\}.$$

Dowód.

Ćwiczenie. □

Definicja.

Ideał I pierścienia element R, dla którego istnieje element $r \in R$ taki, że $I = (r)$, nazywamy GŁÓWNYM.

Pierścień, w którym każdy ideał jest główny, nazywamy PIERŚCIENIEM IDEAŁÓW GŁÓWNYCH.

Definicja.

Pierścień R nazywamy DZIEDZINĄ (CAŁKOWITOŚCI), jeśli $0 \neq 1$ i dla dowolnych elementów r i s pierścienia R z równości $r \cdot s = 0$ wynika, że $r = 0$ lub $s = 0$.

Pierścień ideałów głównych, który jest dziedziną całkowitości, nazywamy DZIEDZINĄ IDEAŁÓW GŁÓWNYCH.

Przykłady.

(0) Każde ciało jest dziedziną całkowitości.

(1) Pierścień $\mathbb{Z}$ jest dziedziną całkowitości.

(2) Pierścień $R[X]$ jest dziedziną całkowitości wtedy i tylko wtedy, gdy pierścień R jest dziedziną całkowitości.

(3) Pierścień $\mathbb{Z}_n$ jest dziedziną całkowitości wtedy i tylko wtedy, gdy n jest liczbą pierwszą.

(4) Jeśli $|R| < \infty$, to pierścień R jest dziedziną całkowitości wtedy i tylko wtedy, gdy R jest ciałem.

Stwierdzenie 2.4.

Jeśli r, s_1 i s_2 są elementami dziedziny całkowitości R takimi, że $r \neq 0$ i $r \cdot s_1 = r \cdot s_2$, to $s_1 = s_2$.

Dowód.

Równość $r \cdot s_1 = r \cdot s_2$ jest równoważna równości $r \cdot (s_1 - s_2) = 0$. Podobnie, $s_1 = s_2$ wtedy i tylko wtedy, gdy $s_1 - s_2 = 0$. Ponieważ $r \neq 0$, więc teza wynika natychmiast z definicji dziedziny całkowitości.

Definicja.

Ideał I pierścienia R nazywamy pierwszym, jeśli $I \neq R$ i z warunku $r \cdot s \in I$ wynika, że $r \in I$ lub $s \in I$.

Stwierdzenie 2.5.

Ideał I pierścienia R jest pierwszy wtedy i tylko wtedy, gdy pierścień R/I jest dziedziną całkowitości.

Dowód.

Ćwiczenie. □

Przykład.

Jeśli n jest dodatnią liczbą całkowitą, to ideał $n\mathbb{Z}$ jest pierwszy wtedy i tylko wtedy, gdy liczba n jest pierwsza.

Definicja.

Ideał I pierścienia R nazywamy maksymalnym, jeśli $I \neq R$ i z inkluzji $I \subseteq J$, gdzie J jest ideałem, wynika, że $J = I$ lub $J = R$.

Stwierdzenie 2.6.

Ideał I pierścienia R jest maksymalny wtedy i tylko wtedy, gdy pierścień R/I jest ciałem.

Dowód.

Zauważmy najpierw, że warunek $I \neq R$ jest równoważny warunkowi $0 + I \neq$

$1 + I$.

Załóżmy, że ideał I jest maksymalny i ustalmy element r pierścienia R nienależący do ideału I. Niech $J := I + (r)$. Wtedy zbiór J jest ideałem pierścienia R i $I \subset J$. Stąd $J = R$, a więc w szczególności istnieje element s pierścienia R taki, że $s \cdot r + I = 1 + I$.

Załóżmy teraz, że pierścień R/I jest ciałem i ustalmy ideał J pierścienia R taki, że $I \subset J$. Wybierzmy element $r \in J \setminus I$. Wtedy istnieje element s pierścienia R taki, że $s \cdot r + I = 1 + I$. Stąd wynika, że $1 \in J$, a więc $J = R$. □

Przykład.

Jeśli n jest dodatnią liczbą całkowitą, to ideał $n\mathbb{Z}$ jest maksymalny wtedy i tylko wtedy, gdy liczba n jest pierwsza.

Wniosek 2.7.

Każdy ideał maksymalny jest pierwszy. □

Twierdzenie 2.8 (Chińskie Twierdzenie o Resztach).

Niech $I_1, \ldots, I_n$ będą ideałami w pierścieniu R takimi, że $I_i + I_j = R$ dla wszystkich $i, j \in \{1, \ldots, n\}$ takich, że $i \neq j$. Wtedy funkcja $R/(I_1 \cap \ldots \cap I_n) \to R/I_1 \times \cdots \times R/I_n$ dana wzorem

$$r + I_1 \cap \ldots I_n \mapsto (r + I_1, \ldots, r + I_n), \qquad (r \in R),$$

jest izomorfizmem pierścieni.

Dowód.

Definiujemy homomorfizm $\varphi\colon R \to R/I_1 \times \cdots \times R/I_n$ wzorem

$$\varphi(r) := (r + I_1, \ldots, r + I_n), \qquad (r \in R).$$

Wtedy $\operatorname{Ker} \varphi = I_1 \cap \ldots \cap I_n$, więc, korzystając z Pierwszego Twierdzenia o Izomorfizmie, wystarczy pokazać, że φ jest epimorfizmem. W tym celu ustalmy elementy $t_2, \ldots, t_n \in I_1$ oraz $s_2 \in I_2, \ldots, s_n \in I_n$ takie, że

$$t_2 + s_2 = \cdots = t_n + s_n = 1.$$

Jeśli $e_1 := s_2 \cdots s_n$, to $e_1 + I_2 = 0 + I_2, \ldots, e_1 + I_n = 0 + I_n$. Ponadto $e_1 + I_1 = 1 + I_1$. Podobnie pokazujemy, że istnieją elementy $e_2, \ldots, e_n$ takie, że $e_i + I_i = 1 + I_i$ oraz $e_i + I_j = 0 + I_j$, jeśli $j \neq i$. Załóżmy teraz, że $r_1, \ldots, r_n \in R$. Wtedy

$$\varphi(r_1 \cdot e_1 + \cdots + r_n \cdot e_n) = (r_1 + I_1, \ldots, r_n + I_n).$$

Stąd wynika, że φ jest epimorfizmem, co kończy dowód. □

2.2. Dziedziny z jednoznacznością rozkładu

Założenie.

Przez cały podrozdział R jest dziedziną całkowitości.

Definicja.

Mówimy, że element r dziedziny R DZIELI element s dziedziny R (i piszemy $r \mid s$), jeśli istnieje element t dziedziny R taki, że $s = t \cdot r$.

Mówimy, że elementy r i s dziedziny R są STOWARZYSZONE (i piszemy $r \approx s$), jeśli $r \mid s$ i $s \mid r$.

Uwaga.

Relacja podzielności jest zwrotna i przechodnia, tzn. $r \mid r$ dla każdego elementu r oraz jeśli $r \mid s$ i $s \mid t$, to $r \mid t$.

Przypomnienie.

Przypomnijmy, że element r dziedziny R nazywamy odwracalnym, jeśli istnieje element s dziedziny R taki, że $r \cdot s = 1$.

Przykłady.

(1) Jedynymi elementami odwracalnymi w pierścieniu $\mathbb{Z}$ są 1 i -1.

(2) Jedynymi elementami odwracalnymi w pierścieniu $R[X]$ są elementy odwracalne w dziedzinie R.

Stwierdzenie 2.9.

(1) Jeśli r i s są elementami dziedziny R, to $r \mid s$ wtedy i tylko wtedy, gdy $(s) \subseteq (r)$ (równoważnie $s \in (r)$).

(2) Jeśli r i s są elementami dziedziny R, to $r \approx s$ wtedy i tylko wtedy, gdy $(r) = (s)$.

(3) Jeśli r jest elementem dziedziny R, to r jest elementem odwracalnym wtedy i tylko wtedy, gdy $r \mid 1$.

(4) Jeśli r jest elementem dziedziny R, to r jest elementem odwracalnym wtedy i tylko wtedy, gdy $r \mid s$ dla wszystkich $s \in R$.

(5) Jeśli r jest elementem dziedziny R, to r jest elementem odwracalnym wtedy i tylko wtedy, gdy $(r) = R$.

(6) $\approx$ jest relacją równoważności.

(7) Jeśli r i s są elementami dziedziny R, to $r \approx s$ wtedy i tylko wtedy, gdy istnieje element odwracalny $u \in R$ taki, że $r = u \cdot s$.

Dowód.

Ćwiczenie. □

Definicja.

Niezerowy element r dziedziny R nazywamy NIEROZKŁADALNYM, jeśli element r nie jest odwracalny oraz z warunku $s \mid r$ wynika, że $s \approx r$ lub s jest elementem odwracalnym.

Stwierdzenie 2.10.

(1) Niezerowy element r dziedziny R jest nierozkładalny wtedy i tylko wtedy, gdy ideał (r) jest maksymalny w zbiorze wszystkich właściwych ideałów głównych dziedziny R, tzn. $(r) \neq R$ i jeśli I jest ideałem głównym takim, że $(r) \subseteq I$, to $I = (r)$ lub $I = R$.

(2) Element stowarzyszony z elementem nierozkładalnym jest nierozkładalny.

Dowód.

(1) Przypuśćmy najpierw, że element r jest nierozkładalny. Wtedy element r nie jest odwracalny, więc $(r) \neq R$ na mocy Stwierdzenia 2.9(5). Ponadto, niech I będzie ideałem głównym taki, że $(r) \subseteq I$. Wybierzmy element s taki, że $I = (s)$. Wtedy $s \mid r$ na mocy Stwierdzenia 2.9(1). Stąd $s \approx r$ lub element s jest odwracalny. Stąd $I = (s) = (r)$ lub $I = (s) = R$ na mocy Stwierdzenie 2.9.

