Wstęp

Kurs Geometrii z algebrą liniową na pierwszym roku poświęcony był badaniu przestrzeni liniowych nad ciałami. Pojawiły się też inne ważne struktury algebraiczne, niektóre znane już ze szkoły. Zbiór liczb całkowitych, zbiór wielomianów o współczynnikach rzeczywistych, czy też zbiór funkcji ciągłych o wartościach rzeczywistych określonych na odcinku, to struktury w których określone są przemienne działania dodawania i mnożenia spełniające wszystkie aksjomaty ciała z wyjątkiem tego, że dla dowolnego elementu różnego od zera istnieje element odwrotny, czyli nie zawsze możemy wykonać dzielenie. Takie struktury nazywają się pierścieniami przemiennymi z jedynką.

Zbiór macierzy odwracalnych $n \times n$ nad ciałem K z działaniem mnożenia, czy też zbiór permutacji zbioru n – elementowego z działaniem składania to przykłady obiektów algebraicznych zwanych grupami.

Badaniu podstawowych własności pierścieni przemiennych i grup poświęcony jest kurs Algebry I.

1. Grupy i pierścienie - podstawowe definicje i przykłady

Grupy i ich homomorfizmy.

1.1. Definicja. **Grupą** *nazywamy zbiór G, wyposażony*[†] *w trzy działania:*
dwuargumentowe — mnożenie $\big((x,y)\mapsto x\cdot y\big)$,
jednoargumentowe — branie elementu odwrotnego $\big(x\mapsto x^{-1}\big)$
i zeroargumentowe — element wyróżniony 1,
takie że spełnione są następujące aksjomaty:

1. $\forall_{x,y,z\in G}\ (x\cdot y)\cdot z = x\cdot(y\cdot z)$,
2. $\forall_{x\in G}\ x\cdot 1 = 1\cdot x = x$,
3. $\forall_{x\in G}\ x\cdot x^{-1} = x^{-1}\cdot x = 1$.

Działanie dwuargumentowe grupy nazywamy zwykle mnożeniem, a element odwrotny odwrotnością. Aksjomaty grupy gwarantują trzy rzeczy:
1. łączność mnożenia,
2. istnienie elementu neutralnego dla mnożenia,
3. istnienie elementu odwrotnego dla mnożenia.

1.2. Definicja. *Jeżeli* $\forall_{x,y\in G}\quad x\cdot y = y\cdot x$, *to grupę nazywamy* **przemienną** *lub* **abelową**.

Z definicji łatwo wynika, że jest tylko jeden element neutralny mnożenia i że dla dowolnego elementu istnieje dokładnie jeden element odwrotny.

Zamiast $x\cdot y$ piszemy często xy. Zwykle mówimy *grupa* G, pomijając wyszczególnianie pozostałych elementów struktury.

W przypadku grup abelowych często działanie dwuargumentowe oznacza się znakiem $+$ ($x+y$ zamiast $x\cdot y$), element odwrotny przez $-$ ($-x$ zamiast x^{-1}), a element neutralny przez 0. Zapis $(G,\cdot,^{-1},1)$ nazywamy zapisem multiplikatywnym, a zapis $(G,+,-,0)$ zapisem addytywnym. W zapisie multiplikatywnym przyjęte jest odczytywać symbol g^{-1} jako *odwrotność elementu* g; w zapisie addytywnym symbol $-g$ odczytujemy jako *element przeciwny do elementu* g.

1.3. Definicja. *Moc zbioru G nazywamy* **rzędem grupy** *G i oznaczamy symbolem* $|G|$.

1.4. Definicja. **Podgrupą** *grupy G nazywamy podzbiór $H\subseteq G$, taki że*
$\forall_{x,y\in H}\quad x\cdot y\in H$
$\forall_{x\in H}\quad x^{-1}\in H$
$1\in H$.

Zapis $H\leqslant G$ będzie oznaczać, że H jest podgrupą grupy G.

Jest jasne, że $\mathbf{1}=\{1\}\leqslant G$ jest podgrupą. Taką podgrupę będziemy nazywać **podgrupą trywialną**. Oczywiście cała grupa G też jest swoją podgrupą: $G\leqslant G$.

1.5. Przykłady.
0) Grupa $\mathbb{Z}$ liczb całkowitych z dodawaniem - jest to grupa przemienna.

[†] z formalnego punktu widzenia należałoby napisać: czwórkę uporządkowaną $(G,\cdot,^{-1},1)$

1) Niech K będzie ciałem. Symbolem K^+ oznaczamy grupę addytywną tego ciała, symbolem K^* grupę multyplikatywną ciała (zbiorem jej elementów jest $K \setminus \{0\}$). Obie grupy są przemienne.
2) Niech teraz $K = \mathbb{C}$ i rozpatrzmy podgrupy grupy $\mathbb{C}^*$.

2a) $S^1 = \{z \in \mathbb{C}^* : |z| = 1\} \leqslant \mathbb{C}^*$.

2b) Grupa $\mathbb{Z}_n = \{1, \exp(\frac{2\pi i}{n}), \ldots, \exp(\frac{2\pi i(n-1)}{n})\}$ pierwiastków z jedynki stopnia n, z mnożeniem jako działaniem dwuargumentowym. Jest to podgrupa grupy S^1 . Jeżeli $k \,|\, n$, $n = km$, to $\mathbb{Z}_k = \{1, \exp(\frac{2\pi im}{n}), \ldots, \exp(\frac{2\pi i(k-1)m}{n})\} \leqslant \mathbb{Z}_n$ jest podgrupą.

3) Niech K będzie ciałem. Symbolem $GL(n, K)$ oznaczamy grupę macierzy odwracalnych $n \times n$ o współczynnikach z K. Macierze o wyznaczniku 1 stanowią podgrupę, oznaczaną symbolem $SL(n, K) \leqslant GL(n, K)$. Innym ważnym przykładem jest podgrupa macierzy górnotrójkątnych z 1 na głównej przekątnej.

4) W grupie $GL(n, \mathbb{R})$ zawarte są dwie szczególnie interesujące grupy:
$O(n) \leqslant GL(n, \mathbb{R})$ — podgrupa złożona z macierzy ortogonalnych i
$SO(n) \leqslant O(n) \leqslant GL(n, \mathbb{R})$ — podgrupa złożona z macierzy ortogonalnych o wyznaczniku 1.

5) Grupa dihedralna — podgrupa $D_{2n} \leqslant O(2)$ przekształceń zachowujących n–kąt foremny o środku symetrii w początku układu współrzędnych.

$$D_{2n} = \{1, \rho, \rho^2, \ldots, \rho^{n-1}, \varepsilon, \rho\varepsilon, \rho^2\varepsilon, \ldots, \rho^{n-1}\varepsilon\},$$

gdzie ρ jest obrotem o $\frac{1}{n}$ kąta pełnego, a ε symetrią osiową.

Odnotujmy ważny fakt, że $\varepsilon^2 = 1$, $\rho^n = 1$ i $\varepsilon\rho\varepsilon = \varepsilon\rho\varepsilon^{-1} = \rho^{-1}$. Zauważmy, że powyższe tożsamości wystarczają do skonstruowania tabeli działania dwuargumentowego dla D_{2n}.

Zauważmy, że $J_n = \{1, \rho, \rho^2, \ldots, \rho^{n-1}\} \leqslant D_{2n}$ jest podgrupą. Nazywamy ją podgrupą obrotów grupy dihedralnej.

6) Niech X będzie zbiorem. Symbolem Σ_X oznaczamy grupę bijekcji zbioru X z działaniem składania jako mnożeniem i identycznością jako elementem neutralnym. Nazywamy ją grupą permutacji zbioru X. Jeżeli X jest zbiorem n – elementowym, to grupę taką oznaczamy symbolem Σ_n.

Często na zbiorze X zadana jest dodatkowa struktura (na przykład przestrzeni liniowej, afinicznej, metrycznej, topologicznej). Wówczas bijekcje zbioru X zachowujące strukturę są podgrupami $S(X)$. Badanie algebraicznych własności tych podgrup jest istotnym elementem badania rozważanej struktury.

1.6. Definicja. *Przekształcenie $\varphi : G \longrightarrow H$ nazywamy* **homomorfizmem** *grup wtedy i tylko wtedy, gdy $\forall_{g_1, g_2 \in G} \quad \varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$.*

Łatwo sprawdzić, że homomorfizm φ przeprowadza element neutralny na element neutralny, a element odwrotny do g na element odwrotny do $\varphi(g)$, możemy wic w definicji homomorfizmu opuścić wymóg zachowywania działań zero i jedno argumentowych.

Zauważmy, że $id_G : G \to G$ jest homomorfizmem i że złożenie homomorfizmów jest homomorfizmem.

1.7. Uwaga. *Jeżeli $\varphi : G \longrightarrow H$ jest homomorfizmem, to $\varphi(G) \leqslant H$ jest podgrupą grupy H. Także dla każdej podgrupy $H' \leqslant H$, $\varphi^{-1}(H') \leqslant G$ jest podgrupą grupy G.*

Istnieją różne szczególne typy homomorfizmów. Poniżej wymieniamy ich nazwy, stosowane bardzo szeroko w matematyce, również poza teorią grup, czy nawet algebrą:
Izomorfizm: taki homomorfizm $\varphi : G \longrightarrow H$, dla którego istnieje homomorfizm $\psi : H \longrightarrow G$, taki że $\varphi\psi = id_H$ i $\psi\varphi = id_G$.

1.8. Uwaga. Homomorfizm grup jest izomorfizmem wtedy i tylko wtedy, gdy jest homomorfizmem i bijekcją zbiorów. Grupy izomorficzne będziemy uważać za *takie same.*
Automorfizm: Izomorfizm z grupy G w tę samą grupę G.
Monomorfizm: homomorfizm różnowartościowy.
Epimorfizm: homomorfizm, który jest *na.*
Endomorfizm: homomorfizm, którego dziedzina i przeciwdziedzina są identyczne (ale nie żądamy, żeby był *na*).

1.9. Definicja. *Niech $\varphi : G \to H$ będzie homomorfizmem. Podgrupę $\varphi^{-1}(\mathbf{1}) = \{g \in G\colon \varphi(g) = 1\} \leqslant G$ oznaczamy symbolem* $\ker\varphi$ *i nazywamy* **jądrem** *homomorfizmu φ.*

1.10. Uwaga. *Homomorfizm φ jest monomorfizmem wtedy i tylko wtedy, gdy* $\ker\varphi = \mathbf{1}$.

Jeżeli homomorfizm $\varphi : G \longrightarrow H$ jest monomorfizmem, to $\varphi : G \longrightarrow \mathrm{im}\,(\varphi)$ jest izomorfizmem ($\mathrm{im}\,(\varphi) = \varphi(G)$).

1.11. Przykłady.

0) Niech $G = \{0, 1, \ldots, n-1\}$ z działaniem dodawania modulo n i zerem jako elementem neutralnym. Funkcja $\varphi : G \to \mathbb{Z}_n$, $\varphi(k) = \exp(\frac{2\pi ik}{n})$ jest izomorfizmem. Dlatego grupę G będziemy także oznaczać symbolem $\mathbb{Z}_n$.
1) $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$, $\varphi(k) = \exp(\frac{2\pi ik}{n})$
2) $det : GL(n, K) \longrightarrow K^*$
3) Niech X będzie przestrzenią liniową n – wymiarową nad ciałem K. Wybór bazy zadaje izomorfizm grupy liniowych automorfizmów przestrzeni X z grupą macierzy $GL(n, K)$.

Pierścienie i ich homomorfizmy.

1.12. Definicja. **Pierścieniem przemiennym z jedynką** *nazywamy zbiór R wyposażony*[†] *w pięć działań:*
dwa dwuargumentowe — dodawanie $\big((x,y)\mapsto x+y\big)$ i mnożenie $\big((x,y)\mapsto x\cdot y\big)$,
jedno jednoargumentowe — branie elementu przeciwnego $(x\mapsto -x)$,
dwa zeroargumentowe — element wyróżniony 0 oraz — element wyróżniony 1,
takie że $(R,+,-,0)$ jest grupą przemienną i są spełnione następujące warunki:
$\forall_{a,b,c\in R}\ a\cdot(b\cdot c)=(a\cdot b)\cdot c$
$\forall_{a,b\in R}\ a\cdot b=b\cdot a$
$\forall_{a,b,c\in R}\ a\cdot(b+c)=a\cdot b+a\cdot c$ *oraz* $\forall_{a,b,c\in R}\ (b+c)\cdot a=b\cdot a+c\cdot a$.
$\forall_{a\in R}\ 1\cdot a=a\cdot 1=a$.

1.13. Definicja. **Podpierścieniem** *pierścienia z jedynką R nazywamy podzbiór $P\subseteq R$, taki że*
P jest podgrupą grupy addytywnej pierścienia R,
$1\in P$,
$\forall_{a,b\in P}\ a\cdot b\in P$.