Implikację przeciwną dowodzimy analogicznie.

(2) Wynika natychmiast z punktu (1) oraz Stwierdzenia 2.9(2). □

Definicja.

Dziedzinę całkowitości R nazywamy DZIEDZINĄ Z ROZKŁADEM, jeśli dla każdego niezerowego i nieodwracalnego elementu r dziedziny R istnieją nierozkładalne elementy $r_1, \ldots, r_n$ w dziedzinie R takie, że

$$r = r_1 \cdots r_n.$$

Definicja.

Dziedzinę z rozkładem R nazywamy DZIEDZINĄ Z JEDNOZNACZNOŚCIĄ ROZKŁADU, jeśli dla dowolnych elementów nierozkładalnych $r_1, \ldots, r_n$ i $s_1, \ldots, s_m$ takich, że

$$r_1 \cdots r_n = s_1 \cdots s_m,$$

mamy $n = m$ oraz istnieje permutacja σ zbioru $\{1, \ldots, n\}$ taka, że $r_i \approx s_{\sigma(i)}$ dla każdego $i = 1, \ldots, n$.

Przykłady.

(1) Pierścień $\mathbb{Z}$ jest dziedziną z jednoznacznością rozkładu.

(2) Niech $R := \{a + b\imath\sqrt{3} : a, b \in \mathbb{Z}\}$. Wtedy R jest podpierścieniem pierścienia $\mathbb{C}$. Ponadto R jest dziedziną z rozkładem, która nie jest dziedziną z jednoznacznością rozkładu. Istotnie, 2 i $1 \pm \imath\sqrt{3}$ są elementami nierozkładalnymi oraz $2 \cdot 2 = (1 + \imath\sqrt{3}) \cdot (1 - \imath\sqrt{3})$, ale $2 \not\approx 1 \pm \imath\sqrt{3}$.

Definicja.

Niezerowy element r dziedziny R nazywamy pierwszym, jeśli element r nie jest odwracalny i z warunku $r \mid s_1 \cdot s_2$ wynika, że $r \mid s_1$ lub $r \mid s_2$.

Stwierdzenie 2.11.

(1) Niezerowy element r dziedziny R jest pierwszy wtedy i tylko wtedy, gdy ideał (r) jest pierwszy.

(2) Element stowarzyszony z elementem pierwszym jest pierwszy.

Dowód.

(1) Zauważmy, że nieodwracalność elementu r, na mocy Stwierdzenia 2.9(5), jest równoważna warunkowi $(r) \neq R$. Ponadto, korzystając ze Stwierdzenia 2.9(1), otrzymujemy równoważność następujących warunków:

- jeśli $r \mid s_1 \cdot s_2$, to $r \mid s_1$ lub $r \mid s_2$;
- jeśli $s_1 \cdot s_2 \in (r)$, to $s_1 \in (r)$ lub $s_2 \in (r)$;

co kończy dowód.

(2) Wynika natychmiast z punktu (1) oraz Stwierdzenia 2.9(2). □

Twierdzenie 2.12.

Dziedzina z rozkładem jest dziedziną z jednoznacznością rozkładu wtedy i tylko wtedy, gdy każdy element nierozkładalny jest pierwszy.

Dowód.

Załóżmy najpierw, że R jest dziedziną z jednoznacznością rozkładu i ustalmy nierozkładalny element r dziedziny R. Przypuśćmy, że $r \mid s_1 \cdot s_2$ dla pewnych elementów s_1 i s_2 pierścienia R. Jeśli $s_1 = 0$ lub $s_2 = 0$, to $r \mid s_1$ lub $r \mid s_2$, odpowiednio. Podobnie, jeśli element s_1 jest odwracalny, to $s_1 \cdot s_2 \approx s_2$ na mocy Stwierdzenia 2.9(7). W szczególności, $s_1 \cdot s_2 \mid s_2$, więc $r \mid s_2$. Podobnie pokazujemy, że $r \mid s_1$, gdy element s_2 jest odwracalny.

Załóżmy zatem, że elementy s_1 i s_2 są niezerowe i nieodwracalne. W szczególności, $s_1 \cdot s_2 \neq 0$, gdyż R jest dziedziną. Ponieważ R jest dziedziną z rozkładem, więc istnieją elementy nierozkładalne $q_1, \ldots, q_m$ takie, że

$$s_1 = q_1 \cdots q_l \qquad \text{i} \qquad s_2 = q_{l+1} \cdots q_m$$

dla pewnych $1 \leq l < m$. Wiemy, że istnieje element t pierścienia R taki, że $r \cdot t = s_1 \cdot s_2$. Ponieważ $s_1 \cdot s_2 \neq 0$, więc $t \neq 0$. Jeśli element t jest odwracalny, to $r \cdot t \approx r$, więc element $r \cdot t$ jest nierozkładalny na mocy Stwierdzenia 2.10(2). To jest niemożliwe, gdyż

$$r \cdot t = q_1 \cdots q_m,$$

$m \geq 2$ i R jest dziedziną z jednoznacznością rozkładu. Zatem element t jest niezerowy i nieodwracalny, więc istnieją elementy nierozkładalne $p_1, \ldots, p_n$ takie, że $t = p_1 \cdots p_n$. Wtedy

$$r \cdot p_1 \cdots p_n = q_1 \cdots q_m.$$

Ponieważ R jest dziedziną z jednoznacznością rozkładu, więc istnieje i takie, że $r \approx q_i$. Jeśli $i \leq l$, to $r \mid s_1$, w przeciwnym wypadku $r \mid s_2$.

Załóżmy teraz, że w dziedzinie z rozkładem R każdy element nierozkładalny jest pierwszy. Aby pokazać, że R jest dziedziną z jednoznacznością rozkładu, ustalmy elementy nierozkładalne $r_1, \ldots, r_n, s_1, \ldots, s_m$ takie, że

$$r_1 \cdots r_n \approx s_1 \cdots s_m.$$

Bez straty ogólności możemy założyć, że $n \leq m$. Przez indukcję ze względu na n pokażemy, że $n = m$ oraz istnieje permutacja σ zbioru $\{1, \ldots, n\}$ taka, że $r_i \approx s_{\sigma(i)}$ dla każdego $i = 1, \ldots, n$.

Niech zatem najpierw $n = 0$. Wtedy $r_1 \cdots r_n = 1$. Gdyby $m > 0$, to $r_1 \mid 1$, a więc element s_1 byłby odwracalny na mocy Stwierdzenia 2.9(3), sprzeczność.

Niech teraz $n > 0$. Zauważmy, że $r_n \mid s_1 \cdots s_m$. Ponieważ element r_n jest nierozkładalny, a więc na mocy założenia również pierwszy, zatem istnieje $j \in \{1, \ldots, m\}$ takie, że $r_n \mid s_j$. Bez straty założenia możemy założyć, że $j = m$. Ponieważ element r_n nie jest odwracalny i element s_m jest nierozkładalny, więc $r_n \approx s_m$. Ze Stwierdzenia 2.9(7) wynika, że istnieją elementy odwracalne u i v takie, że $s_m = u \cdot r_n$ i

$$r_1 \cdots r_{n-1} \cdot r_n = s_1 \cdots s_{m-1} \cdot s_m \cdot v.$$

Wtedy

$$r_1 \cdots r_{n-1} \cdot r_n = s_1 \cdots s_{m-1} \cdot r_n \cdot u \cdot v.$$

więc

$$r_1 \cdots r_{n-1} = s_1 \cdots s_{m-1} \cdot u \cdot v$$

na mocy Stwierdzenia 2.4, zatem

$$r_1 \cdots r_{n-1} \approx s_1 \cdots s_{m-1}$$

na mocy Stwierdzenia 2.9(7). Z założenia indukcyjnego $n-1 = m-1$ oraz istnieje permutacja σ zbioru $\{1, \ldots, m-1\}$ taka, że $r_i \approx s_{\sigma(i)}$ dla każdego $i = 1, \ldots, n-1$, co kończy dowód. □

Stwierdzenie 2.13.

(1) Każdy element pierwszy jest nierozkładalny.

(2) Jeśli R jest dziedziną ideałów głównych, to każdy element nierozkładalny jest pierwszy.

Dowód.

(1) Przypuśćmy, że element r dziedziny R jest pierwszy oraz załóżmy, że $s \mid r$. Wtedy $r = s \cdot t$ dla pewnego elementu t dziedziny R (zauważmy, że $t \neq 0$, gdyż $r \neq 0$), a więc w szczególności $r \mid s \cdot t$. Stąd $r \mid s$ lub $r \mid t$. W pierwszym przypadku $r \approx s$, a w drugim $r \approx t$. Na mocy Stwierdzenie 2.9(7) to oznacza, że $r = u \cdot t$ dla pewnego elementu odwracalnego $u \in R$. Wtedy $s \cdot t = u \cdot t$, a więc, korzystając ze Stwierdzenia 2.4, otrzymujemy, że $s = u$ jest elementem odwracalny.

(2) Jeśli R jest dziedziną ideałów głównych, to, korzystając ze Stwierdzenia 2.10(1), otrzymujemy, że element r jest nierozkładalny wtedy i tylko wtedy, gdy $(r) \neq 0$ i ideał (r) jest maksymalny. Ponieważ każdy ideał maksymalny jest pierwszy na mocy Wniosku 2.7, więc teza wynika ze Stwierdzenia 2.11(1). □

Lemat 2.14.