Zapis $P\leqslant R$ będzie oznaczać, że P jest podpierścieniem pierścienia R.

W definicji pierścienia z jedynką nie zakładaliśmy, że $0\neq 1$. Jednak istnieje tylko jeden pierścień, w którym $0=1$, tak zwany pierścień zerowy.

1.14. Przykład. Pierścieniem zerowym nazywamy pierścień zawierający tylko jeden element $0=1$.

1.15. Uwaga Jeżeli $0=1$, to w rozpatrywanym pierścieniu R nie ma żadnych innych elementów.

Dowód. Niech $x\in R$. Wówczas $x=x\cdot 1=x\cdot 0=0$. □

1.16. Uwaga W algebrze rozpatruje się także pierścienie nieprzemienne oraz pierścienie bez 1, czyli bez wyróżnionego elementu neutralnego względem mnożenia. Jednym z ważnych przykładów nieprzemiennego pierścienia z 1 jest pierścień macierzy.

1.17. Przykład. Jeżeli R jest niezerowym pierścieniem przemiennym z jedynką, to zbiór macierzy $n\times n$, oznaczany symbolem $M_{n\times n}(R)$, ze zwykłymi działaniami na macierzach, jest pierścieniem z jedynką. Dla $n>1$ pierścień ten jest nieprzemienny.

Na tym wykładzie ograniczamy się do rozpatrywania pierścieni przemiennych z jedynką.

1.18. Przykład. Ciało jest pierścieniem przemiennym z jedynką.

1.19. Przykład. Jeżeli R jest pierścieniem pierścieniem przemiennym z jedynką, a X jest dowolnym niepustym zbiorem, to zbiór R^X, z działaniami określonymi w oczywisty sposób (np. $f\cdot g=h$, gdzie $h(x)=f(x)\cdot g(x)$), jest pierścieniem przemiennym z jedynką.

1.20. Przykład. $C[0,1]$ - zbiór funkcji ciągłych określonych na odcinku $[0,1]$, ważny obiekt badań analizy matematycznej, z działaniami jak w poprzednim przykładzie, jest pierścieniem przemiennym z 1.

1.21. Przykład. Pierścień $\mathbb{Z}_n$ liczb całkowitych modulo n z dodawaniem i mnożeniem modulo n.

[†] z formalnego punktu widzenia należałoby napisać: szóstkę uporządkowaną $(R,+,\cdot,-,0,1)$.

1.22. Przykład. Pierścień wielomianów: Niech R będzie pierścieniem przemiennym z jedynką. Pierścieniem wielomianów jednej zmiennej nad R nazywamy zbiór ciągów

$$\{(a_0, a_1, \dots)\colon a_i \in R, \quad a_i = 0 \ \text{ dla prawie wszystkich } i\}$$

z działaniami

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$$

$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (c_0, c_1, \dots), \quad \text{gdzie } c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

$$-(a_0, a_1, \dots) = (-a_0, -a_1, \dots)$$

oraz elementami: $(0, 0, 0, \dots)$ jako zerem i $(1, 0, 0, \dots)$ jako jedynką.

1.23. Definicja. *Stopniem wielomianu $f = (a_0, a_1, \dots)$ nazywamy największą liczbę naturalną n, taką że $a_n \neq 0$ i oznaczmy symbolem* $\deg(f)$.

Oznaczymy przez X ciąg $(0, 1, 0, 0, \dots)$. Ciąg $(a, 0, 0, \dots)$ będziemy w skrócie oznaczać literą a. Wówczas $X^n = (0, 0, \dots, 0, 1, 0, \dots)$ — ciąg z jedynką na n–tym miejscu. Ponadto $(a_0, a_1, \dots, a_n, 0, 0, \dots) = a_0 + a_1 X + \cdots + a_n X^n$. W tej konwencji mnożenie wielomianów wyraża się znanym wzorem.
Pierścień wielomianów nad R oznaczamy symbolem $R[X]$.
Konstrukcję pierścienia wielomianów można iterować: $(R[X])[Y]$ oznaczamy symbolem $R[X, Y]$ i nazywamy pierścieniem wielomianów dwóch zmiennych.

W podobny sposób definiujemy też pierścień wielomianów dowolnej skończonej liczby zmiennych.

1.24. Przykład. Pierścień szeregów formalnych: Jeżeli w Przykładzie 8.9 opuścimy założenie, że prawie wszystkie współczynniki a_i są równe 0, to z analogicznie określonymi działaniami otrzymamy pierścień szeregów formalnych, który oznaczamy symbolem $R[[X]]$. Tak, jak w przypadku wielomianów, zamiast ciągu $(a_1, a_2, \dots)$ piszemy $\sum\limits_{i=0}^{\infty} a_i X^i$. Działania wyrażają się znanymi wzorami:

$$\sum_{i=0}^{\infty} a_i X^i + \sum_{i=0}^{\infty} b_i X^i = \sum_{i=0}^{\infty} (a_i + b_i) X^i$$

$$\Big(\sum_{i=0}^{\infty} a_i X^i\Big) \cdot \Big(\sum_{i=0}^{\infty} b_i X^i\Big) = \sum_{i=0}^{\infty} c_i X^i, \quad \text{gdzie } c_i = \sum_{j=0}^{i} a_j b_{i-j} \quad .$$

Podobnie jak w przypadku wielomianów konstrukcję pierścienia szeregów formalnych można iterować: $(R[[X]])[[Y]]$ oznaczamy $R[[X, Y]]$ i nazywamy pierścieniem szeregów formalnych dwóch zmiennych, itd.

Podajemy jeszcze jeden przykład, dla zilustrowania tego, jak ważne jest precyzyjne określenie rodzaju rozpatrywanych obiektów.

1.25. Przykład. Rozpatrujemy pierścień przemienny z jedynką $\mathbb{Z}_{10}$. Działania dodawania i mnożenia są wykonywane modulo 10, jedynką jest oczywiście liczba 1,

a zerem liczba 0. Rozpatrzmy podzbiór $P = \{0, 5\}$. Podzbiór ten nie zawiera jedynki pierścienia z jedynką $\mathbb{Z}_{10}$, więc nie jest podpierścieniem pierścienia z jedynką $\mathbb{Z}_{10}$. Zauważmy jednak, że zbiór P jest zamknięty ze względu na mnożenie, dodawanie, branie elementu odwrotnego i zawiera element zerowy. Przyjęty sposób wyrażenia tej sytuacji, to stwierdzenie, że P jest podpierścieniem $\mathbb{Z}_{10}$ w kategorii pierścieni, ale *nie* w kategorii pierścieni przemiennych z jedynką. Zauważmy jeszcze, że w zbiorze P *jest* element neutralny ze względu na mnożenie — liczba 5 ($5 \cdot 5 = 25 = 5,\ 5 \cdot 0 = 0$). Ale to nie wystarcza, żeby P uznać za podpierścień pierścienia $\mathbb{Z}_{10}$ w kategorii pierścieni przemiennych z jedynką. Definicja wymaga, żeby do podpierścienia pierścienia przemiennego z jedynką należała jedynka wyjściowego pierścienia.

1.26. Przykład. Niech $d \in \mathbb{Z}$ będzie liczba całkowitą,$d \neq 1$, która nie jest podzielna przez kwadrat liczby naturalnej różnej od 1 - taką liczbę nazywamy bezkwadratową. Oznaczmy przez $\mathbb{Z}[\sqrt{d}]$ podpierścień ciała liczb zespolonych, którego elementami są liczby postaci $a + b\sqrt{d}$, $a, b \in \mathbb{Z}$. Jak się przekonamy wąsności tych pierścieni mają ścisły związek z teorią liczb.

1.27. Definicja. *Przekształcenie $\varphi : R \to P$ pierścieni przemiennych z jedynką nazywamy* **homomorfizmem**, *jeżeli są spełnione następujące warunki.*
a) φ *jest homomorfizmem grup addytywnych,*
b) $\forall_{a,b \in R}\ \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$,
c) $\varphi(1) = 1$.

1.28. Uwaga. *Jeżeli $\varphi : R \longrightarrow P$ jest homomorfizmem, to $\varphi(R) \leqslant P$ jest podpierścieniem pierścienia P. Także dla każdego podpierścienia $P' \leqslant P$, $\varphi^{-1}(P') \leqslant R$ jest podpierścieniem pierścienia R.*

Określenia izomorfizm, monomorfizm, epimorfizm, automorfizm, endomorfizm są używane w sposób analogiczny, jak w teorii grup.

1.29. Uwaga. Homomorfizm pierścieni jest izomorfizmem wtedy i tylko wtedy, gdy jest homomorfizmem i bijekcją zbiorów.

1.30. Przykład. Jedynym homomorfizmem $\mathbb{Z} \to \mathbb{Z}$ jest identyczność.
1.31. Przykład. Istnieje dokładnie jeden homomorfizm $f : \mathbb{Z} \to \mathbb{Z}_n$ — określony wzorem $f(x) = x \pmod{n}$.
1.32. Przykład. Istnieje dokładnie jeden homomorfizm z dowolnego pierścienia w pierścień zerowy.
1.33. Przykład. Dla każdego elementu a pierścienia R wzór

$$\phi_a(a_n X^n + \cdots + a_1 X + a_0) = a_n a^n + \cdots + a_1 a + a_0$$

określa pewien homomorfizm $\phi_a : R[X] \to R$.
1.34. Przykład. Określimy pewien homomorfizm $\Phi : R[X] \to R^R$. Niech $w = a_n X^n + \cdots + a_1 X + a_0$. Obraz wielomianu w oznaczamy symbolem Φ_w i zadajemy wzorem:

$$\Phi_w(a) = a_n a^n + \cdots + a_1 a + a_0.$$

Tak więc $\Phi_w(a)$ to po prostu $w(a)$ — wartość wielomianu w w punkcie a. Elementy zbioru $\Phi(R[X])$ nazywamy funkcjami wielomianowymi.

Dobrze wiadomo, że dla ciał $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ homomorfizm Φ jest monomorfizmem — różne wielomiany wyznaczają różne funkcje. Spójrzmy jednak na następujący przykład: $R = \mathbb{Z}_2$, $w_1 = X^2 + X$, $w_2 = X^3 + X$. Łatwo sprawdzić, że $\Phi_{w_1} = \Phi_{w_2}$ — jest to w obydwu przypadkach funkcja zerowa.

1.35. Przykład. Niech R będzie dowolnym pierscieniem przemiennym z jedynką. Dla każdego elementu $r \in R$ istnieje dokładnie jeden homomorfizm $f : \mathbb{Z}[X] \to R$, dla którego $f(X) = r$

Podstawowa konstrukcja - produkt

(część ujęta w gwiazdkach jest materiałem nieobowiązkowym)

*Konstrukcja produktu i sumy występuje w wielu sytuacjach w matematyce. Zanim więc podamy ją dla pierścieni i grup przedstawimy problem w ogólniejszym kontekście - teorii kategorii. Taki punkt widzenia został zaproponowany przez Samuela Eilenberga (absolwenta i doktora UW, doktora Honoris Causa UW, który przed wojną wyjechał do USA i tam pozostał) w latach czterdziestych i pięćdziesiątych ubiegłego stulecia i przyjął się w większości dziedzin matematyki, informatyki nie wyłączając.

1.36. Definicja. *Kategoria $\mathcal{C}$ składa się z klasy obiektów $ob\mathcal{C}$ oraz zbiorów morfizmów $Mor_{\mathcal{C}}(A, B)$ danych dla dowolnych dwóch obiektów $A, B \in ob\mathcal{C}$. Ponadto*

- *Dla każdego $A \in ob\mathcal{C}$ wyróżniony jest element $id_A \in Mor_{\mathcal{C}}(A, A)$*
- *Dla każdych $A, B, C \in ob\mathcal{C}$ zadana jest operacja składania*

$$\circ : Mor_{\mathcal{C}}(A, B) \times Mor_{\mathcal{C}}(B, C) \longrightarrow Mor_{\mathcal{C}}(A, C)$$

- *operacja składania jest łączna, zaś elementy wyróżnione są dla niej "neutralne", tzn. dla morfizmów f, g, h,*

$$(f \circ g) \circ h = f \circ (g \circ h), \qquad id \circ f = f, \qquad f \circ id = f$$

1.37. Definicja. *Morfizm $f \in Mor_{\mathcal{C}}(A, B)$ nazywa się izomorfizmem wtedy i tylko wtedy, gdy istnieje morfizm $g \in Mor_{\mathcal{C}}(B, A)$ taki, że $g \circ f = id_A$ i $f \circ g = id_B$.*

1.38. Przykład. $\mathcal{S}et$ – kategoria zbiorów. Obiektami są zbiory, zaś morfizmami przekształcenia zbiorów. Operacja składania to składanie przekształceń. Izomorfizmami są przekształcenia wzajemnie jednoznaczne i "na", czyli bijekcje zbiorów.