Jeśli r_i, $i \in \mathbb{N}$, są elementami dziedziny ideałów głównych R takimi, że $r_{i+1} \mid r_i$ dla każdego $i \in \mathbb{N}$, to istnieje $n \in \mathbb{N}$ takie, że $r_{i+1} \approx r_i$ dla każdego $i \geq n$.

Dowód.

Dla każdego $i \in \mathbb{N}$ oznaczmy przez I_i ideał generowany przez element r_i. Z założeń oraz Stwierdzenia 2.9(1) wynika, że $I_i \subseteq I_{i+1}$ dla każdego $i \in \mathbb{N}$. Wykorzystując tę obserwację, łatwo pokazać, że zbiór $I := \bigcup_{i \in \mathbb{N}} I_i$ jest ideałem. Ponieważ R jest dziedziną ideałów głównych, więc istnieje element r dziedziny R taki, że $I = (r)$. Z definicji ideału I istnieje $n \in \mathbb{N}$ takie, że $r \in I_n$. Wtedy dla $i \geq n$ otrzymujemy, że $r \in I_i$, więc

$$I = (r) \subseteq I_i \subseteq I_{i+1} \subseteq I,$$

skąd $I_i = I_{i+1}$, a więc $r_i \approx r_{i+1}$ na mocy Stwierdzenia 2.9(2). □

Uwaga.

Kluczową rolę w dowodzie Lematu 2.14 odgrywała następująca własność: jeśli I_i, $i \in \mathbb{N}$, są ideałami pierścienia R takimi, że $I_i \subseteq I_{i+1}$ dla każdego $i \in \mathbb{N}$, to istnieje $n \in \mathbb{N}$ takie, że $I_i = I_{i+1}$ dla każdego $i \geq n$. Pierścienie posiadające tę własność są nazywane NOETHEROWSKIMI.

Stwierdzenie 2.15.

Każda dziedzina ideałów głównych jest dziedziną z rozkładem.

Dowód.

Niech R będzie dziedziną ideałów głównych oraz niech X będzie zbiorem niezerowych elementów r dziedziny R, które nie są odwracalne i dla których nie istnieją elementy nierozkładalne $r_1, \ldots, r_n$ takie, że $r = r_1 \cdots r_n$.

Zauważmy, że istnieje funkcja $\tau\colon X \to X$ taka, że $\tau(r) \mid r$ i $\tau(r) \not\approx r$ dla każdego elementu r zbioru X. Istotnie, ustalmy element r zbioru X. Wtedy element r jest niezerowy, nie jest odwracalny i nie jest nierozkładalny. Stąd istnieją niezerowe elementy s i t, które nie są odwracalne i $r = s \cdot t$. W szczególności, $s, t \mid r$ i $s, t \not\approx r$ (na mocy Stwierdzenia 2.9(7)). Ponadto, ponieważ $r \in X$, więc $s \in X$ lub $t \in X$. Jeśli $s \in X$, to definiujemy $\tau(r) := s$, w przeciwnym wypadku $\tau(r) := t$.

Musimy pokazać że $X = \varnothing$. Załóżmy przez sprzeczność, że $X \neq \varnothing$, i wybierzmy element $r \in X$. Definiujemy elementy r_i, $i \in \mathbb{N}$, ..., wzorem

$$r_i := \tau^i(r) \qquad (i \in \mathbb{N}).$$

Wtedy $r_{i+1} \mid r_i$ oraz $r_{i+1} \not\approx r_i$ dla każdego $i \in \mathbb{N}$, co jest sprzeczne z Lematem 2.14. □

Wniosek 2.16.

Każda dziedzina ideałów głównych jest dziedziną z jednoznacznością rozkładu.

Dowód.

Wynika natychmiast ze Stwierdzenia 2.15, Twierdzenia 2.12 oraz Stwierdzenia 2.13(2). □

2.3. Dziedziny Euklidesa

Definicja.

Dziedzinę R nazywamy DZIEDZINĄ EUKLIDESA, jeśli istnieje funkcja $\alpha\colon R \to \mathbb{N}$ taka, że jeśli s i t są elementami dziedziny R takimi, że $t \neq 0$, to istnieją elementy q i r dziedziny R takie, że $s = q \cdot t + r$ i $\alpha(r) < \alpha(t)$.

Przykład.

Pierścień $\mathbb{Z}$ jest dziedziną Euklidesa.

Twierdzenie 2.17.
Każda dziedzina Euklidesa jest dziedziną ideałów głównych.

Dowód.
Niech R wraz z funkcją $\alpha\colon R \to \mathbb{N}$ będzie dziedziną Euklidesa. Niech I będzie ideałem dziedziny Euklidesa R. Jeśli $I = \{0\}$, to $I = (0)$. Załóżmy zatem, że $I \neq \{0\}$, i wybierzmy element $t \in I \setminus \{0\}$ taki, że

$$\alpha(t) = \min\{\alpha(s) : s \in I \setminus \{0\}\}.$$

Pokażemy, że $(t) = I$. Oczywiście $(t) \subseteq I$. Dla dowodu inkluzji $I \subseteq (t)$ ustalmy element s ideału I. Z definicji dziedziny Euklidesa wynika, że istnieją elementy q i r dziedziny R takie, że $s = q \cdot t + r$ i $\alpha(r) < \alpha(t)$. Zauważmy, że $r = s - q \cdot t \in I$, więc z wyboru elementu t wynika, że $r = 0$. Stąd $s = q \cdot t \in (t)$. □

Wniosek 2.18.
Każda dziedzina Euklidesa jest dziedziną z jednoznacznością rozkładu.

Dowód.
Wynika natychmiast z Twierdzenia 2.17 i Wniosku 2.16. □

Twierdzenie 2.19 (Algorytm dzielenia dla wielomianów).
Niech F będzie ciałem. Jeśli f i g są wielomianami o współczynnikach ciele F oraz $g \neq 0$, to istnieją (jednoznacznie wyznaczone) wielomiany q i r takie, że $f = q \cdot g + r$ i $\deg r < \deg g$.

Dowód.
Pokażemy istnienie, dowód jednoznaczności zostawiamy jako ćwiczenie. Dowód będzie indukcyjny ze względu na $\deg f$. Jeśli $\deg f < \deg g$ (w szczególności, gdy $f = 0$), to $q := 0$ i $r := f$. Jeśli $n := \deg f \geq \deg g =: m$, to istnieje element λ ciała F taki, że wielomiany $\lambda \cdot X^{n-m} \cdot g$ i f mają ten sam współczynnik przy najwyższej potędze. Jeśli $f_0 := f - \lambda \cdot X^{n-m} \cdot g$, to $\deg f_0 < \deg f$, a więc z założenia indukcyjnego istnieją wielomiany q_0 i r takie, że $f_0 = q_0 \cdot g + r$ i $\deg r < \deg g$. Biorąc $q := \lambda \cdot X^{n-m} + q_0$, otrzymujemy tezę. □

Wniosek 2.20.
Jeśli F jest ciałem, to pierścień $F[X]$ jest dziedziną Euklidesa.

Dowód.
Korzystając z Twierdzenia 2.19, łatwo widać, że funkcja $\alpha\colon F[X] \to \mathbb{N}$ dana wzorem

$$\alpha(f) := 2^{\deg f} \qquad (f \in F[X]),$$

spełnia warunki definicji. □

Wniosek 2.21.
Jeśli F jest ciałem, to pierścień $F[X]$ jest dziedziną z jednoznacznością rozkładu.

Dowód.
Wynika natychmiast z Wniosków 2.20 i 2.18. □

Uwaga.
Można pokazać, że jeśli R jest dziedziną z jednoznacznością rozkładu, to pierścień $R[X]$ jest dziedziną z jednoznacznością rozkładu. W szczególności, jeśli n jest dodatnią liczbą całkowitą i F jest ciałem, to pierścień $F[X_1, \ldots, X_n]$ jest dziedziną z jednoznacznością rozkładu.

2.4. Największy wspólny dzielnik

Założenie.
Przez cały podrozdział R jest dziedziną całkowitości.

Definicja.
Niech r i s będą elementami dziedziny R. Element d dziedziny R nazywamy największym wspólnym dzielnikiem elementów r i s, jeśli spełnione są następujące warunki:

(1) $d \mid r$ i $d \mid s$;

(2) jeśli c jest elementem dziedziny R takim, że $c \mid r$ i $c \mid s$, to $c \mid d$.

Lemat 2.22.
Niech d będzie największym wspólnym dzielnikiem elementów r i s dziedziny R. Jeśli d' jest elementem dziedziny R, to d' jest największym wspólnym dzielnikiem elementów r i s wtedy i tylko wtedy, gdy $d' \approx d$.

Dowód.
Jeśli d' jest największym wspólnym dzielnikiem elementów r i s, to, korzystając z definicji największego wspólnego dzielnika, otrzymujemy łatwo, że $d \mid d'$ i $d' \mid d$, więc $d' \approx d$. Z drugiej strony, gdy $d' \approx d$, to $d' \mid d$, więc $d' \mid r$ i $d' \mid s$. Ponadto, jeśli $c \mid r$ i $c \mid s$, to $c \mid d$, a więc również $c \mid d'$, gdyż $d \mid d'$. □

Przykład.
Niech $R := \{a + b\imath\sqrt{3} : a, b \in \mathbb{Z}\}$. Wtedy nie istnieje największy wspólny dzielnik liczb $2 + 2\imath\sqrt{3}$ oraz 4.

Lemat 2.23.
Niech $p_1, \ldots, p_n$ będą elementami nierozkładalnymi dziedziny z jednoznacznością rozkładu R takimi, że $p_i \not\approx p_j$ dla $i \neq j$. Jeśli $l_1, \ldots, l_n, k_1, \ldots, k_n$ są

nieujemnymi liczbami całkowitymi, to

$$p_1^{l_1} \cdots p_n^{l_n} \mid p_1^{k_1} \cdots p_n^{k_n}$$

wtedy i tylko wtedy, gdy $l_i \leq k_i$ dla każdego i.