1.39. Przykład. $\mathcal{V}ect_K$ – kategoria przestrzeni liniowych nad ustalonym ciałem. Obiektami są przestrzenie liniowe nad K, morfizmami przekształcenia liniowe.

1.40. Przykład. $\mathcal{G}r$ – kategoria grup. Obiektami są grupy, morfizmami homomorfizmy grup.

1.41. Przykład. $\mathcal{A}b$ – kategoria grup abelowych. Jak wyżej, tylko obiektami są wyłącznie grupy abelowe.

1.42. Przykład. $\mathcal{R}$ – kategoria pierścieni przemiennych z 1. Obiektami są pierścienie przemienne z 1, zaś morfizmami homomorfizmy pierścieni z 1.

1.43. Przykład. $\mathcal{T}op$ – Obiektami są przestrzenie topologiczne, morfizmami przekształcenia ciągłe. Izomorfizmy nazywają się homeomorfizmami.

We wszystkich powyższych przykładach obiektami są zbiory wyposażone w pewne dodatkowe struktury a morfizmami są przekształcenia, które te struktury zachowują. Tak wcale być nie musi - na kategorię trzeba patrzeć jak na klasę obiektów i zbiory strzałek między nimi i strzałki te można składać. Pomysł polega na tym, by definiować konstrukcje i własności patrząc wyłącznie na owe strzałki. W ten sposób pewne konstukcje i ich własności są uniwersalne, niezależnie od tego w jakim matematycznym kontekście je roważamy.

1.44. Definicja. *Niech $\{X_\alpha\}_{\alpha\in\Lambda}$ będzie rodziną obiektów kategorii $\mathcal{C}$. Ich produktem nazywamy obiekt $\prod_{\alpha\in\Lambda} X_\alpha$ oraz rodzinę morfizmów $\pi_\alpha\colon \prod_{\alpha\in\Lambda} \to X_\alpha$, taką że dla każdego obiektu $Y \in ob\mathcal{C}$ i każdej rodziny morfizmów $\varphi_\alpha\colon Y \to X_\alpha$ istnieje dokładnie jeden morfizm $\psi : Y \to \prod_{\alpha\in\Lambda} X_\alpha$ dla którego $\pi_\alpha \circ \psi = \varphi_\alpha$, dla każdego $\alpha \in \Lambda$.*

1.45. Definicja. *Niech $\{X_\alpha\}_{\alpha\in\Lambda}$ będzie rodziną obiektów kategorii $\mathcal{C}$. Ich sumą nazywamy obiekt $\coprod_{\alpha\in\Lambda} X_\alpha$ oraz rodzinę morfizmów $i_\alpha\colon X_\alpha \to \coprod_{\alpha\in\Lambda}$, taką że dla każdego obiektu $Y \in ob\mathcal{C}$ i każdej rodziny morfizmów $\varphi_\alpha\colon X_\alpha \to Y$ istnieje dokładnie jeden morfizm $\psi : \coprod_{\alpha\in\Lambda} \to Y$ dla którego $\psi \circ i_\alpha = \varphi_\alpha$, dla każdego $\alpha \in \Lambda$.*

Jednoznaczność produktu (analogicznie sumy), z dokładnością do izomorfizmu w $\mathcal{C}$, wynika z definicji, natomiast istnienie trzeba dowodzić dla każdej kategorii oddzielnie.

Powiemy, że kategoria *dopuszcza produkty* (odp. dopuszcza sumy) jeżeli dla dowolnej skończonej rodziny obiektów istnieje ich produkt (odp. suma). Oczywiście na to by pokazać. że kategoria dopuszcza produkty (odp. sumy) wystarczy zdefiniować produkt (odp. sumę) dwóch obiektów. Nie każda kategoria dopuszcza produkty ew. sumy. Poniżej pokażemy, że kategoria grup $\mathcal{G}r$ i kategoria pierścieni z 1, $\mathcal{R}$ dopuszczają produkty. *

1.46. Definicja. Produkt grup: *Jeżeli G i H są grupami, to iloczyn kartezjański $G \times H$ z działaniami $(g, h) \cdot (g', h') = (g \cdot g', h \cdot h')$, $(g, h)^{-1} = (g^{-1}, h^{-1})$ oraz elementem neutralnym $(1_G, 1_H)$ jest grupą, zaś $\pi_G \times H \to G$, $p_G(x, y) = x$ i $\pi_H \times H \to H$, $\pi_H(x, y) = y$ homomorfizmami. Grupa $G \times H$ wraz z homomorfizmami π_G, π_H jest produktem grup G i H.*

Zbiory $G \times \mathbf{1}_H = \{(g, 1_H) : g \in G\} \leqslant G \times H$ i $\mathbf{1}_G \times H = \{(1_G, h) : h \in H\} \leqslant G \times H$ są podgrupami — oczywiście pierwsza podgrupa jest izomorficzna z G, a druga z H. Niech homomorfizmy $i_G : G \to G \times H$, $i_H : H \to G \times H$ będą zadane wzorami $i_G(g, h) = (g, 1_H)$, $i_H(g, h) = (1_G, h)$.

*Niech teraz grupy G i H będą przemienne - użyjemy więc zapisu addytywnego.

1.47. Stwierdzenie. *Jeżeli grupy G i H są przemienne, to $G \times H$ wraz z homomorfizmami i_G, i_H jest sumą grup G i H w kategorii grup abelowych.*

Dowód. Niech J będzie dowolną grupą przemienną, a $\varphi_G : G \to J$ i $\varphi_H : H \to J$ będĄ dowolnymi homomorfizmami. Jest jasne, że $\psi : G \times H \to J$ zadane wzorem $\psi(g, h) = \varphi_G(g) + \varphi_H(h)$ jest jedynym homomorfizmem spełniającym warunek $\psi \circ i_G = \varphi_G$ i $\psi \circ i_H = \varphi_H$. □

Sumę grup abelowych G i H oznacza się także symbolem $G \oplus H$ - tak więc w kategorii grup abelowych oznaczenia skończonej sumy ($\oplus$) i skończonego produktu ($\times$) są używane zamiennie.

1.48. Przykład. Produkt $G \times H$ wraz z homomorfizmami i_G, i_H **nie jest** sumą w kategorii wszystkich grup. Rozpatrzmy $G = H = \mathbb{Z}$, i grupę Σ_3 permutacji trzech elementów lub równoważnie grupę symetrii trójkąta równobocznegoABC na płaszczyźnie. Niech $\varphi_1 : \mathbb{Z} \to \Sigma_3$, przyporządkowuje $1 \in \mathbb{Z}$ symetrię względem symetralnej boku AB, zaś φ_2 względem boku AC. Nie istnieje żądany w definicji homomorfizm z grupy przemiennej $\mathbb{Z} \times \mathbb{Z} \to \Sigma_3$ gdyż symetrie $\varphi_i(1)$, $i = 1, 2$ nie są przemienne. Zainteresowany czytelnik może spróbować wykazać, że szukaną sumą jest grupa słów o dwuelementowym alfabecie.*

1.49. Definicja. Produkt pierścieni: *Na iloczynie kartezjańskim $P \times R$ pierścieni przemiennych z jedynką można określić działania wzorami*

$$(x,y)+(x',y')=(x+x',y+y'),\ -(x,y)=(-x,-y),\ 0=(0_P,0_R)$$
$$(x,y)(x',y')=(xx',yy'),\qquad 1=(1_P,1_R).$$

Zbiór $P\times R$ z tak określonymi działaniami jest pierścieniem przemiennym z jedynką, zaś $p_P \times R \to P$, $p_P(x,y)=x$ i $p_R \times R \to R$, $p_R(x,y)=y$ homomorfizmami. Pierścień $P \times R$ wraz z homomorfizmami p_P, p_R jest produktem pierścieni P i R.

Kategoria grup i kategoria pierścieni przemiennych z 1 dopuszczają sumy - to zagadnienie odłożymy na później.

TEORIA GRUP

2. Zbiór generatorów grupy. Grupa cykliczna, rząd elementu

Teorię grup zacznijmy od następującego oczywistego stwierdzenia.

2.1. Stwierdzenie. *Jeżeli $\{H_i\}_{i\in I}$ jest rodziną podgrup grupy G, to zbiór $\bigcap_{i\in I} H_i \leqslant G$ jest podgrupą grupy G.*

Wobec tego, dla dowolnego podzbioru $X \subseteq G$ istnieje najmniejsza podgrupa grupy G zawierająca X. Nazywamy ją **podgrupą generowaną** przez X i oznaczamy symbolem $\langle X \rangle$.

Oczywiście $\langle \emptyset \rangle = \mathbf{1}$.

2.2. Stwierdzenie. *Jeżeli $X \neq \emptyset$, to*

$$\langle X \rangle = \{g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_k^{\varepsilon_k} \colon k \in \mathbb{N},\ \varepsilon_i = \pm 1,\ g_i \in X\}.$$

Dowód. Jest jasne, że zbiór elementów tej postaci tworzy podgrupę grupy G i jest zawarty w każdej podgrupie grupy G zawierającej X. □

Jeżeli $\langle X \rangle = G$, to X nazywamy zbiorem generatorów G. Mówimy, że grupa jest skończenie generowana jeżeli posiada skończony zbiór generatorów.

2.3. Definicja. *Grupę G nazywamy* **cykliczną** *jeżeli istnieje element $g \in G$, taki że $\langle g \rangle = G$.*

2.4. Twierdzenie. *Grupy $\mathbb{Z}_n$ i $\mathbb{Z}$ są cykliczne. Każda grupa cykliczna jest izomorficzna z jedną z nich.*

Dowód. $\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z}_n = \langle \exp(\frac{2\pi i}{n}) \rangle$, zatem grupy te są cykliczne.

Niech $G = \langle g \rangle$, czyli $G = \{g^i, i \in \mathbb{Z}\}$.

Przypuśćmy, że istnieje $n \in \mathbb{N}$, takie że $g^n = 1$ i załóżmy, że n jest najmniejszą liczbą naturalną o tej własności. Każda liczba całkowita $k \in \mathbb{Z}$ może być przedstawiona w postaci $k = ln + r$, gdzie $r \in \{0, 1, \ldots, n-1\}$, a zatem $g^k = g^r$. Wynika stąd, że $G = \{1, g, \ldots, g^{n-1}\}$. Wszystkie te elementy są różne (z równości $g^i = g^j$ wynika bowiem $g^{i-j} = 1$). Zatem $|G| = n$ i przekształcenie $\varphi : \mathbb{Z}_n \longrightarrow G$, $\varphi(\exp(\frac{2\pi i m}{n})) = g^m$ jest izomorfizmem.

Jeżeli nie istnieje $n \in \mathbb{N}$, takie że $g^n = 1$, to wszystkie elementy $\{g^i, i \in \mathbb{Z}\}$ są różne, $|G| = \infty$, a odwzorowanie $\varphi : \mathbb{Z} \longrightarrow G$, zadane wzorem $\varphi(m) = g^m$ jest izomorfizmem. □

2.5. Twierdzenie. *Niech G będzie grupą cykliczną. Wówczas:*

1) Jeżeli $H \leqslant G$, to H jest grupą cykliczną.

2) Jeżeli $H \leqslant G$ i $|G| < \infty$, to $|H| \,\big|\, |G|$.

3) Jeżeli $|G| < \infty$, to dla każdego $l \,\big|\, |G|$ istnieje dokładnie jedna podgrupa $H \leqslant G$, taka że $|H| = l$.

Dowód. Niech $G = \langle g \rangle$. Niech k będzie najmniejszą liczbą całkowitą i dodatnią, taką że $g^k \in H$. Jest jasne, że $\langle g^k \rangle \leqslant H$. Jeżeli $g^m \in H$, $m = ks + r$, $0 \leq r < k$, to $g^m = (g^k)^s g^r$, więc $g^r \in H$. Z minimalności k wynika, że $r = 0$, wobec czego $g^m = (g^k)^s \in \langle g^k \rangle$. Zatem $H = \langle g^k \rangle$, co kończy dowód 1).

Zakładamy teraz, że $|G| < \infty$. Niech więc $|G| = n$, i $n = kl + r$, $r < k$. Ponieważ $g^n = 1 \in H$, zatem, tak jak poprzednio, z minimalności k wynika, że $k \,|\, n$. Wówczas $H = \{1, g^k, g^{2k}, \ldots, g^{(l-1)k}\}$ i $|H| = \frac{n}{k}$, co kończy dowód punktu 2). Punkt 3) wynika już z tych rozważań – jedyną taką podgrupą jest $H = \langle g^k \rangle$, gdzie $k = \frac{n}{l}$.□

2.6. Definicja. **Rzędem** *elementu $g \in G$ nazywamy liczbę $|\langle g \rangle|$, czyli rząd podgrupy generowanej przez element g. Rząd elementu g oznaczamy symbolem $o(g)$.*

Z poprzednich rozważań wynika jasno, że jeżeli $o(g) < \infty$, to :
1. $o(g)$ jest najmniejszą liczbą naturalną n, taką że $g^n = 1$
2. $o(g) = n$ wtedy i tylko wtedy, gdy $g^n = 1$ i dla każdej liczby całkowitej k, takiej że $g^k = 1$, ma miejsce podzielność: $n \mid k$.
3. Jeżeli $\varphi : G \to H$ jest homomorfizmem, to dla każdego elementu $g \in G$ $o(\varphi(g)) \mid o(g)$.

2.7. Stwierdzenie. *Jeżeli $o(g) = n$, to $o(g^k) = \frac{n}{(n,k)}$.*

Dowód. Mamy $n = (n,k)m$ i $k = (n,k) \cdot l$, gdzie $(m,l) = 1$. Wynika stąd, że $(g^k)^m = g^{(n,k)lm} = g^{nl} = 1$, a zatem $o(g^k) \mid m$. Przypuśćmy, że $(g^k)^r = 1$. Wynika stąd, że $n \mid kr$, a zatem $m \mid lr$. Wobec $(m,l) = 1$, $m \mid r$, co dowodzi, że $o(g^k) = m$.□

Z poprzedniego stwierdzenia wynika, że jeżeli $G = \langle g \rangle$ i $|G| = n$, to generatorami G, czyli elementami rzędu n są elementy g^k, gdzie $(k,n) = 1$. Liczbę tych generatorów, to jest ilość takich liczb naturalnych nie większych od n, które są względnie pierwsze z n, oznaczamy symbolem $\varphi(n)$. Funkcję φ nazywamy funkcją Eulera.

2.8. Uwaga. *Jeżeli $k \mid n$, to w grupie cyklicznej rzędu n jest $\varphi(k)$ elementów rzędu k. Mamy więc*

$$\sum_{k \mid n} \varphi(k) = n.$$

2.9. Wniosek. *Jeżeli p jest liczbą pierwszą, to grupa $\mathbb{Z}_p$ nie posiada nietrywialnych podgrup właściwych, każdy element różny od neutralnego jest rzędu p i $\varphi(p) = p - 1$.*

2.10. Stwierdzenie. *Jeżeli $(k,n) = 1$, to $\mathbb{Z}_k \times \mathbb{Z}_n \cong \mathbb{Z}_{kn}$. W przeciwnym przypadku ten produkt nie jest grupą cykliczną.*

Dowód. Niech $g \in \mathbb{Z}_k$ i $h \in \mathbb{Z}_n$ będą generatorami. Element $(g,h)^l = (g^l, h^l)$ jest elementem neutralnym wtedy i tylko wtedy, gdy $n \mid l$ oraz $k \mid l$. Jeżeli $(k,n) = 1$, jest to równoważne $kn \mid l$, a zatem $o((g,h)) = kn = |\mathbb{Z}_k \times \mathbb{Z}_n|$ i grupa jest cykliczna. Jeżeli $(k,n) > 1$, to z tych rozważań wynika, że w $\mathbb{Z}_k \times \mathbb{Z}_n$ nie ma elementu rzędu kn. □

2.11. Wniosek. *Jeżeli $(k,n) = 1$, to $\varphi(kn) = \varphi(k)\varphi(n)$*

2.12. Wniosek. *Jeżeli p jest liczbą pierwszą, to w grupie $\mathbb{Z}_{p^n}$ jest dokładnie $\varphi(p^n) = p^n - p^{n-1}$ elementów rzędu p^n.*

Rzędy elementów w grupach permutacji

Znamy już grupy permutacji. Wiemy, że każda grupa jest, z dokładnością do izomorfizmu, podgrupą pewnej grupy permutacji. Teraz przyjrzymy się dokładniej grupom permutacji zbiorów skończonych. Dla ustalenia uwagi, załóżmy, że n–elementowy zbiór składa się z liczb $\{1, 2, \ldots, n\}$. Permutację $\sigma \in \Sigma_n$ możemy zapisać w postaci macierzowej:

$$\begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

W górnym wierszu macierzy piszemy permutowane elementy, a w dolnym ich obrazy. Na przykład: $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ oznacza permutację γ, taką że $\gamma(1) = 3$, $\gamma(2) = 1$, $\gamma(3) = 4$, $\gamma(4) = 2$.

2.13. Definicja. *Permutację $\gamma \in \Sigma_n$ nazywamy* **cyklem** *długości k, jeżeli istnieją takie elementy $c_1, c_2, \ldots c_k$, że*

$$\gamma(c_i) = \begin{cases} c_{i+1} & gdy\ i < k \\ c_1 & gdy\ i = k, \end{cases}$$

przy czym dla każdego elementu x spoza tej listy zachodzi $\gamma(x) = x$.

Cykl taki będziemy oznaczać symbolem $\gamma = (c_1, \ldots, c_k)$. Oczywiście zapis ten ma sens tylko wtedy, gdy dobrze wiemy, na jakim zbiorze jest określona cała permutacja. Na przykład pytanie o to, czy permutacja $\sigma = (1, 4, 3, 2)$ ma punkty stałe jest bez sensu, jeżeli nie mamy zewnętrznej informacji o tym, na jakim zbiorze ta permutacja jest określona. Warto też zwrócić uwagę na fakt, że zapis ten nie jest jednoznaczny — równie dobrze można by napisać na przykład $\sigma = (2, 1, 4, 3)$.
Cykl długości dwa, (a, b), nazywamy **transpozycją** elementów a i b.

2.14. Definicja. *Cykle $\sigma = (b_1, b_2, \ldots, b_r) \in \Sigma_n$ i $\tau = (c_1, c_2, \ldots, c_s) \in \Sigma_n$ są rozłączne jeżeli $\{b_1, b_2, \ldots, b_r\} \cap \{c_1, c_2, \ldots, c_s\} = \emptyset$.*

Jest jasne, że dwa cykle rozłączne są przemienne.

2.15. Twierdzenie. *Każdą permutację można przedstawić jako iloczyn rozłącznych cykli. Przedstawienie to jest jednoznaczne z dokładnością do kolejności cykli.*

Dowód tego faktu przeprowadza się przez indukcję ze względu na moc permutowanego zbioru — jest on bardzo łatwy i pomijamy go. Ideę dowodu można łatwo zrozumieć analizując przykład.

Rozkład na cykle rozłączne permutacji:

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

W rozkładzie permutacji na cykle rozłączne często opuszcza się cykle długości jeden.

2.16. Stwierdzenie. *Jeżeli permutacja σ jest iloczynem cykli rozłącznych długości $n_1, n_2, \ldots, n_k$, to $o(\sigma) = NWW(n_1, n_2, \ldots, n_k)$*

Dowód. Cykle rozłączne są przemienne, zatem $o(\sigma) \,|\, NWW(n_1, n_2, \ldots, n_k)$. Z drugiej strony, skoro $\sigma^l = id$, to $l-$ ta potęga każdego cyklu jest identycznością (korzystamy tu z rozłączności cykli). Zatem dla każdego $1 \leq i \leq k$ mamy $n_i \,|\, l$, więc $NWW(n_1, n_2, \ldots, n_k) \,|\, o(\sigma)$. □

3. Warstwy grupy względem podgrupy, twierdzenie Lagrange'a

Stwierdzenie, że rząd podgrupy jest dzielnikiem rzędu grupy, które już udowodniliśmy dla grup cyklicznych, jest prawdziwe dla *wszystkich* grup skończonych i nosi nazwę twierdzenia Lagrange'a.

Niech G będzie dowolną (niekoniecznie skończoną) grupą, a $H \leqslant G$ jej podgrupą. Dla dowolnego $g \in G$ rozpatrzmy podzbiór $gH = \{gh;\, h \in H\} \subseteq G$. Łatwo zauważyć, że:

1) zbiór gH jest klasą abstrakcji zawierającą g następującej relacji równoważności w zbiorze elementów G: $x \sim y \iff x^{-1}y \in H$. Zbiór gH nazywamy **warstwą lewostronną elementu g względem podgrupy H**.
2) $1H = H$
3) Dowolne dwie warstwy lewostronne są równoliczne, w szczególności każda warstwa jest równoliczna ze zbiorem H (przyporządkowanie $h \mapsto gh$ ustala bijekcję zbioru H i warstwy gH).

Zbiór warstw lewostronnych oznaczamy symbolem G/H, a jego moc nazywamy **indeksem podgrupy H w grupie** G i oznaczamy $[G\colon H]$. (Uwaga: analogicznie można zdefiniować warstwy prawostronne grupy G względem podgrupy H — są to podzbiory postaci $Hg = \{hg :\, h \in H\} \subseteq G$).

Z faktu, że każda warstwa lewostronna ma tyle samo elementów, co podgrupa H wynika natychmiast następujące twierdzenie.

3.1. Twierdzenie Lagrange'a. *Jeżeli G jest grupą skończoną i $H \leqslant G$, to $|G| = |H| \cdot [G\colon H]$.*

To proste twierdzenie ma szereg oczywistych, ale ważnych, konsekwencji:

3.2. Wniosek. *Rząd elementu jest dzielnikiem rzędu grupy.*

3.3. Wniosek. *Każda grupa rzędu p, gdzie p jest liczbą pierwszą, jest izomorficzna z $\mathbb{Z}_p$.*

Dowód. Z twierdzenia Lagrange'a wynika, że podgrupa cykliczna generowana przez dowolny element różny od neutralnego musi być rzędu p, a więc musi być równa całej rozpatrywanej grupie. □

3.4. Stwierdzenie. *Grupa skończona G rzędu n jest cykliczna wtedy i tylko wtedy, gdy dla każdego $k \mid n$ zawiera co najwyżej jedną podgrupę rzędu k.*

Dowód. Wystarczy pokazać, że w grupie G istnieje element rzędu n. Niech $\nu(k)$ oznacza liczbę elementów rzędu k w grupie G. Z założenia wynika, że

$$\nu(k) \leq \varphi(k),$$

gdzie φ jest funkcją Eulera.Z twierdzenia Lagrange'a wnioskujemy że $\nu(k)$ ma szansę być niezerowe tylko wtedy, gdy $k \mid n$. Zatem

$$n = \sum_{k \mid n} \nu(k) \leq \sum_{k \mid n} \varphi(k) = n,$$

a więc dla każdego $k \mid n$ zachodzi równość $\nu(k) = \varphi(k)$. W szczególności $\nu(n) = \varphi(n) > 0$, co kończy dowód. □

W związku z twierdzeniem Lagrange'a nasuwa się pytanie o możliwość jego odwrócenia. Załóżmy, że k jest dzielnikiem $|G|$. Czy istnieje podgrupa rzędu k grupy G i ile jest takich podgrup? Częściową odpowiedzią na to pytanie będzie twierdzenie Cauchy'ego, które mówi, że jeżeli liczba pierwsza p jest dzielnikiem $|G|$, to w G istnieje element rzędu p, a więc i cykliczna podgrupa rzędu p. Udowodnimy je w następnym rozdziale.

4. Działanie grupy na zbiorze

Znaczna część poznanych przez nas przykładów grup, to podgrupy grupy bijekcji jakiegoś zbioru. Często taka podgrupa składa się z bijekcji, które zachowują dodatkową strukturę geometryczną, topologiczną lub algebraiczną, zdefiniowaną na rozpatrywanym zbiorze.

4.1. Definicja. **Działaniem grupy** *G na zbiorze X nazywamy homomorfizm $\phi\colon G \longrightarrow \Sigma_X$. Działanie nazywamy wiernym, jeżeli ϕ jest monomorfizmem.*

Jeżeli zadane jest działanie grupy G na zbiorze X, to mówimy że X jest G – zbiorem. Zamiast oznaczenia $\phi(g)(x)$ będziemy na ogół używać bardziej czytelnego symbolu $\phi_g(x)$. W tym zapisie ϕ_g jest nazwą pewnej bijekcji zbioru X—bijekcji, którą homomorfizm ϕ przypisuje elementowi g z grupy G. Natomiast $\phi_g(x)$ oznacza wartość tej bijekcji dla argumentu x. Czasem stosuje się jeszcze bardziej uproszczony zapis: $g(x)$ zamiast $\phi_g(x)$.

4.2. Przykład. Dla dowolnej grupy G, niech $\psi_g : G \longrightarrow G$ będzie zadane wzorem $\psi_g(x) = gx$ (poza przypadkiem $g = 1$, ψ_g nie jest automorfizmem G lecz tylko bijekcją zbioru elementów). Przekształcenie $\psi : G \longrightarrow \Sigma_G$, $\psi(g) = \psi_g$ jest oczywiście monomorfizmem grup. Wobec tego prawdziwe jest następujące twierdzenie.