Dowód.
Ćwiczenie. □

Stwierdzenie 2.24.
Jeśli R jest dziedziną z jednoznacznością rozkładu, to dla dowolnych elementów r i s istnieje ich największy wspólny dzielnik.

Dowód.
Jeśli $r = 0$, to s jest największym wspólnym dzielnikiem elementów r i s. Podobnie, gdy r jest elementem odwracalnym, to r (lub 1) jest największym wspólnym dzielnikiem. Możemy zatem założyć, że elementy r i s są niezerowe i nie są odwracalne. Ponieważ R jest dziedziną z rozkładem, to istnieją elementy nierozkładalne $p_1, \ldots, p_n$, elementy odwracalne u i v oraz nieujemne liczby całkowite $l_1, \ldots, l_n, k_1, \ldots, k_n$ takie, że $p_i \not\approx p_j$ dla $i \neq j$,

$$r = up_1^{k_1} \cdots p_n^{k_n} \qquad \text{i} \qquad s = vp_1^{l_1} \cdots p_n^{l_n}.$$

Wtedy z Lematu 2.23 wynika, że element $d := p_1^{\min(k_1,l_1)} \cdots p_n^{\min(k_n,l_n)}$ jest największym wspólnym dzielnikiem elementów r i s. □

Uwaga.
W pierścieniu $\mathbb{Z}$ największy wspólny dzielnik jest wyznaczony z dokładnością do znaku. Zwykle wybiera się spośród możliwych liczb liczbę nieujemną. Podobnie, jeśli F jest ciałem, to największy wspólny dzielnik w pierścieniu $F[X]$ jest wyznaczony z dokładnością do niezerowego skalara. Z wyjątkiem sytuacji, gdy 0 jest największym wspólnym dzielnikiem, to jako największy wspólny dzielnik wybieramy wielomian, który przy najwyższej potędze ma współczynnik równy 1.

Stwierdzenie 2.25.
Jeśli R jest dziedziną z ideałów głównych, to dla dowolnych elementów r i s istnieją elementy x i y takie, że $x \cdot r + y \cdot s$ jest największym wspólnym dzielnikiem elementów r i s.

Dowód.
Łatwo sprawdzić, że zbiór $(r)+(s)$ jest ideałem dziedziny R. Ponieważ R jest dziedziną ideałów głównych, więc istnieje element d taki, że $(d) = (r) + (s)$. Wtedy d jest największym wspólnym dzielnikiem elementów r i s oraz ze Stwierdzenia 2.3 wynika, że istnieją elementy x i y takie, że $d = x \cdot r + y \cdot s$. □

Uwaga.

Jeśli R jest dziedziną Euklidesa, to największy wspólny dzielnik oraz elementy x i y, o których mowa w Stwierdzeniu 2.25, można znaleźć, korzystając z (rozszerzonego) algorytmu Euklidesa.

Definicja.

Niech r i s będą elementami dziedziny R. Element t dziedziny R nazywamy najmniejszą wspólną wielokrotnością elementów r i s, jeśli spełnione są następujące warunki:

(1) $r \mid t$ i $s \mid t$;

(2) jeśli t' jest elementem dziedziny R takim, że $r \mid t'$ i $s \mid t'$, to $t \mid t'$.

Lemat 2.26.

Niech t będzie najmniejszą wspólną wielokrotnością elementów r i s dziedziny R. Jeśli t' jest elementem dziedziny R, to t' jest najmniejszą wspólną wielokrotnością elementów r i s wtedy i tylko wtedy, gdy $t' \approx t$.

Dowód.

Ćwiczenie. □

Stwierdzenie 2.27.

Jeśli istnieje najmniejsza wspólna wielokrotność t elementów r i s dziedziny R, to istnieje najmniejszy wspólny dzielnik d elementów r i s oraz $t \cdot d \approx r \cdot s$.

Dowód.

Jeśli $r = 0$, to teza jest oczywista ($t = 0$ i $d = s$). Podobnie jest, gdy $s = 0$. Załóżmy zatem, że $r \neq 0 \neq s$.

Ponieważ $r \cdot s$ jest wspólną wielokrotnością elementów r i s, więc $t \mid r \cdot s$. W szczególności, $t \neq 0$ (gdyż $r \cdot s \neq 0$) oraz istnieje element d taki, że $t \cdot d = r \cdot s$. Pokażemy, że element d jest największym wspólnym dzielnikiem elementów r i s.

Najpierw pokażemy, że element d dzieli elementy r i s. Ponieważ $r \mid t$, więc istnieje element s' taki, że $r \cdot s' = t$. Wtedy $r \cdot s' \cdot d = r \cdot s$, więc $s = s' \cdot d$ na mocy Stwierdzenia 2.4. Zatem $d \mid s$. Podobnie pokazujemy, że $d \mid r$.

Pokażemy teraz, że jeśli $c \mid r$ i $c \mid s$, to $c \mid d$. Nasze założenia implikują, że istnieją elementy s'' i r'' takie, że $r = c \cdot r''$ i $s = c \cdot s''$. Wtedy element $c \cdot r'' \cdot s''$ jest wspólną wielokrotnością elementów r i s, a więc $t \mid c \cdot r'' \cdot s''$, tzn. istnieje element d' taki, że $t \cdot d' = c \cdot r'' \cdot s''$. Zauważmy, że

$$t \cdot d = r \cdot s = c^2 \cdot r'' \cdot s'' = c \cdot t \cdot d',$$

skąd $d = c \cdot d'$, a więc $c \mid d$. □

Przykład.

Niech $R := \{a+bi\sqrt{3} : a, b \in \mathbb{Z}\}$. Wtedy istnieje największy wspólny dzielnik elementów 2 i $1+i\sqrt{3}$ (1), ale nie istnieje ich najmniejsza wspólna wielokrotność.

Stwierdzenie 2.28.

Jeśli dla dowolnych dwóch elementów dziedziny R istnieje ich największy wspólny dzielnik, to dla dowolnych dwóch elementów dziedziny R istnieje ich najmniejsza wspólna wielokrotność.

Dowód.

Ustalmy elementy r i s dziedziny R. Jeśli $r = 0$ lub $s = 0$, to teza jest oczywista – najmniejszą wspólną wielokrotnością jest 0. Załóżm zatem, że $r \neq 0 \neq s$.

Niech d będzie ich największy wspólnym dzielnikiem. Wtedy $r = d \cdot r'$ i $s = d \cdot s'$ dla pewnych elementów r' i s' dziedziny R. Zauważmy, że największym wspólnym dzielnikiem elementów r' i s' jest 1.

Pokażemy, że $t := d \cdot r' \cdot s'$ jest najmniejszą wspólną wielokrotnością elementów r i s. Oczywiście $r \mid t$ i $s \mid t$. Przypuśćmy zatem, że $r \mid t'$ i $s \mid t'$ dla pewnego elementu t' dziedziny R. Niech d' będzie największym wspólnym dzielnikiem elementów t i t'. Wtedy istnieje element c taki, że $t = d' \cdot c$. Ponadto $r \mid d'$, ponieważ $r \mid t$ i $r \mid t$, więc istnieje element s'' taki, że $d = r \cdot s''$. Podobnie istnieje element r'' takie, że $d' = s \cdot r''$. Wtedy

$$r \cdot s' = d \cdot r' \cdot s' = t = d' \cdot c = r \cdot s'' \cdot c,$$

więc $s' = s'' \cdot c$ mocy Stwierdzenia 2.4, tzn. $c \mid s'$. Podobnie, $c \mid r'$, więc c jest elementem odwracalnym. Stąd t jest największym wspólnym dzielnikiem elementów t i t' (na mocy Lematu 2.22 i Stwierdzenia 2.9(7)), a więc w szczególności $t \mid t'$. □

Wniosek 2.29.

Jeśli R jest dziedziną z jednoznacznością rozkładu, to dla dowolnych dwóch elementów dziedziny R istnieje ich najmniejsza wspólna wielokrotność.

Dowód.

Wynika natychmiast ze Stwierdzeń 2.28 oraz 2.24. □

3. Klasyfikacja skończonych grup abelowych

Oznaczenie.

Przez cały rozdział wszystkie rozważane grupy są grupami abelowymi. Działanie w rozważanych grupach oznaczamy symbolem $+$.

Uwaga.

Celem tego rozdziału jest udowodnienie, że jeśli G jest skończoną grupą abelową, to istnieją jednoznacznie wyznaczone liczby pierwsze $p_1, \ldots, p_k$, oraz dodatnie liczby całkowite $n_{i,j}$, $i \in \{1, \ldots, k\}$, $j \in \{1, \ldots, l_i\}$, takie, że

$$G \simeq \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{l_i} \mathbb{Z}_{p_i^{n_{i,j}}},$$

$p_1 < p_2 < \cdots < p_k$ oraz

$$n_{i,1} \leq n_{i,2} \leq \cdots \leq n_{i,l_i},$$

dla każdego i.

3.1. Sumy proste

Definicja.

Jeśli G i H są grupami, to sumą prostą grup G i H nazywamy zbiór $G \times H$ wraz z działaniem po współrzędnych, tzn. jeśli $g_1, g_2 \in G$ i $h_1, h_2 \in H$, to

$$(g_1, h_1) + (g_2, h_2) := (g_1 + g_2, h_1 + h_2).$$

Sumę prostą grup G i H oznaczamy symbolem $G \oplus H$.

Uwaga.