4.3. Twierdzenie Cayleya. *Każda grupa G jest izomorficzna z pewną podgrupą grupy bijekcji zbioru G. W szczególności każda grupa rzędu n jest izomorficzna z pewną podgrupą grupy Σ_n.*

4.4. Definicja. *Każdy element $g \in G$ grupy G wyznacza pewien automorfizm $\phi_g : G \longrightarrow G$, zadany wzorem $\phi_g(x) = gxg^{-1}$. Nazywamy go* **automorfizmem wewnętrznym** *grupy G wyznaczonym przez element g.*

Otrzymujemy homomorfizm $\phi : G \longrightarrow Aut(G)$, $\phi(g) = \phi_g$. Jest to ważny przykład działania grupy G na zbiorze jej elementów - nazywamu go działaniem poprzez automorfizmy wewnętrzne. Zauważmy, że

$$\ker \phi = \{g \in G : \forall_{x\in G}\ gx = xg\}.$$

Tak określona podgrupa ma swoją nazwę:

4.5. Definicja. *Podgrupę*

$$Z(G) = \{g \in G : \forall_{x\in G}\ gx = xg\} \leqslant G$$

nazywamy **centrum grupy.**

Przyjrzyjmy się bliżej strukturze dowolnego G—zbioru X.

4.6. Definicja.
Orbitą *punktu $x \in X$ nazywamy zbiór*

$$G(x) = \{g(x)\colon\ g \in G\} \subseteq X.$$

Punktem stałym *działania grupy G na zbiorze X nazywamy każdy punkt spełniający warunek $G(x) = \{x\}$ lub równoważnie $\forall_{g\in G}\ g(x) = x$. Zbiór punktów stałych oznaczamy symbolem X^G.*
Grupą izotropii *punktu $x \in X$ nazywamy podgrupę*

$$G_x = \{g \in G\colon g(x) = x\} \leqslant G.$$

4.7. Uwaga. *Jeżeli punkt $x' \in G(x)$, to $x' = g(x)$ dla pewnego $g \in G$ i wówczas $G_{x'} = g(G_x)g^{-1}$.*

Rozpatrzmy na zbiorze X relację zadaną wzorem

$$x \sim y \iff \exists_{g\in G} \quad y = g(x).$$

Bez trudu sprawdzimy, że relacja ta jest relacją równoważności, a klasą abstrakcji zawierającą punkt $x \in X$ jest orbita tego punktu $G(x)$. Zatem niepusty G–zbiór X jest sumą parami rozłącznych orbit.

4.8. Definicja. *Działanie grupy G na zbiorze X nazywamy* **tranzytywnym** *(inaczej: przechodnim) wtedy i tylko wtedy, gdy*

$$\forall_{x,\,y\in X}\ \exists_{g\in G}\ g(x) = y.$$

Zauważmy, że działanie na niepustym zbiorze jest tranzytywne wtedy i tylko wtedy, gdy ma dokładnie jedną orbitę.

Rozpatrzymy teraz podstawowy i w pewnym sensie uniwersalny przykład działania grupy:

4.9. Przykład. Niech G będzie dowolną grupą, a H jej podgrupą. Zdefiniujemy działanie $\phi : G \to \Sigma_{G/H}$, grupy G na zbiorze warstw lewostronnych G/H, wzorem $\phi_g(xH) = (gx)H$.

Odnotujmy następujące własności powyższego działania:

1. jest ono tranzytywne;
2. $G_{gH} = gHg^{-1}$.
3. jeżeli $H = \mathbf{1}$, to działanie jest wierne, czyli $\phi : G \to \Sigma_G$ jest monomorfizmem.

Zauważmy, że ten ostatni fakt, to znane nam już **Twierdzenie Cayley'a**. Wyjaśnienie, dlaczego powyższe działanie jest uniwersalnym przykładem, poprzedzimy definicją.

4.10. Definicja. *Mówimy, że dwa G–zbiory X i Y są G–izomorficzne, jeżeli istnieje bijekcja $f : X \to Y$, taka że*

$$\forall_{x\in X}\,\forall_{g\in G} \quad f(g(x)) = g(f(x)).$$

Zauważmy, że zachodzi łatwe, ale ważne stwierdzenie:

4.11. Stwierdzenie. *Niech X będzie G–zbiorem i niech $x \in X$. Wówczas przekształcenie $f_x : G/G_x \to G(x)$, zadane wzorem*

$$f_x(gG_x) = g(x),$$

jest G–izomorfizmem G–zbiorów.

Dowód. Zauważmy, że $gG_x = g'G_x$ wtedy i tylko wtedy, gdy $g'g^{-1} \in G_x$ czyli wtedy i tylko wtedy $g'g^{-1}(x) = x$, co jest równoważne $g(x) = g'(x)$. Wynika ztego, że f_x jest dobrze określone i różnowartościowe. To, że f_x jest "na" jest oczywiste. Co więcej f_x zachowuje działanie grupy G, to znaczy $f(g(g'G_x)) = g(f(g'G_x))$ dla każdego $g \in G$ i każdej warstwy w G/G_x. □

4.12. Wniosek. *Jeżeli X jest G–zbiorem, to dla każdego $x \in X$*

$$|G(x)| = [G\colon G_x],$$

gdzie $|G(x)|$ oznacza moc orbity $G(x)$.

Podsumowując: każdy G–zbiór jest rozłączną suma orbit, a każda orbita jest G–izomorficzna z dobrze znanym G–zbiorem (postaci G/H). Jeżeli X jest skończonym G–zbiorem, to moc X jest równa sumie długości orbit rozpatrywanego działania. Uwzględniając wzór na długość orbity podany we Wniosku 4.11 możemy to stwierdzenie zapisać w postaci następującego wzoru.

4.13. Stwierdzenie. *Jeżeli X jest skończonym niepustym G–zbiorem, to*

$$|X| = [G : G_{x_1}] + [G : G_{x_2}] + \cdots + [G : G_{x_n}], \tag{4.14}$$

gdzie $G(x_1)$, $G(x_2), \ldots, G(x_n)$ są wszystkimi orbitami działania G na X.

Zanotujmy jeszcze wniosek wypływający z powyższego stwierdzenia:

4.15. Wniosek. *Jeżeli X jest skończonym G–zbiorem i $|G| = p^k$, gdzie p jest liczbą pierwszą, to*

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

Dowód. Suma długości orbit jednoelementowych jest oczywiście równa mocy zbioru punktów stałych. Z twierdzenia Lagrange'a i Wniosku 4.12 wynika zatem, że suma mocy pozostałych orbit jest podzielna przez p. □

Stwierdzenie 4.12 i Wniosek 4.13 są często używane w taki sposób, że dowodzi się iż grupa G nie może działać na zbiorze mocy n bez punktów stałych, bo liczba n nie daje się przedstawić w postaci sumy, takiej jak we wzorze (4.14), chyba że co najmniej jednym ze składników jest jedynka. Oczywiście dopuszczalne składniki muszą nie tylko być dzielnikami liczby $|G|$ ale muszą to być liczby wyrażające indeksy podgrup grupy G (wkrótce będziemy potrafili pokazać, że np. w grupie Σ_5, która jest rzędu 120, nie ma podgrupy indeksu 8, chociaż $120 = 8 \cdot 15$).

Wniosek 4.15 pozwala także na udowodnienie ważnego, a wcale nie oczywistego twierdzenia:

4.16. Twierdzenie Cauchy'ego. *Jeżeli G jest grupą skończoną i liczba pierwsza p jest dzielnikiem rzędu grupy G, to w G istnieje element rzędu p.*

Dowód. Niech $X = \{(g_1, g_2, \ldots, g_p) \in G \times G \times \cdots \times G\colon\ g_1 \cdot g_2 \cdot \ldots \cdot g_p = 1\}$. Zbiór X ma $|G|^{p-1}$ elementów, w szczególności

$$|X| \equiv 0 \pmod{p}.$$

Niech $f \in \Sigma_X$, $f(g_1, g_2, \ldots, g_p) = (g_p, g_1, g_2, \ldots, g_{p-1})$. Łatwo sprawdzić, że $o(f) = p$, a więc $\langle f \rangle \cong \mathbb{Z}_p$. Zauważmy, że

$$X^{\langle f \rangle} = \{(g, g, \ldots, g) \in G \times G \times \cdots \times G\colon\ g^p = 1\}.$$

Zgodnie z Wnioskiem 4.15

$$|X^{\langle f \rangle}| \equiv |X| \equiv 0 \pmod{p}.$$

Moc zbioru $X^{\langle f \rangle}$ jest na pewno różna od zera, bo na pewno $(1, 1, \ldots, 1) \in X^{\mathbb{Z}_p}$. Wobec faktu, że $p \,\big|\, |X^{\langle f \rangle}|$, zbiór $X^{\langle f \rangle}$ musi zawierać jeszcze co najmniej $p-1$ innych ciągów $(g, g, \ldots, g) \in X$, teraz już takich, że $g \neq 1$. Oczywiście z tego, że $g \neq 1$ i $g^p = 1$, gdzie p jest liczbą pierwszą, wynika że $o(g) = p$. □

Wróćmy do przykładu, od którego rozpoczęliśmy ten rozdział.

4.17. Przykład. Niech grupa G działa na zbiorze jej elementów przez automorfizmy wewnętrzne, $\phi : G \longrightarrow Aut(G)$. O automorfizmie wewnętrznym ϕ_g mówimy także, że jest sprzężeniem wyznaczonym przez element g. Jak się przekonamy, analiza tego działania odgrywa ważną rolę w badaniu struktury grupy i dlatego jego orbity i grupy izotropii mają odrębne nazwy:

orbitę $\{gxg^{-1} : g \in G\}$ elementu x nazywamy **klasą sprzężoności** elementu x;

grupę izotropii elementu x nazywamy **centralizatorem** elementu x w G i oznaczamy symbolem $C_G(x)$. Zatem

$$C_G(x) = \{g \in G : \, gxg^{-1} = x\},$$

a moc klasy sprzężoności elementu x jest równa $[G : C_G(x)]$.

Zbiór punktów stałych działania przez automorfizmy wewnętrzne ma już swoją nazwę — jest to **centrum** $Z(G)$ grupy G.

Jeżeli G jest grupą skończoną, to równość (4.14) występująca w Stwierdzeniu 4.13 nazywa się **równaniem klas** i przybiera postać:

$$|G| = |Z(G)| + [G : C_G(g_1)] + [G : C_G(g_2)] + \cdots + [G : C_G(g_k)], \tag{4.18}$$

gdzie $g_1, g_2, \ldots, g_k$ jest listą reprezentantów wszystkich nie jednoelementowych klas sprzężoności.

Zanotujmy ważny wniosek z równości 4.18.

4.19. Wniosek. *Jeżeli $|G| = p^k$, gdzie p jest liczbą pierwszą, $k > 0$, to centrum $Z(G)$ grupy G jest nietrywialne.*

Dowód. Z równości 3.13 wynika, że $|G| \equiv |Z(G)| \equiv 0 \pmod{p}$. Ponieważ $|Z(G)| \geq 1$ i $p \,\big|\, |Z(G)|$, to $|Z(G)| \geq p$, a więc centrum jest nietrywialne. □

4.20. Wniosek. *Jeżeli p jest liczbą pierwszą, to każda grupa G rzędu p^2 jest przemienna.*

Dowód. Mamy udowodnić, że $G = Z(G)$. Z poprzedniego wniosku wiemy, że w $Z(G)$ jest jakiś element nietrywialny x.

Jeżeli $\langle x \rangle = G$, to grupa G jest cykliczna, a więc przemienna.

Jeżeli $\langle x \rangle$ jest podgrupą właściwą, to istnieje jakiś element $y \in G$, taki że $y \notin \langle x \rangle$. Oczywiście $xy = yx$. Zatem $\langle x, y \rangle$ jest grupą przemienną. Ale $\langle x, y \rangle$, to już na pewno jest cała grupa G. □

Zastanówmy się jeszcze nad związkiem liczby klas sprzężoności grupy skończonej z jej rzędem - czy jeżeli grupa ma k klas sprzężoności, to jej rząd może być dowolnie duży? Okazuje się, że nie i że prawdziwy jest następujący fakt.

4.21. Stwierdzenie. *Dla liczby naturalnej $k \in \mathbb{N}$ istnieje liczba naturalna $B(k) \in \mathbb{N}$, taka że jeżeli grupa skończona G ma dokładnie k klas sprzężoności, to $|G| \leq B(k)$.*

Skorzystamy z łatwego lematu, którego dowód pozostawiamy czytelnikowi.

4.22. Lemat. *Dla ustalonej liczby naturalnej k i dodatniej liczby rzeczywistej a równanie*

$$\frac{1}{x_1} + \cdots + \frac{1}{x_k} = a$$

ma skończoną liczbę rozwiązań w zbiorze liczb naturalnych.