Można pokazać, że suma prosta dwóch grup (abelowych) jest grupą (abelową). Jeśli G, H i K są grupami, to

$$G \oplus H \simeq H \oplus G \qquad \text{i} \qquad (G \oplus H) \oplus K \simeq G \oplus (H \oplus K).$$

W związku w powyższym, jeśli $G_1, \ldots, G_n$ są grupami, to definicja

$$\bigoplus_{i=1}^{n} G_i := G_1 \oplus \cdots \oplus G_n$$

jest poprawna.

Lemat 3.1.

Niech $G_1, \ldots, G_m$ i $H_1, \ldots, H_n$ będą grupami. Jeśli $\varphi_{j,i} \colon G_i \to H_j$, $i \in$

$\{1,\dots,m\}$, $j \in \{1,\dots,n\}$, są homomorfizmami, to funkcja $\varphi\colon G_1 \oplus \cdots \oplus G_m \to H_1 \oplus \cdots \oplus H_n$ dana wzorem

$$\varphi(g_1,\dots,g_m) := (\varphi_{1,1}(g_1)+\cdots+\varphi_{1,m}(g_m),\dots,\varphi_{n,1}(g_1)+\cdots+\varphi_{n,m}(g_m)) \qquad (g_1 \in G_1,\ \dots,\ g_m \in G_m),$$

jest homomorfizmem grup.

Dowód.
Ćwiczenie. □

Definicja.
Jeśli G i H są grupami oraz istnieje grupa H' taka, że $H \oplus H' \simeq G$, to mówimy, że grupa H jest składnikiem prostym grupy G.

Uwaga.
Jeśli H i H' są grupami, to istnieją homomorfizmy $\mu\colon H \to H \oplus H'$ i $\pi\colon H \oplus H' \to H$ takie, że $\pi \circ \mu = \mathrm{Id}_H$.

Stwierdzenie 3.2.
Niech G i H będą grupami. Jeśli istnieją homomorfizmy $\mu\colon H \to G$ oraz $\pi\colon G \to H$ takie, że $\pi \circ \mu = \mathrm{Id}_H$, to

$$G \simeq H \oplus \operatorname{Ker}\pi.$$

Dowód.
Definiujemy homomorfizm $\varphi\colon H \oplus \operatorname{Ker}\pi$ wzorem

$$\varphi(h,g) := \mu(h) + g \qquad (h \in H,\ g \in \operatorname{Ker}\pi).$$

Pokażemy, że φ jest izomorfizmem. Korzystając ze Stwierdzenia 1.6, wystarczy pokazać, że φ jest monomorfizmem i epimorfizmem. Aby pokazać, że φ jest monomorfizmem, ustalmy $h \in H$ i $g \in \operatorname{Ker}\pi$ takie, że $\mu(h) + g = 0$. Wtedy

$$0 = \pi(0) = \pi(\mu(h)) + \pi(g) = h + 0 = h.$$

Ponadto, $g = -\mu(h) = -\mu(0) = -0 = 0$. Zatem $\operatorname{Ker}\varphi = \{(0,0)\}$ i teza wynika z Stwierdzenia 1.12(1).

Aby pokazać, że φ jest epimorfizmem, ustalmy $g \in G$. Niech

$$h := \pi(g) \qquad \text{i} \qquad g' := g - \mu(\pi(g)).$$

Wtedy

$$\pi(g') = \pi(g) - \pi(\mu(\pi(g)) = \pi(g) - \pi(g) = 0,$$

więc $(h, g') \in H \oplus \operatorname{Ker} \pi$. Ponadto,

$$\varphi(h, g') = \mu(h) + g' = \mu(\pi(g)) + g - \mu(\pi(g)) = g,$$

co kończy dowód. □

Wniosek 3.3.
Jeśli H jest podgrupą grupy G taką, że istnieje homomorfizm $\pi\colon G \to H$ taki, że $\pi(h) = h$ dla każdego elementu h podgrupy H, to

$$G \simeq H \oplus \operatorname{Ker} \pi.$$

Dowód.
Wynika natychmiast ze Stwierdzenia 3.2 (jako homomorfizm $\mu\colon H \to G$ bierzemy naturalne włożenie). □

Wniosek 3.4.
Jeśli H jest podgrupą grupy G taką, że istnieje homomorfizm $\mu\colon G/H \to G$ taki, że $\pi \circ \mu = \mathrm{Id}_{G/H}$, gdzie $\pi\colon G \to G/H$ jest naturalnym rzutowaniem, to

$$G \simeq H \oplus G/H.$$

Dowód.
Zauważmy, że $\operatorname{Ker} \pi = H$, więc teza wynika natychmiast ze Stwierdzenia 3.2. □

3.2. Grupy cykliczne

Definicja.
Grupę G nazywamy cykliczną, jeśli istnieje element g grupy G taki, że $G = \langle g \rangle$.

Element g grupy G taki, że $\langle g \rangle = G$, nazywamy generatorem grupy G.

Lemat 3.5.
Niech $G = \langle X \rangle$. Jeśli $\varphi, \psi\colon G \to H$ są homomorfizmami takimi, że $\varphi(g) = \psi(g)$ dla każdego elementu g zbioru X, to $\varphi = \psi$.

Dowód.
Niech G' będzie zbiorem elementów g grupy G takich, że $\varphi(g) = \psi(g)$. Łatwo sprawdzić, że G' jest podgrupą grupy G. Ponadto z założenia $X \subseteq G'$, więc $G = \langle X \rangle \subseteq G'$. Oczywiście $G' \subseteq G$. □

Stwierdzenie 3.6.
Niech g będzie generatorem skończonej grupy cyklicznej G i $n := \operatorname{ord}(g)$. Jeśli h jest elementem grupy H takim, że $\operatorname{ord}(h) \mid n$, to istnieje jedyny homomorfizm $\varphi\colon G \to H$ taki, że $\varphi(g) = h$.

Dowód.

Jedność homomorfizmu φ wynika natychmiast Lematu 3.5. Aby pokazać istnienie przypomnijmy, że na mocy Stwierdzenia 1.32

$$G = \{kg : k \in \{0, 1, \ldots, n-1\}\}.$$

Definiujemy funkcję $\varphi\colon G \to H$ wzorem

$$\varphi(kg) := kh \qquad (k \in \{0, 1, \ldots, n-1\}).$$

Aby pokazać, że φ jest homomorfizmem, ustalmy $k, l \in \{0, 1, \ldots, n-1\}$. Wtedy $kg + lg = ((k+l) \bmod n)g$, więc

$$\varphi(kg + lg) = ((k+l) \bmod n)h.$$

Z drugiej strony,

$$\varphi(kg) + \varphi(lg) = (k+l)h.$$

Stąd

$$(\varphi(kg) + \varphi(lg)) - \varphi(kg + lg) = (((k+l) \operatorname{div} n)n)h = 0,$$

gdyż $\operatorname{ord}(h) \mid n$. Innymi słowy,

$$\varphi(kg + lg) = \varphi(kg) + \varphi(lg). \qquad \square$$

Stwierdzenie 3.7.

Jeśli G jest skończoną grupą cykliczną i $n := |G|$, to $G \simeq \mathbb{Z}_n$.

Dowód.

Ustalmy generator g grupy G. Ze Stwierdzenia 3.6 wiemy, że istnieją homomorfizmy $\varphi\colon G \to \mathbb{Z}_n$ i $\psi\colon \mathbb{Z}_n \to G$ takie, że $\varphi(g) = 1$ i $\psi(1) = g$. Wtedy $\varphi(\psi(1)) = 1$ i $\psi(\varphi(g)) = g$, więc $\varphi \circ \psi = \mathrm{Id}_{\mathbb{Z}_n}$ i $\psi \circ \varphi = \mathrm{Id}_G$ na mocy Lematu 3.5, co kończy dowód. $\square$

Wniosek 3.8.

Niech g jest elementem grupy G.

(1) Jeśli $\operatorname{ord}(g) < \infty$ i $kg = 0$ dla pewnej liczby całkowitej k, to $\operatorname{ord}(g) \mid k$.

(2) Jeśli $kg = 0$ dla pewnej niezerowej liczby całkowitej k, to $\operatorname{ord}(g) < \infty$ (a więc w szczególności $\operatorname{ord}(g) \mid k$).

Dowód.

Dla dowodu pierwszej części niech $H := \langle g \rangle$ i $n := \operatorname{ord}(g)$. Ze Stwierdzenia 3.6 wiemy, że istnieje homomorfizm $\varphi\colon H \to \mathbb{Z}_n$ taki, że $\varphi(g) = 1$. Jeśli $kg = 0$, to $k \cdot 1$ jest zerem w grupie $\mathbb{Z}_n$, więc $n \mid k$.

Dla dowodu drugiej części zauważmy, że jeśli $kg = 0$, to $|k|g = 0$. Zatem jeśli $k \neq 0$, to zbiór $\{m \in \mathbb{N}_+ : mg = 1\}$ jest niepusty, więc $\operatorname{ord}(g) < \infty$ na mocy Stwierdzenia 1.32. $\square$

3.3. Istnienie

Lemat 3.9.
Jeśli $\varphi\colon G \to H$ jest epimorfizmem grup, to

$$\sup\{\mathrm{ord}(g) : g \in G\} \geq \sup\{\mathrm{ord}(h) : h \in H\}.$$

Dowód.
Ustalmy element $h \in H$. Ponieważ φ jest epimorfizmem, więc istnieje element g grupy G taki, że $\varphi(g) = h$. Jeśli $\mathrm{ord}(g) = \infty$, to $\mathrm{ord}(g) \geq \mathrm{ord}(h)$. W przeciwnym wypadku

$$\mathrm{ord}(g)h = \mathrm{ord}(g)\varphi(g) = \varphi(\mathrm{ord}(g)g) = \varphi(0) = 0,$$

więc $\mathrm{ord}(h) \leq \mathrm{ord}(g)$ na mocy Stwierdzenia 1.32. Z dowolności elementu h wynika teza. □

Stwierdzenie 3.10.
Niech G będzie grupą (abelową), której rząd jest potęgą liczby pierwszej p. Wtedy istnieją dodatnie liczby całkowite $n_1, \ldots, n_l$ takie, że

$$G \simeq \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_l}}.$$

Dowód.
Dowód będzie indukcyjny ze względu na $|G|$. Gdy $|G| = 1$, to teza jest oczywista (jeśli przyjmiemy, że pusta suma prosta jest grupą trywialną). Jeśli $|G| > 1$, to wybierzmy element g_0 taki, że

$$\mathrm{ord}(g_0) = \max\{\mathrm{ord}(g) : g \in G\}.$$

Z Wniosku 1.31 wiemy, że $\mathrm{ord}(g_0) \mid |G|$. W szczególności, $\mathrm{ord}(g_0) = p^{n_0}$ dla pewnej dodatniej liczby całkowitej n_0. Niech $H := \langle g_0 \rangle$. Wtedy $H \simeq \mathbb{Z}_{p^{n_0}}$ na mocy Stwierdzenia 3.7. Z Twierdzenia 1.30 $|G/H| = |G|/|H|$. Zatem $|G/H|$ jest potęgą liczby p i $|G/H| < |G|$. Z założenia indukcyjnego istnieją dodatnie liczby całkowite $n_1, \ldots, n_l$ takie, że

$$G/H \simeq \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_l}}.$$

Powyższy izomorfizm będziemy traktować jako utożsamienie. Dla zakończenia dowodu wystarczy pokazać, że $G \simeq H \oplus G/H$.

Ustalmy $i \in \{1, \ldots, l\}$ i wybierzmy element $g_i' \in G$ taki, że $g_i' + H = e_i$, gdzie $e_i := (0, \ldots, 0, 1, 0, \ldots, 0)$, przy czym 1 jest na i-tym miejscu. Zauważmy, że $\mathrm{ord}(e_i) = p^{n_i}$, więc $p^{n_i} = \mathrm{ord}(e_i) \leq \mathrm{ord}(g_0) = p^{n_0}$ na mocy Lematu 3.9. Ponieważ $p^{n_i}e_i = (0, \ldots, 0)$, więc $p^{n_i}g_i' \in H$, skąd $p^{n_i}g_i' = k_i g_0$ dla pewnego

$k_i \in \mathbb{Z}$. Z Wniosku 1.31 wiemy, że $\operatorname{ord}(g_i')$ jest potęgą liczby p. Ponadto z wyboru elementu g_0 mamy, że $\operatorname{ord}(g_i') \leq \operatorname{ord}(g_0)$. Stąd $\operatorname{ord}(g) \mid p^{n_0}$, więc $p^{n_0} g_i' = 0$. Stąd $p^{n_0-n_i} k_i g_0 = 0$, więc $p^{n_0} \mid p^{n_0-n_i} k_i$ na mocy Wniosku 3.8. W konsekwencji istnieje liczba całkowita k_i' taka, że $k_i = p^{n_i} k_i'$. Niech $g_i := g_i' - k_i' g_0$. Wtedy $g_i + H = g_i' + H = e_i$ oraz

$$p^{n_i} g_i = p^{n_i} g_i' - p^{n_i} k_i' g_0 = k_i g_0 - k_i g_0 = 0.$$

W szczególności, $\operatorname{ord}(g_i) \mid p^{n_i} = \operatorname{ord}(e_i)$.

Z powyższych rozważań, Stwierdzenia 3.6 oraz Lematu 3.1 wynika, że istnieje homomorfizm $\mu\colon G/H \to G$ taki, że $\mu(e_i) = g_i$ dla każdego $i \in \{1, \ldots, n\}$. Wtedy

$$\pi(\mu(e_i)) = \pi(g_i) = g_i + H = e_i$$

dla każdego $i \in \{1, \ldots, n\}$, więc $\pi \circ \mu = \mathrm{Id}_{G/H}$ na mocy Lematu 3.5. Stąd teza wynika z Wniosku 3.4. □

Lemat 3.11.

Niech p będzie liczbą pierwszą. Jeśli G jest skończoną grupą abelową taką, że $\operatorname{ord}(g)$ jest potęgą liczby p dla każdego elementu g grupy G, to rząd grupy G jest również potęgą liczby p.

Uwaga.

Teza powyższego lematu zachodzi również bez założenia abelowości grupy G (patrz Wniosek 4.10).

Dowód.

Tezę udowodnimy przez indukcję ze względu na rząd grupy G. Jeśli $|G| = 1$, to teza jest oczywista. Załóżmy zatem, że $|G| > 1$ i wybierzmy element h grupy G różny od 0. Niech H będzie podgrupą grupy G generowaną przez element h. Wtedy $|H| = \operatorname{ord}(h) = p^n$ dla pewnej dodatniej liczby całkowitej n. Ponadto, jeśli $g \in G$, to $\operatorname{ord}(g) \cdot (g + H) = H$, więc $\operatorname{ord}(g + H) \mid \operatorname{ord}(g)$ na mocy Wniosku 3.8, zatem rząd każdego elementu grupy G/H jest potęgą liczby p. Ponieważ $|G/H| < |G|$, więc na mocy założenia indukcyjnego istnieje dodatnia liczba całkowita m taka, że $|G/H| = p^m$. Z Twierdzenia 1.30 otrzymujemy zatem, że

$$|G| = |H| \cdot |G/H| = p^n \cdot p^m = p^{n+m}.$$ □

Stwierdzenie 3.12.

Jeśli G jest skończoną grupą abelową, to istnieją grupy $G_1, \ldots, G_n$ takie, że dla każdego i rząd grupy G_i jest potęgą liczby pierwszej oraz

$$G \simeq G_1 \oplus \cdots \oplus G_n.$$

Dowód.

Niech $p_1, \ldots, p_n$ będą wszystkimi parami różnymi liczbami pierwszymi dzielącymi rząd grupy G. Istnieją dodatnie liczby całkowite $k_1, \ldots, k_n$ takie, że

$$|G| = p_1^{k_1} \cdots p_n^{k_n}.$$

Dla każdego $i \in \{1, \ldots, n\}$ niech G_i będzie zbiorem elementów g grupy G takich, że $p_i^{k_i} g = 0$. Ponieważ grupa G jest abelowa, więc łatwo można pokazać, że zbiory $G_1, \ldots, G_n$ są podgrupami grupy G. Ponadto, z Wniosku 3.8 i Lematu 3.11 wynika, że dla każdego i rząd grupy G_i jest potęgą liczby p_i. Pokażemy, że

$$G \simeq G_1 \oplus \cdots \oplus G_n.$$

Dokładniej, pokażemy, że homomorfizm $\varphi\colon G_1 \oplus \cdots \oplus G_n \to G$ dany wzorem

$$\varphi(g_1, \ldots, g_n) := g_1 + \cdots + g_n \qquad (g_1 \in G_1,\ \ldots,\ g_n \in G_n),$$

jest izomorfizmem.

Pokażemy najpierw, że homomorfizm φ jest monomorfizmem. Przypuśćmy zatem, że

$$g_1 + \cdots + g_n = 0$$

dla pewnych elementów $g_1 \in G_1, \ldots, g_n \in G_n$. Ustalmy $i \in \{1, \ldots, n\}$. Wiemy, że istnieją liczby całkowite m i l takie, że

$$m p_i^{k_i} + l p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_n^{k_n} = 1.$$

Wtedy

$$\begin{aligned} g_i &= 1 \cdot g_i = (m p_i^{k_i} + l p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_n^{k_n}) \cdot g_i \\ &= m p_i^{k_i} g_i \\ &\qquad - l p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_n^{k_n} (g_1 + \cdots + g_{i-1} + g_{i+1} + \cdots + g_n) \\ &= 0 + 0 = 0. \end{aligned}$$

Pokażemy teraz, że φ jest epimorfizmem. Niech zatem $g \in G$. Ponieważ liczby $\frac{|G|}{p_i^{k_i}} = p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_n^{k_n}$, $i = 1, \ldots, n$, są względnie pierwsze, więc istnieją liczby całkowite $m_1, \ldots, m_n$ takie, że

$$m_1 \frac{|G|}{p_1^{k_1}} + \cdots + m_n \frac{|G|}{p_n^{k_n}} = 1.$$

Niech

$$g_i := m_i \frac{|G|}{p_i^{k_i}}, \qquad (i \in \{1, \ldots, n\}).$$

Wtedy dla każdego $i \in \{1, \ldots, n\}$ mamy

$$p_i^{k_i} g_i = m_i |G| g_i = m_i \cdot 0 = 0,$$

więc $g_i \in G_i$. Ponadto

$$g = g_1 + \cdots + g_n = \varphi(g_1, \ldots, g_n),$$

co kończy dowód. □

Wniosek 3.13.

Jeśli G jest skończoną grupą abelową, to istnieją parami różne liczby pierwsze $p_1, \ldots, p_n$ oraz dodatnie liczby całkowite n_{ij}, $i = 1, \ldots, n$, $j = 1, \ldots, l_i$, takie, że

$$G \simeq \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{l_i} \mathbb{Z}_{p^{n_{ij}}}.$$

Dowód.

Wynika natychmiast ze Stwierdzeń 3.12 i 3.10. □

3.4. Jednoznaczność

Oznaczenie.