Dowód Stwierdzenia 4.21 Rozpatrzmy równanie klas:

$$|G| = [G : C_G(g_1)] + [G : C_G(g_2)] + \cdots + [G : C_G(g_k)],$$

gdzie $g_1, g_2, \ldots, g_k$ są reprezentantami wszystkich (także tych jednoelementowych) klas sprzężoności grupy G. Możemy założyć, że $g_1 = 1$. Korzystając z twierdzenia Lagrange'a i dzieląc obie strony równości przez $|G|$ otrzymujemy

$$1 = \frac{1}{|C_G(g_1)|} + \cdots + \frac{1}{|C_G(g_k)|}.$$

Ponieważ liczba rozwiązań równania $\frac{1}{x_1} + \cdots + \frac{1}{x_k} = 1$ jest skończona, to istnieje $B(k) \in \mathbb{N}$, zależne tylko od k i takie że dla każdego i, $|C_G(g_i)| \leq B(k)$. W szczególności dla $g_1 = 1$, $|C_G(g_1)| = |G| \leq B(k)$. □

Na zakończenie tych rozważań zobaczymy jak można skorzystać z wprowadzonych pojęć odpowiadając na pytanie: Czy istnieje grupa, która ma dokładnie osiem elementów rzędu 5?

Pokażemy, że nie. Przypuśćmy, że jednak istnieje. Wówczas taka grupa G ma dokładnie dwie podgrupy cykliczne rzędu 5, $H = \langle x \rangle \leqslant G$ i $K = \langle y \rangle \leqslant G$. Działanie grupy H na grupie G przez automorfizmy wewnętrzne wyznacza działanie H na zbiorze podgrup grupy G. Działanie to zachowuje dwuelementowy zbiór podgrup 5–cio elementowych. Mamy więc homomorfizm $H \to \Sigma_2$. Homomorfizm ten jest trywialny Wynika stąd, że automorfizmy wewnętrzne wyznaczone przez elementy grupy H zachowują podgrupę K, a więc grupa H działa na grupie K i mamy homomorfizm $H \to Aut(K)$. Ponieważ $|Aut(K)| = \varphi(5) = 4$, to analogiczne rozumowanie jak poprzednio dowodzi, że działanie to jest trywialne. Oznacza to w szczególności, że $xyx^{-1} = y$. Spełnione są założenia zadania 2.6, a więc $\langle x, y \rangle \cong \mathbb{Z}_5 \times \mathbb{Z}_5$. Wobec tego w grupie G są co najmniej 24 elementy rzędu 5. Dochodzimy do sprzeczności z założeniem, że jest ich dokładnie 8.

Klasy sprzężoności w grupach permutacji

Niech $\sigma = (c_1, \ldots, c_s)$ będzie pewnym cyklem, a γ pewną permutacją w Σ_n. Wówczas $\gamma\sigma\gamma^{-1} = (\gamma(c_1), \ldots, \gamma(c_s))$ — łatwo to sprawdzić w drodze bezpośredniego rachunku. Korzystając (wielokrotnie) z równości $axya^{-1} = (axa^{-1})(aya^{-1})$ otrzymujemy następujący wniosek.

4.23. Wniosek. *Dwie permutacje są sprzężone wtedy i tylko wtedy, gdy mają podobne rozkłady na iloczyn cykli rozłącznych, tzn. w obydwu rozkładach występuje po tyle samo cykli tej samej długości.*

4.24. Przykład. Permutacje (126)(347)(58)(9) i (6)(345)(29)(178) są sprzężone w Σ_9, bo mają po jednym cyklu długości jeden, po jednej transpozycji i po dwa cykle długości trzy w rozkładzie na iloczyn cykli rozłącznych.

5. Podgrupy normalne i grupy ilorazowe

Niech $\varphi : G \longrightarrow H$ będzie homomorfizmem. Rozpatrzmy zbiór warstw lewostronnych $G/\ker\varphi$ grupy G względem podgrupy $\ker\varphi$. Łatwo zauważyć, że

$$\varphi(x) = \varphi(y) \iff x^{-1}y \in \ker\varphi \iff x\ \ker\varphi = y\ \ker\varphi$$

— homomorfizm φ przeprowadza dwa elementy grupy G na ten sam element grupy H wtedy i tylko wtedy, gdy te dwa elementy wyznaczają tę samą warstwę lewostronną. Wynika stąd następujący wniosek:

5.1. Wniosek. *Jeżeli $\varphi : G \longrightarrow H$ jest homomorfizmem, to*

$$|\operatorname{im}\varphi| = [G : \ker\varphi].$$

Załóżmy teraz, że φ jest *epimorfizmem.* Wówczas $\varphi : G \longrightarrow H$ wyznacza bijekcję $\bar{\varphi} : G/\ker\varphi \longrightarrow H$ (określoną wzorem $\bar{\varphi}(x\ \ker\varphi) = \varphi(x)$) zbioru $G/\ker\varphi$ i zbioru elementów grupy H. Na zbiorze warstw $G/\ker\varphi$ można więc w naturalny sposób zdefiniować działania, tak by bijekcja $\bar{\varphi}$ stała się izomorfizmem grup. Łatwo sprawdzić, że działania te są określone następującymi wzorami:

$$\begin{aligned}(x\ \ker\varphi)\cdot(y\ \ker\varphi) &= xy\ \ker\varphi,\\ (x\ \ker\varphi)^{-1} &= x^{-1}\ \ker\varphi,\end{aligned}$$

a elementem neutralnym jest warstwa $1\ker\varphi$ (czyli po prostu $\ker\varphi$).

Uwaga. Jeżeli założymy tylko tyle, że H jest podgrupą grupy G, to wzór $xH\cdot yH = xyH$ na ogół nie ma sensu, bo warstwa występująca po prawej stronie zależy od wyboru reprezentantów warstw występujących po lewej stronie. Można się o tym przekonać rozpatrując na przykład zbiór warstw $D_6/\{1,\varepsilon\}$.

Zdefiniujemy teraz taką klasę podgrup, dla których powyższy wzór *ma* sens.

5.2. Definicja. *Podgrupę $H \leqslant G$ nazywamy* **podgrupą normalną** *(lub* **dzielnikiem normalnym***), co oznaczamy symbolem $H \trianglelefteq G$, wtedy i tylko wtedy, gdy dla każdego $g \in G$, $gHg^{-1} = \{ghg^{-1} : h \in H\} = H$, czyli dla każdego automorfizmu wewnętrznego ϕ_g grupy G zachodzi równośc $\phi_g(H) = H$.*

5.3. Uwaga. *Warunek $\forall_{g\in G}\ gHg^{-1} = H$, jest równoważny warunkowi $\forall_{g\in G}\ gHg^{-1} \subseteq H$.*

Dowód. Wystarczy przeprowadzić łatwy rachunek. Niech $h \in H$. Wówczas $h = (gg^{-1})h(gg^{-1}) = g(g^{-1}hg)g^{-1} \in gHg^{-1}$, a zatem $H \subseteq gHg^{-1}$ (a zawieranie w drugą stronę jest bezpośrednio zagwarantowane w założeniu). □

5.4. Uwaga. *Warunek $H \trianglelefteq G$ jest równoważny warunkowi $\forall_{g\in G}\ gH = Hg$, czyli równości warstw prawostronnych i lewostronnych.*

Przykłady podgrup normalnych.

5.5. Przykład. $\mathbf{1} \trianglelefteq G$, $G \trianglelefteq G$

5.6. Przykład. Jeżeli $\varphi : G \longrightarrow H$ jest homomorfizmem, to $\ker\varphi \trianglelefteq G$. Ten, jak się okaże uniwersalny, przykład ma wiele ważnych podprzykładów:

a) $Z(G) \trianglelefteq G$, gdzie $Z(G) = \ker\phi$, $\phi : G \longrightarrow Aut(G)$

b) $SO(n) \trianglelefteq O(n)$, gdzie $SO(n) = \ker det$, $det : O(n) \longrightarrow \mathbb{Z}_2$. Skonstruujemy najpierw monomorfizm $\Psi : \Sigma_n \longrightarrow GL(n, \mathbb{R})$. Wybieramy bazę uporządkowaną $e_1, \ldots, e_n$ w $\mathbb{R}^n$ i określamy $\Psi(\sigma)$ jako przekształcenie liniowe, które permutuje elementy bazy tak jak każe σ, to jest $\Psi(\sigma)(e_i) = e_{\sigma(i)}$. Wyznacznik macierzy takiego przekształcenia jest równy ± 1. Zatem mamy homomorfizm $det \circ \Psi : \Sigma_n \longrightarrow \{-1, 1\} \leqslant \mathbb{R}^*$

5.7. Definicja. *Permutację nazywamy* **permutacją parzystą**, *jeżeli należy do jądra homomorfizmu* $\det\circ\Psi$. *W przeciwnym przypadku permutację nazywamy* **permutacją nieparzystą**. *Podgrupę permutacji parzystych grupy* Σ_n *oznaczamy symbolem* A_n.

Jako jądro pewnego homomorfizmu podgrupa $A_n \leq \Sigma_n$ jest oczywiście normalna w Σ_n. Z twierdzenia o izomorfizmie wynika, że dla $n \geq 2$, $\Sigma_n/A_n \cong \mathbb{Z}_2$.

Ponadto złożenie

✓ dwóch permutacji parzystych jest permutacją parzystą,

✓ dwóch permutacji nieparzystych jest permutacją parzystą,

✓ permutacji parzystej i permutacji nieparzystej jest permutacją nieparzystą.

Zbadamy parzystość cykli. Jest jasne, że cykl długości 2, czyli transpozycja, jest permutacją nieparzystą — wynika to z algorytmu liczenia wyznacznika. Aby ocenić parzystość cyklu dowolnej długości odnotujmy najpierw następujący fakt.

5.8. Stwierdzenie. *Zachodzi równość:*

$$(a_1, a_2, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \ldots (a_1, a_3)(a_1, a_2).$$

□

5.9. Wniosek. *Cykl długości k jest permutacją parzystą jeżeli k jest liczbą nieparzystą, a permutacją nieparzystą jeżeli k jest liczbą parzystą. Jeżeli permutacja jest iloczynem cykli o długościach* $k_1, \ldots, k_s$, *to jest ona parzysta wtedy i tylko wtedy, gdy wśród liczb* $k_1, \ldots, k_s$ *jest parzyście wiele parzystych.* □

5.10. Przykład. Każda podgrupa grupy przemiennej jest normalna. (Ta własność nie charakteryzuje grup przemiennych — mają ją również niektóre grupy nieprzemienne).

5.11. Przykład. $1 \times K \trianglelefteq H \times K$ i $H \times 1 \trianglelefteq H \times K$.

5.12. Stwierdzenie. *Jeżeli* $H \leqslant G$ *i* $[G : H] = 2$, *to* $H \trianglelefteq G$.

Dowód. Oczywiście $\forall_{g\in H}\forall_{h\in H}\ ghg^{-1} \in H$. Pozostaje przypadek, gdy $g \notin H$. Przypuśćmy, że $\exists_{h\in H}\ ghg^{-1} \notin H$. Skoro tak, to $ghg^{-1} \in G \setminus H = gH$. Jak widać, elementy g i ghg^{-1} należą do tej samej warstwy (gH) względem podgrupy H. Ale to oznacza, że $g^{-1} \cdot ghg^{-1} \in H$. Po redukcji otrzymujemy $hg^{-1} \in H$, skąd $g \in H$, a to oznacza sprzeczność. □

Przykłady

a) Podgrupa obrotów $J = \{1, \rho, \ldots, \rho^{n-1}\}$ grupy dihedralnej D_{2n} jest dzielnikiem normalnym.

b) W nieprzemiennej grupie Q_8 każda podgrupa jest normalna,

Odnotujmy jeszcze następujące, łatwe do udowodnienia, własności podgrup normalnych:

1) Jeżeli $\varphi : G \longrightarrow H$ jest homomorfizmem i $N \trianglelefteq H$, to $\varphi^{-1}(N) \trianglelefteq G$
2) Jeżeli $\varphi : G \longrightarrow H$ jest epimorfizmem i $N \trianglelefteq G$, to $\varphi(N) \trianglelefteq H$.
   Jeżeli o przekształceniu φ zakładamy tylko tyle, że jest homomorfizmem, to w każdym razie możemy twierdzić, że $\varphi(N) \trianglelefteq \operatorname{im}(\varphi)$.
3) Jeżeli $N_i \trianglelefteq G$ dla $i \in I$ to $\bigcap_{i \in I} N_i \trianglelefteq G$.
4) Jeżeli $N \trianglelefteq G$ i $K \leqslant G$, to $N \cap K \trianglelefteq K$.

Wiemy, że jeżeli $K \leq H$ i $H \leq G$ to $K \leq G$. Czy jeżeli $K \trianglelefteq H$ i $H \trianglelefteq G$ to $K \trianglelefteq G$? **5.13. Przykład.** W grupie D_8, $\{1, \epsilon\} \trianglelefteq \{1, \rho^2, \epsilon, \epsilon\rho^2\}, \{1, \rho^2, \epsilon, \epsilon\rho^2\} \trianglelefteq D_8$, ale $\{1, \epsilon\}$ nie jest normalną podgrupą D_8.