Jeśli G jest grupą abelową oraz m jest liczbą całkowitą, to definiujemy zbiór $0 :_G m$ wzorem

$$0 :_m G := \{g \in G : m \cdot g = 0\}.$$

Zauważmy, że zbiór $0 :_m G$ jest podgrupą grupy G.

Lemat 3.14.

Niech $\varphi \colon G \to H$ będzie izomorfizmem grup abelowych. Jeśli m jest liczbą całkowitą,

$$\varphi(0 :_G m) = 0 :_H m,$$

a więc w szczególności $0 :_G m \simeq 0 :_H m$.

Dowód.

Łatwo widać, że $\varphi(0 :_G m) \subseteq 0 :_H m$. Podobnie, $\varphi^{-1}(0 :_H m) \subseteq 0 :_G m$. Stąd

$$0 :_H m = \varphi(\varphi^{-1}(0 :_H m)) \subseteq \varphi(0 :_G m),$$

co kończy dowód. □

Oznaczenie.

Jeśli G jest grupą abelową oraz m jest liczbą całkowitą, to definiujemy zbiór mG wzorem

$$mG := \{mg : g \in G\}.$$

Zauważmy, że zbiór mG jest podgrupą grupy G.

Lemat 3.15.

Niech $\varphi\colon G \to H$ będzie izomorfizmem skończonych grup abelowych. Jeśli m jest liczbą całkowitą, to $\varphi(mG) = mH$, a więc w szczególności $mG \simeq mH$.

Dowód.

Ćwiczenie (analogicznie jak dowód Lematu 3.14). □

Lemat 3.16.

Niech p będzie liczbą pierwszą. Niech $n_1, \ldots, n_l$ będą dodatnimi liczbami całkowitymi. Jeśli

$$G = \bigoplus_{i=1}^{l} \mathbb{Z}_{p^{n_i}},$$

to

$$|p^m G| = \prod_{i=1}^{l} |p^{\max(0,n_i-m)}|$$

dla każdej nieujemnej liczby całkowitej m.

Dowód.

Wystarczy zauważyć, że jeśli n jest dodatnią liczbą całkowitą, to $|p^m\mathbb{Z}_{p^n}| = p^{\max(0,n-m)}$. □

Stwierdzenie 3.17.

Niech $p_1, \ldots, p_n$ będą liczbami pierwszymi takimi, że

$$p_1 < p_2 < \cdots < p_n.$$

Dodatkowo, dla każdego $i = 1, \ldots, n$, niech $n_{i,1}, \ldots, n_{i,l_i}$ i $m_{i,1}, \ldots, m_{i,k_i}$ będą dodatnimi liczbami całkowitymi takimi, że

$$n_{i,1} \leq n_{i,2} \leq \cdots \leq n_{i,l_i} \qquad \text{i} \qquad m_{i,1} \leq m_{i,2} \leq \cdots \leq m_{i,k_i}.$$

Jeśli

$$\bigoplus_{i=1}^{n} \bigoplus_{j=1}^{l_i} \mathbb{Z}_{p_i^{n_{i,j}}} \simeq \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{k_i} \mathbb{Z}_{p_i^{m_{i,j}}},$$

to $l_1 = k_1, \ldots, l_n = k_n$ oraz $n_{i,j} = m_{i,j}$ dla wszystkich $i = 1, \ldots, n$, $j = 1, \ldots, l_i$.

Dowód.

Niech

$$G := \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{l_i} \mathbb{Z}_{p_i^{n_{i,j}}} \qquad \text{i} \qquad H := \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{k_i} \mathbb{Z}_{p_i^{m_{i,j}}}.$$

Ustalmy izomorfizm $\varphi\colon G \to H$. Dla każdego $i = 1, \ldots, n$ definiujemy

$$q_i := p_i^{\max(n_{i,l_i}, m_{i,k_i})},$$

gdzie $n_{i,l_i} := 0$, gdy $l_i = 0$, $m_{i,k_i} := 0$, gdy $k_i = 0$, oraz

$$G_i := 0 :_G q_i \qquad \text{i} \qquad H_i := 0 :_H q_i.$$

Wtedy

$$G_i \simeq \bigoplus_{j=1}^{l_i} \mathbb{Z}_{p_i^{n_{i,j}}} \qquad \text{i} \qquad H_i \simeq \bigoplus_{j=1}^{k_i} \mathbb{Z}_{p_i^{m_{i,j}}}.$$

Z Lematu 3.14 wynika, że

$$\bigoplus_{j=1}^{l_i} \mathbb{Z}_{p_i^{n_{i,j}}} \simeq \bigoplus_{j=1}^{k_i} \mathbb{Z}_{p_i^{m_{i,j}}}.$$

Stosując teraz Lemat 3.16 dla $m = \max(n_{i,l_i}, m_{i,k_i}) - 1, \ldots, 0$, otrzymujemy tezę. □

Twierdzenie 3.18.

Jeśli G jest skończoną grupą abelową, to istnieją jednoznacznie wyznaczone: nieujemna liczba całkowita n, liczby pierwsze $p_1, \ldots, p_n$, dodatnie liczby całkowite $l_1, \ldots, l_n$, oraz dodatnie liczby całkowite $n_{i,j}$, $i = 1, \ldots, n$, $j = 1, \ldots, l_i$, takie, że

$$G \simeq \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{l_i} \mathbb{Z}_{p_i^{n_{i,j}}}$$

oraz $p_1 < \cdots < p_n$ i, dla każdego $i = 1, \ldots, n$,

$$n_{i,1} \leq n_{i,2} \leq \cdots \leq n_{i,l_i}.$$

Dowód.

Istnienie wynika z Wniosku 3.13, zaś jednoznaczność ze Stwierdzenia 3.17. □

4. Działania grupa na zbiorach i twierdzenia Sylowa

4.1. Działania grup na zbiorach

Definicja.

Działaniem grupy G na zbiorze X nazywamy każdą funkcję $\delta\colon G\times X \to X$, $(g,x)\mapsto g*x$, taką, że

$$1*x = x \qquad \text{i} \qquad (gh)*x = g*(h*x)$$

dla dowolnych $g,h\in G$ 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

$$\sigma * x := \sigma(x) \qquad (\sigma\in S_X,\ x\in X).$$

Powyższy wzór zadaje też działanie dowolnej podgrupy grupy S_X

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

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

Powyższe działanie grupy H nazywamy działaniem przez lewe przesunięcia.

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

$$h*g := hgh^{-1} \qquad (h\in H,\ g\in G).$$

Działanie powyższe nazywamy działaniem przez sprzężenia.

Stwierdzenie 4.1.

(1) Jeśli $\delta : G\times X\to X$ jest działaniem grupy G na zbiorze X, to funkcja $\varphi_\delta\colon G\to S_X$ dana wzorem

$$(\varphi_\delta(g))(x) := \delta(g,x) \qquad (g\in G,\ x\in X),$$

jest homomorfizmem.

(2) Jeśli X jest zbiorem oraz $\varphi : G\to S_X$ jest homomorfizmem grup, to funkcja $\delta_\varphi\colon G\times X\to X$ dana wzorem

$$\delta_\varphi(g,x) := (\varphi(g))(x) \qquad (g\in G,\ x\in X),$$

jest działaniem grupy G na zbiorze X.

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

(4) Jeśli X jest zbiorem oraz $\varphi\colon G \to S_X$ jest homomorfizmem grup, to $\varphi_{\delta_\varphi} = \varphi$.

Dowód.
Ćwiczenie.

Wniosek 4.2 (Cayley).
Jeśli G jest grupą, to istnieje monomorfizm grup $G \to S_G$.

Dowód.
Niech $\delta\colon G \times G \to G$ będzie działaniem grupy G na zbiorze G przez lewe przesunięcia. Wtedy $\varphi_\delta\colon G \to S_G$ jest homomorfizmem grup. Musimy sprawdzić, że $\operatorname{Ker}\varphi_\delta = \{1\}$. Zauważmy, że $\varphi_\delta(g) = \mathrm{Id}_G$ wtedy i tylko wtedy, gdy $gh = h$ dla dowolnego elementu h grupy G. W szczególności $a = a \cdot 1 = 1$, co kończy dowód. □

Stwierdzenie 4.3.
Jeśli δ jest działaniem grupy G na grupie G przez sprzężenia, to $\operatorname{Im}\varphi_\delta \subseteq \operatorname{Aut}(G)$.

Dowód.
Należy sprawdzić, że dla każdego elementu g grupy G funkcja $\varphi_g := \varphi_\delta(g)$ jest homomorfizmem grupy G, co wynika natychmiast z bezpośrednich rachunków. □

Definicja.
Automorfizmem wewnętrznym grupy G nazywamy każdy automorfizm postaci $\varphi_\delta(g)$, gdzie g jest elementem grupy G, zaś δ jest działaniem grupy G na grupie G przez sprzężenia. Zbiór wszystkich automorfizmów wewnętrznych grupy G tworzy grupę (gdyż jest równy $\operatorname{Im}\varphi_\delta$), którą nazywamy grupą automorfizmów wewnętrznych grupy G i oznaczamy $\operatorname{Inn}(G)$.

Definicja.
Centrum grupy G nazywamy zbiór wszystkich elementów g grupy G takich, że $gh = hg$ dla dowolnego elementu h grupy G. Centrum grupy G oznaczamy $C(G)$.

Przykłady.

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

(2) Jeśli F jest ciałem oraz n jest dodatnią liczbą całkowitą, to $C(\mathrm{GL}_n(F))$ składa się z wszystkich macierzy postaci $\lambda\,\mathrm{Id}_n$, gdzie $\lambda \in F^\times$.

Stwierdzenie 4.4.

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

Dowód.