5.14. Definicja. *Podgrupę $H \leqslant G$ nazywamy podgrupą* **charakterystyczną**, *co oznaczamy symbolem $H \blacktriangleleft G$, wtedy i tylko wtedy, gdy dla każdego automorfizmu $\phi \in AutG$ grupy G zachodzi równość $\phi(H) = H$.*

Przykłady

a) Dla dowolnej grupy G jej centrum $Z(G)$ jest podgrupą charakterystyczną.
b) Dla dowolnej grupy G, $\Phi(G) \blacktriangleleft G$, gdzie $\Phi(G)$ jest częścią wspólną podgrup maksymalnych.
c) Każda podgrupa grupy cyklicznej jest charakterystyczna.

5.15. Stwierdzenie. *Jeżeli $K \blacktriangleleft H$ i $H \trianglelefteq G$ to $K \trianglelefteq G$.*

Dowód jest oczywisty.

Jeżeli $H \trianglelefteq G$, to z taką parą związana jest ważna konstrukcja grupy ilorazowej.

5.16. Definicja. *Niech $H \trianglelefteq G$.* **Grupą ilorazową** *grupy G przez podgrupę normalną H nazywamy zbiór warstw G/H z warstwą $1H$ jako elementem wyróżnionym i z działaniami:*

$$xH \cdot yH = xyH$$
$$(xH)^{-1} = x^{-1}H.$$

Należy sprawdzić, że działanie jest dobrze zdefiniowane, to znaczy nie zależy od wyboru reprezentantów warstw. Niech $xH = x'H$ i $yH = y'H$. Należy pokazać, że $xyH = x'y'H$. Założyliśmy, że $x^{-1}x' \in H$ i $y^{-1}y' \in H$, a chcemy wykazać że $(xy)^{-1}x'y' \in H$. Rozpatrzmy ciąg równości:

$$(xy)^{-1}x'y' = y^{-1}x^{-1}x'y' = y^{-1}x^{-1}x'yy^{-1}y' = \left(y^{-1}(x^{-1}x')y\right)(y^{-1}y').$$

Założyliśmy, że $H \trianglelefteq G$. Zatem $y^{-1}(x^{-1}x')y \in H$. Również $y^{-1}y' \in H$. Wobec tego $(xy)^{-1}x'y' \in H$. Analogicznie sprawdzamy, że działanie jednoargumentowe jest dobrze określone. Fakt, że tak określone działania spełniają aksjomaty grupy jest oczywisty.

Odnotujmy także stwierdzenie:

5.17. Stwierdzenie. *Jeżeli $H \trianglelefteq G$, to odwzorowanie $\pi : G \longrightarrow G/H$, określone wzorem $\pi(g) = gH$ jest epimorfizmem i* $\ker \pi = H$.

Epimomorfizm π nazywamy rzutowaniem grupy G na grupę ilorazową G/H.

5.18. Przykład. Grupa ilorazowa grupy cyklicznej $G = \langle g \rangle$ przez podgrupę H jest grupą cykliczną i oczywiście $G/H = \langle gH \rangle$

Przy pomocy grupy ilorazowej możemy opisać obraz dowolnego homomorfizmu.

5.19. Twierdzenie o homomorfizmie. *Niech $\varphi : G \longrightarrow H$ będzie homomorfizmem, a $\pi : G \longrightarrow G/\ker \varphi$ rzutowaniem. Wówczas istnieje dokładnie jeden monomorfizm $\tilde{\varphi} : G/\ker \varphi \longrightarrow H$, taki że $\tilde{\varphi} \circ \pi = \varphi$. W szczególności $\tilde{\varphi} : G/\ker \varphi \longrightarrow im\,\varphi$ jest izomorfizmem.*

Dowód. Szukanym monomorfizmem jest odwzorowanie ψ, określone wzorem $\psi(g \ker \varphi) = \varphi(g)$. □

Zanotujmy jeszcze przydatny wniosek z powyższego twierdzenia.

5.20. Wniosek. *Niech $\varphi : G \longrightarrow H$ będzie epimorfizmem i niech $K \trianglelefteq H$. Wówczas*

$$G/\varphi^{-1}(K) \cong H/K.$$

Dowód. Złożenie $G \xrightarrow{\varphi} H \xrightarrow{\pi_K} H/K$ (gdzie $\pi_K : H \longrightarrow H/K$ jest rzutowaniem) jest epimorfizmem, a jego jądrem jest $\varphi^{-1}(K)$. □

Twierdzenie o izomorfizmie leży u podstaw ważnego sposobu przedstawienia grupy. Niech $G =< A >$ i niech $F(A)$ będzie grupą słów o alfabecie A. Mamy naturalny epimorfizm φ: $F(A) \to G$. Zgodnie z twierdzeniem o izomorfizmie indukuje on izomorfizm $\tilde{\varphi} : F(A)/\ker\varphi \to G$. Niech $R \subset \ker\varphi$ będzie zbiorem generatorów $\ker\varphi$ **jako podgrupy normalnej**. Wówczas przedstawienie $G = \{A \mid R\}$ nazywamy przedstawieniem grupy przy pomocy generatorów i relacji.

5.21. Przykład. Niech $G = \mathbb{Z}_n$ i niech ρ będzie generatorem G. Wówczas $F(\rho) \cong \mathbb{Z}$, generatorem jądra jest ρ^n i piszemy $\mathbb{Z}_n = \{\rho \mid \rho^n\}$ lub stosowany jest też zapis $\mathbb{Z}_n = \{\rho \mid \rho^n = 1\}$

5.22. Przykład. Niech $G = \mathbb{Z} \times \mathbb{Z}$ (w zapisie addytywnym) i niech $a = (1, 0)$, $b = (0, 1)$. Mamy $F(\{a, b\}) \to \mathbb{Z} \times \mathbb{Z}$ i przedstawienie $\mathbb{Z} \times \mathbb{Z} = \{a, b \mid aba^{-1}b^{-1} = 1\}$.

5.23. Przykład. Niech $G = D_{2n} =< \rho, \epsilon >$. Przedstawienie w postaci generatorów i relacji grupy dihedralnej : $D_{2n} = \{\rho, \epsilon \mid \rho^n = 1, \epsilon^2 = 1, \epsilon\rho\epsilon\rho = 1\}$ lub równoważnie $D_{2n} = \{\rho, \epsilon \mid \rho^n = 1, \epsilon^2 = 1, \epsilon\rho\epsilon = \rho^{n-1}\}$.

Przedstawienie grupy w postaci generatorów i relacji nie jest jednoznaczne - zależy tak od wyboru generatorów grupy, jak i generatorów jądra . Rozstrzygnięcie, czy dwie grupy przedstawione przy pomocy generatorów i relacji są izomorficzne nie jest zadaniem łatwym, podobnie jak rozstrzygnięcie czy dane słowo jest elementem trywialnym.

Wróćmy do rozważania homomorfizmów. Na początek niech $\varphi : G \longrightarrow A$ będzie homomorfizmem i niech A będzie przemienna. Wówczas $\forall_{x,y \in G}\ x^{-1}y^{-1}xy \in \ker\varphi$. Element $x^{-1}y^{-1}xy$ nazywamy **komutatorem** elementów x i y i oznaczamy symbolem $[x, y]$. **Komutantem** grupy G nazywamy podgrupę

$$[G, G] = \langle \{[x, y] : \ x, y \in G\} \rangle.$$

5.24. Stwierdzenie. *Komutant jest podgrupą charakterystyczną.*

Dowód. Niech $\phi : G \to G$ będzie dowolnym automorfizmem grupy G. Wówczas $\phi([x,y]) = [\phi(x), \phi(y)]$. Wobec tego $\phi([G,G]) = [G,G]$. □

Jest jasne, że grupa ilorazowa $G/[G,G]$ jest przemienna i że wśród podgrup normalnych grupy G podgrupa $[G,G]$ jest najmniejszą taką, że grupa ilorazowa jest przemienna. Grupę $G/[G,G]$ nazywamy **abelianizacją grupy** G. Jest to największa przemienna grupa ilorazowa grupy G. Precyzyjnie wyraża to następujące twierdzenie.

5.25. Twierdzenie. *Dla każdego homomorfizmu $\varphi : G \longrightarrow A$, gdzie A jest grupą przemienną, istnieje dokładnie jeden homomorfizm $\psi : G/[G,G] \longrightarrow A$, taki że $\psi \circ \pi = \varphi$ ($\pi : G \longrightarrow G/[G,G]$ jest rzutowaniem).*

Spróbujmy teraz znaleźć wszystkie homomorfizmy $G \longrightarrow H$, dla danych grup G i H lub przynajmniej obliczyć ile ich jest.
Umiemy to zadanie rozwiązać, gdy $G = \langle\, g \,\rangle$ jest grupą cykliczną — homomorfizm $\varphi : \langle\, g \,\rangle \longrightarrow H$ jest jednoznacznie wyznaczony przez wskazanie elementu $\varphi(g)$, takiego że $o(\varphi(g)) \,|\, o(g)$. Homomorfizmów jest więc dokładnie tyle ile elementów $h \in H$, takich że $o(h) \,|\, o(g)$.

W przypadku dowolnej grupy G zaczniemy od zbadania liczby epimorfizmów $G \longrightarrow K$ dla ustalonego K. Po pierwsze trzeba znaleźć wszystkich kandydatów na jądro takiego epimorfizmu, czyli wszystkie normalne podgrupy $N \trianglelefteq G$, takie że $G/N \cong K$. Nie ma tu żadnego algorytmu. Dwa epimorfizmy ϕ, ψ o tym samym jądrze N różnią się o automorfizm $\tilde{\phi}(\tilde{\psi})^{-1}$ grupy K — mamy bowiem $\phi = \tilde{\phi}\pi_N = \tilde{\phi}(\tilde{\psi})^{-1}\tilde{\psi}\pi_N = \tilde{\phi}(\tilde{\psi})^{-1}\psi$. Zatem liczba epimorfizmów $G \longrightarrow K$ jest równa $n_K \cdot |Aut(K)|$, gdzie n_K jest liczbą normalnych podgrup G, takich że grupa ilorazowa jest izomorficzna z K. Zanotujmy jeszcze, że $|Aut(\mathbb{Z}_n)| = \varphi(n)$.

5.26. Przykład. Niech $H \leqslant G$ będzie dowolną podgrupą. Rozpatrzymy znany nam homomorfizm $\phi : G \longrightarrow \Sigma_{G/H}$ zadany wzorem $\phi_g(xH) = gxH$, opisujący działanie G na zbiorze warstw G/H. Wówczas $\ker \phi = \bigcap_{g \in G} gHg^{-1} \leqslant H$ jest podgrupą normalną grupy G — jest to *największa ze względu na zawieranie podgrupa normalna grupy G, spośród tych, które są zawarte w H* nazywamy ją **rdzeniem** podgrupy H. Oczywiście jeżeli $H \trianglelefteq G$, to $H = \ker \phi$.

Informacja, że otrzymana podgrupa jest jądrem homomorfizmu ϕ jest użyteczna w dowodzie następującego wniosku.

5.27. Wniosek. *Niech H będzie podgrupą indeksu n w grupie skończonej G. Wówczas istnieje podgrupa normalna $N \trianglelefteq G$, $N \leq H$, taka że $n \big| [G:N]$ i $[G:N] \big| n!$ (tzn. indeks N w G jest wielokrotnością n, a dzielnikiem $n!$).*

Dowód. Szukaną grupą jest właśnie grupa $N = \ker \varphi$ opisana w przykładzie 5.26. Podzielność $n \big| [G:N]$ jest oczywista — indeks mniejszej podgrupy jest wielokrotnością indeksu większej podgrupy. Natomiast podzielność $[G:N] \big| n!$ wynika z faktu, że $|\operatorname{im} \varphi| = [G : \ker \phi] = [G:N]$ (Wniosek 5.1), z drugiej zaś strony $|\operatorname{im} \phi| \,\big|\, |\Sigma_{G/H}|$ (Twierdzenie Lagrange'a). □

5.28. Przykład. Niech $H \leqslant G$. Zdefiniujmy podgrupę

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

Oczywiście $H \leqslant N_G(H) \leqslant G$ i $H \trianglelefteq N_G(H)$. Zauważmy, że $N_G(H)$ jest *największą taką podgrupą grupy G zawierającą H, w której H jest normalna.* Jest jasne, że jeżeli $H \trianglelefteq G$, to $N_G(H) = G$. Podgrupę $N_G(H)$ nazywamy **normalizatorem** H w G.

Jeżeli rozpatrzymy działanie grupy G na zbiorze jej podgrup, zadane przez automorfizmy wewnętrzne, to $N_G(H)$ jest grupą izotropii podgrupy H, a punktami stałymi tego działania są podgrupy normalne.

Grupy proste

Grupy, które mają mało podgrup normalnych są z pewnych względów szczególnie interesujące. Wobec tego odnotujmy w tym miejscu następującą definicję.

5.29. Definicja. *Niech G będzie nietrywialną grupą. Jeżeli jedynymi podgrupami normalnymi grupy G są G i podgrupa trywialna, to mówimy, że grupa G jest* **grupą prostą**.