Cześć pierwszą łatwo sprawdzić bezpośrednim rachunkiem, natomiast druga wynika ze Stwierdzenia 1.25 oraz Pierwszego Twierdzenia o Izomorfizmie (Twierdzenie 1.34). □

Uwaga.

Grupa $C(G)$ jest zawsze abelowa.

Oznaczenie.

Jeśli g_1 i g_2 są elementami grupy G oraz X podzbiorem grupy G, to definiujemy zbiór g_1Xg_2 wzorem

$$g_1Xg_2 := \{g_1 \cdot hg_2 : h \in X\}.$$

Wniosek 4.5.

Jeśli H jest podgrupą grupy G oraz g jest elementem grupy G, to gHg^{-1} jest podgrupą grupy G izomorficzną z grupą H.

Dowód.

Ze Stwierdzenia 4.3 wynika, że funkcja $\varphi\colon G \to G$ dana wzorem $\varphi(h) := ghg^{-1}$, $h \in G$, jest automorfizmem grupy G. Stąd funkcja $\varphi\mu\colon H \to G$, gdzie $\mu : H \to G$ jest naturalnym włożeniem, jest monomorfizmem. Ponieważ $\operatorname{Im}(\varphi\mu) = gHg^{-1}$, więc teza wynika ze Stwierdzeń 1.11 i 1.12(1) oraz Pierwszego Twierdzenia o Izomorfizmie (Twierdzenie 1.34). □

Definicja.

Podgrupy H i K grupy G nazywamy sprzężonymi, jeśli istnieje element g grupy G taki, że $K = gHg^{-1}$.

Uwaga.

(1) Relacja sprzężenia jest relacją równoważności.

(2) Możemy powiedzieć, że podgrupa H grupy G jest dzielnikiem normalnym wtedy i tylko wtedy, gdy $H = K$ dla dowolnej podgrupy K sprzężonej z H.

Definicja.

Jeśli grupa G działa na zbiorze X, to dla dowolnego elementu x zbioru X definiujemy

$$G_x := \{g \in G : g * x = x\}$$

oraz

$$G * x := \{g * x : g \in G\}.$$

Zbiór G_x nazywamy STABILIZATOREM lub PODGRUPĄ IZOTROPII ELEMENTU x, natomiast Gx będziemy nazywać ORBITĄ ELEMENTU x.

Stwierdzenie 4.6.
Załóżmy, że grupa G działa na zbiorze X.

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

$x \sim y$ wtedy i tylko wtedy, gdy $y = g * x$ dla pewnego elementu g grupy G

jest relacją równoważności.

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

(3) Dla każdego elementu x zbioru X zbiór G_x jest podgrupą grupy G.

(4) Jeśli x jest elementem zbioru X oraz g jest elementem grupy G, to

$$G_{gx} = gG_xg^{-1}.$$

Dowód.
Bezpośrednie rachunki.

Twierdzenie 4.7.
Jeśli grupa G działa na zbiorze X oraz x jest elementem zbioru X, to funkcja

$$G/G_x \in gG_x \mapsto g * x \in G * x$$

jest bijekcją.

Dowód.
Bezpośredni rachunek. □

4.2. Twierdzenia Sylowa

Definicja.
Jeśli G jest grupą, która działa na zbiorze X, to

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

Elementy zbioru X^G nazywamy PUNKTAMI STAŁYMI dla działania grupy G na zbiorze X.

Lemat 4.8.
Jeśli p jest liczbą pierwszą oraz G jest grupą rzędu p^n, $n \in \mathbb{N}_+$, która działa na zbiorze skończonym X, to

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

Dowód.

Ze Stwierdzenia 4.6 wynika, że istnieją elementy $x_1, \ldots, x_k \in X$ takie, że

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

zbiory X^G, $G * x_1$, $\ldots$, $G * x_k$ są parami rozłączne oraz $|G * x_i| > 1$ dla każdego $i \in \{1, \ldots, n\}$. Z Twierdzenia 4.7 (i Twierdzenia Lagrange'a) wiemy, że $|G * x_i| = |G|/|G_{x_i}|$. Ponieważ $|G * x_i| > 1$, $|G| = p^n$, oraz p jest liczbą pierwszą, więc wnioskujemy stąd, że p dzieli $|G * x_i|$, $i = 1, \ldots, n$, co kończy dowód. □

Twierdzenie 4.9 (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 $(g_1, \ldots, g_p)$ takich, że $g_i \in G$ dla każdego $i \in \{1, \ldots, p\}$ oraz $g_1 \cdots g_p = 1$. Zauważmy, że $|X| = |G|^{p-1}$, zatem p dzieli $|X|$. Rozważmy działanie grupy $\mathbb{Z}_p$ na zbiorze X dane wzorem

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

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

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

Z Lematu 4.8 wynika, że p dzieli $|X^{\mathbb{Z}_p}|$. Ponieważ $(1, \ldots, 1) \in X^{\mathbb{Z}_p}$, więc $|X^{\mathbb{Z}_p}| \geq p > 1$. W szczególności istnieje $g \neq 1$ takie, że $g^p = 1$. Ponieważ p jest liczbą pierwszą, więc z Wniosku 3.8 wynika, że $\operatorname{ord}(g) = p$. □

Definicja.

Jeśli p jest liczbą pierwszą, to grupę G nazwiemy p-grupą, jeśli rząd każdego elementu grupy G jest potęgą liczby p. Jeśli podgrupa H grupy G jest p-grupą, to podgrupę H nazywamy p-podgrupą grupy G.

Wniosek 4.10.

Jeśli p jest liczbą pierwszą oraz G jest grupą skończoną, to grupa G jest p-grupą wtedy i tylko wtedy, gdy rząd grupy 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 Twierdzenia 4.9 wynika, że istnieje element grupy G, którego rząd jest równy q. Stąd natychmiast otrzymujemy, że $q = p$, co kończy dowód. □

Definicja.

Niech H będzie podgrupą grupy G. Wtedy

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

Zbiór $N_G(H)$ nazywamy normalizatorem podgrupy H w grupie G.

Uwaga.

Jeśli H jest podgrupą grupy G, to $N_G(H)$ jest podgrupą grupy G oraz H jest dzielnikiem normalnym grupy $N_G(H)$.

Lemat 4.11.

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

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

(Trzeba sprawdzić, że gdy $g' \sim_H g''$, to $hg' \sim_H hg''$ dla dowolnych $h \in H$ oraz $g', g'' \in G$.) Zauważmy, że $gH \in (G/H)^H$ wtedy i tylko wtedy, gdy $g \in N_G(H)$. Stąd $|(G/H)^H| = [N_G(H) : H]$, co kończy dowód wobec Lematu 4.8. □

Wniosek 4.12.

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

Dowód.

Ponieważ $[N_G(H) : H] \equiv [G : H] \pmod{p}$ na mocy Lematu 4.11, więc p dzieli $[N_G(H) : H]$.

Dla dowodu drugiej części wniosku zauważmy, że z Twierdzenia 4.9 istnieje podgrupa L rzędu p w grupie $N_G(H)/H$. Niech $K = \pi^{-1}(L)$, gdzie $\pi\colon N_G(H) \to N_G(H)/H$ jest naturalnym rzutowaniem. Wtedy K jest podgrupą grupy $N_G(H)$ na mocy Stwierdzenia 1.11, a więc także grupy G. Ponadto $[K : H] = |L| = p$, zatem K jest p-grupą. Wreszcie H jest dzielnikiem normalnym grupy K, gdyż $K \subseteq N_G(H)$. □

Twierdzenie 4.13 (Pierwsze Twierdzenie Sylowa).

Niech p będzie liczbą pierwszą oraz G będzie grupą rzędu $p^n m$, gdzie $n, m \in \mathbb{N}$ oraz $p \nmid m$. Wtedy

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

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

Dowód.
Wynika natychmiast z Wniosku 4.12 przez indukcję ze względu na i. □

Definicja.
Jeśli p jest liczbą pierwszą, to podgrupę P grupy G nazywamy p-podgrupą Sylowa, jeśli P jest maksymalną (w sensie zawierania) p-podgrupą grupy G.

Uwaga.
Każda p-podgrupa jest zawarta w pewnej p-podgrupie Sylowa. W szczególności w każdej grupie istnieje p-podgrupa Sylowa.

Wniosek 4.14.
Niech p będzie liczbą pierwszą oraz G będzie grupą rzędu $p^n m$, gdzie $n, m \in \mathbb{N}$ oraz $p \nmid m$.

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

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

Dowód.
Natychmiast z Pierwszego Twierdzenia Sylowa (z wykorzystaniem Twierdzenia Lagrange'a oraz Wniosku 4.10). □

Twierdzenie 4.15 (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 zgodnie ze wzorem

$$g * (hP) \mapsto (gh)P \qquad (g \in Q,\ h \in G).$$

Wiemy, że $|(G/P)^Q| \equiv [G : P] \pmod{p}$ na mocy Lematu 4.8. Ponieważ P jest p-podgrupą Sylowa, więc p nie dzieli $[G : P]$, stąd $(G/P)^Q \neq \emptyset$. Zauważmy, że $hP \in (G/P)^Q$ wtedy i tylko wtedy, gdy $Q \subseteq hPh^{-1}$. Ponieważ $|Q| = |P| = |hPh^{-1}|$, więc $Q = hPh^{-1}$. □

Twierdzenie 4.16 (Trzecie Twierdzenie Sylowa).
Niech p będzie liczbą pierwszą oraz N będzie liczbą p-podgrup Sylowa grupy skończonej G. Wtedy N dzieli $|G|$ oraz $N \equiv 1 \pmod{p}$.

Dowód.

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

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

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

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

więc N dzieli $|G|$ na mocy Twierdzenia 1.30.

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