Oczywistym przykładem grupy prostej jest dowolna grupa $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą. Grupy $\mathbb{Z}_p$ są jedynymi przemiennymi grupami prostymi. Grupy A_n (dla $n \geq 5$) również są proste (to już jest mniej oczywiste; pokażemy to dla $n = 5$). Grupy proste są jakby "nierozkładalnymi cegiełkami, z których zbudowane są inne grupy". Skończone grupy proste zostały sklasyfikowane. Dowód twierdzenia o klasyfikacji grup prostych był jednym z największych przedsięwzięć w historii matematyki i został zakończony w kwietniu 1981 roku. Jednym z najważniejszych jego kroków było twierdzenie Feita i Thompsona, z którego wynika, że rząd skończonej nieabelowej grupy prostej jest liczbą parzystą. Dowód tego twierdzenia, opublikowany w 1963 roku w pracy *Solvability of groups of odd order,* zajmuje 225 stron.

Na zakończenie tego rozdziału udowodnimy, że A_5 jest grupą prostą.

Przypomnijmy, że w dowolnej grupie G moc klasy sprzężoności elementu x jest równa $[G : C_G(x)]$. Zauważmy, że jeżeli dla permutacji $\sigma \in A_n$ jeżeli istnieje permutacja nieparzysta $\tau \in C_{\Sigma_n}$, to klasa sprzężoności σ w A_n jest tożsama z klasą sprzężoności σ w Σ_n. W przeciwnym przypadku klasa sprzężoności σ w Σ_n rozpada się na dwie równoliczne klasy sprzężoności σ w A_n.

Zaczniemy od policzenia ile jest klas sprzężoności elementów A_5 i ile elementów liczy każda klasa. W poniższej tabeli przedstawiamy możliwe typy rozkładów na cykle, rzędy centralizatorów, moce klas sprzężoności elementów każdego typu ($conj(x)$), liczby elementów o ustalonym typie rozkładu ($sim(x)$) i liczby klas sprzężoności elementów o danym typie rozkładu.

Tabela

rozkład na cykle	$\lvert C_{A_5}(x)\rvert$	$conj(x)$	$sim(x)$	liczba klas sprzężoności
(.)(.)(.)(.)(.)	60	1	1	1
(..)(..)(.)	4	15	15	1
(...)(.)(.)	3	20	20	1
(.....)	5	12	24	2

5.30. Twierdzenie. *Grupa A_5 jest prosta.*

Dowód. Podgrupa normalna (w każdej grupie) jest zawsze sumą mnogościową pewnych klas sprzężoności — bo jeżeli pewien element należy do tej podgrupy normalnej, to już cała jego klasa sprzężoności musi być w niej zawarta. Zatem rząd podgrupy normalnej musi się dać wyrazić jako suma liczebności pewnych klas sprzężoności. W przypadku podgrupy normalnej N grupy A_5 dochodzimy do wniosku, że $|N| = 1 + b \cdot 15 + c \cdot 20 + d \cdot 12$, przy czym współczynniki b i c mogą przyjmować wartości 0 lub 1, a współczynnik d być może również 2 (bo są dwie klasy sprzężoności cykli długości 5 w grupie A_5 i być może obie są zawarte w N). Z twierdzenia Lagrange'a wiemy, że $|N| \,\big|\, 60$. Łatwo sprawdzić, że jedynymi dzielnikami liczby 60, dającymi się przedstawić w żądany sposób są 1 i 60. Zatem w A_5 nie ma podgrup normalnych innych niż sama grupa A_5 i jej podgrupa trywialna. □

6. Rozszerzenia. Produkt i produkt półprosty

Zdefiniowaliśmy pojęcie podgrupy normalnej. Jeżeli $N \trianglelefteq G$, to zdefiniowana jest grupa ilorazowa i rzutowanie $\pi : G \longrightarrow G/N$. Powstaje pytanie, do jakiego stopnia struktura grupy G jest zdeterminowana przez grupy N i G/N. Czy klasa izomorfizmu grupy G jest wyznaczona jednoznacznie przez N i G/N? Czy może jest tak przy jakichś jeszcze dodatkowych założeniach o położeniu podgrupy N w grupie G? A może przy jeszcze jakichś dodatkowych informacjach?

Przejdziemy do sytuacji, gdy grupa G *posiada* podgrupę normalną N, o której na razie nic więcej nie zakładamy. Wówczas N jest oczywiście jądrem rzutowania π grupy G na iloraz G/N. Możemy to zapisać w następującej postaci:

$$N \longrightarrow G \xrightarrow{\pi} G/N.$$

Bardziej ogólnie:

6.1. Definicja. *Mówimy, że grupa G jest* **rozszerzeniem grupy N za pośrednictwem grupy** *H, jeżeli istnieją: monomorfizm i oraz epimorfizm π, $N \xrightarrow{i} G \xrightarrow{\pi} H$, takie że* $\ker \pi = \operatorname{im} i$.

Oczywiście z twierdzenia o homomorfizmie wynika, że jeżeli grupa G jest rozszerzeniem grupy N za pośrednictwem grupy H, to H jest izomorficzna z grupą ilorazową G/N. Definicja dopuszcza możliwości $N = 1$ i $N = G$. Rozszerzenia $G \xrightarrow{id} G \longrightarrow 1$ i $1 \longrightarrow G \xrightarrow{id} G$ są jednak mało interesujące. Oczywiście grup prostych nie można w nietrywialny sposób przedstawić jako rozszerzenie. Na drugim biegunie leżą p – grupy. które można przedstawić jako kolejne rozszerzenia za pośrednictwem grupy $\mathbb{Z}_p$.

6.2. Twierdzenie. *Jeżeli G jest p-grupą i $|G| = p^m$, to istnieje ciąg podgrup*

$$\mathbf{1} = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_{m-1} \leqslant G_m = G,$$

taki że $G_i \trianglelefteq G$ i $|G_i| = p^i$.

Dowód. Zastosujemy indukcję ze względu na m. Teza jest oczywista dla $m = 0$. Załóżmy, że teza jest prawdziwa dla $m-1$, gdzie $m > 0$. Niech z będzie nietrywialnym elementem rzędu p w centrum grupy G (istnienie takiego elementu wynika z nietrywialności $Z(G)$ i z twierdzenia Cauchy'ego). Niech $G_1 = \langle z \rangle$. Oczywiście $G_1 \trianglelefteq G$, bo $G_1 \leqslant Z(G)$. Grupa G/G_1 jest rzędu p^{m-1}, zatem na mocy założenia indukcyjnego istnieje ciąg podgrup normalnych $H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{m-2} \leqslant H_{m-1} = G/G_1$. Przyjmując $G_0 = \mathbf{1}$, a dla $i \geq 1$, $G_i = \pi^{-1}(H_{i-1})$, gdzie $\pi : G \longrightarrow G/G_1$, otrzymujemy szukany ciąg podgrup grupy G. □

Jak można się spodziewać, informacja że G jest rozszerzeniem grupy N za pośrednictwem grupy H nie wystarczy do zidentyfikowania typu izomorficznego grupy G.

Przykłady

a) $\mathbb{Z}_2 \trianglelefteq \mathbb{Z}_4 \to \mathbb{Z}_2$.
b) $\mathbb{Z}_2 \trianglelefteq \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$.
c) $SO(n) \trianglelefteq O(n) \to Z_2$.

d) $\mathbb{R}^n \trianglelefteq Aff(n) \to GL(n, \mathbb{R}^n)$, gdzie $Aff(n)$ jest grupą izomorfizmów afinicznych przestrzeni $\mathbb{R}^n$.
e) Grupa $\mathbb{R}^n \trianglelefteq Iso(n) \to O(n)$, gdzie $Iso(n)$ jest grupą izometrii przestrzeni $\mathbb{R}^n$ (wyposażonej w iloczyn skalarny).
4) $A_n \trianglelefteq \Sigma_n \to \mathbb{Z}_2$
e) $J \trianglelefteq D_{2n} \to \mathbb{Z}_2$.

Dalsze rozważania poprzedzimy następującą obserwacją.

6.3. Uwaga. *Niech $N \trianglelefteq G$ i niech $K \leqslant G$. Wówczas:*
a) zbiór $K \cdot N = \{kn : k \in K, n \in N\}$ jest podgrupą. Jest to podgrupa generowana przez $K \cup N$. W szczególności $K \cdot N = N \cdot K$.
b) jeżeli dodatkowo $K \cap N = \{1\}$, to przedstawienie elementu $K \cdot N$ w postaci iloczynu $k \cdot n$, $k \in K$, $n \in N$ jest jednoznaczne.

Dowód.
a) Wystarczy sprawdzić, że działania grupowe nie wyprowadzają poza zbiór $K \cdot N$:

$$k_1 n_1 k_2 n_2 = k_1 k_2 \underbrace{k_2^{-1} n_1 k_2} n_2 = k_1 k_2 n_1' n_2 \text{ gdzie } n_1' = k_2^{-1} n_1 k_2 \in N$$

$$(kn)^{-1} = n^{-1} k^{-1} = k^{-1} \underbrace{k n^{-1} k^{-1}} = k^{-1} n' \text{ gdzie } n' = k n^{-1} k^{-1} \in N.$$

Ponieważ $K \cdot N \subset < K \cup N >$ i $K \cdot N$ jest podgrupą, to $K \cdot N = < K \cup N >$. Równość $K \cdot N = N \cdot K$ jest oczywista.
b) Jeżeli $k_1 n_1 = k_2 n_2$, to $k_2^{-1} k_1 = n_2 n_1^{-1} \in K \cap N$. Zatem $k_2^{-1} k_1 = n_2 n_1^{-1} = 1$ i $k_1 = k_2$, $n_1 = n_2$. □

Niech $N \trianglelefteq G$ i załóżmy, że podgrupa normalna jest położona w rozpatrywanej grupie w szczególnie dobry sposób, opisany w następującej definicji.

6.4. Definicja. *Niech $N \trianglelefteq G$. Podgrupę $K \leqslant G$ nazywamy* **dopełnieniem** *podgrupy N wtedy i tylko wtedy, gdy $N \cap K = 1$ i $N \cdot K = G$. Grupę G nazywamy wówczas* **produktem półprostym wewnętrznym** *podgrupy normalnej N i jej dopełnienia K.*

Odnotujmy jeszcze przydatny wniosek dla grup skończonych.

6.5. Wniosek. *Jeżeli $N \trianglelefteq G$, $K \leqslant G$, $N \cap K = 1$ i $|N| \cdot |K| = |G| < \infty$, to $NK = G$, czyli G jest produktem półprostym wewnętrznym N i K.*

Dowód. Na mocy Uwagi 6.3 b) zbiór ND ma $|N| \cdot |D| = |G|$ elementów, czyli rzeczywiście $ND = G$. □

Przypomnijmy następujące oznaczenie: φ_x jest automorfizmem wewnętrznym grupy G zadanym wzorem $\varphi_x(a) = xax^{-1}$. Jeżeli $N \trianglelefteq G$ i $K \leqslant G$ jest podgrupą, to mamy homomorfizm $\Phi : K \to Aut(N)$, który elementowi $k \in K$ przyporządkowuje element φ_k. Zauważmy, że jeżeli G jest produktem półprostym wewnętrznym N i K, to struktura grupy G jest wyznaczona przez strukturę grupy N, grupy K oraz homomorfizm $\Phi : K \to Aut(N)$:

$$n_1 k_1 n_2 k_2 = n_1 \underbrace{k_1 n_2 k_1^{-1}} k_1 k_2 = n_1 \varphi_{k_1}(n_2) k_1 k_2$$

$$(nk)^{-1} = k^{-1} n^{-1} = \underbrace{k^{-1} n^{-1} k} k^{-1} = \varphi_{k^{-1}}(n^{-1}) k^{-1}.$$

Jest oczywiste, że $\pi : G = N \cdot K \to K$ zadane wzorem $\pi(nk) = k$ jest epimorfizmem o jądrze N. Zatem produkt półprosty wewnętrzny N i K jest rozszerzeniem

$$N \trianglelefteq N \cdot K \xrightarrow{\pi} K.$$

Wśród wymienionych powyżej przykładów tylko a) czyli $\mathbb{Z}_2 \trianglelefteq \mathbb{Z}_4$ nie ma dopełnienia. Pozostałe przykłady są produktami półprostymi wewnętrznymi. Z przykładów tych wynika też, że dopełnienie nie jest wyznaczone jednoznacznie. W przykładach b) i c) dla n nieparzystego można znaleźć dopełnienie, które jest podgrupą normalną. Jeżeli *tak jest*, to jest to sytuacja już nam znana:

6.6. Definicja. *Jeżeli $M, N \trianglelefteq G$, $N \cap M = 1$ i $N \cdot M = G$, to grupę G nazywamy* **produktem prostym wewnętrznym** *podgrup N i M.*

Pojęcie produktu prostego wewnętrznego jest bardzo zbliżone do pojęcia produktu grup, zdefiniowanego w rozdziale 1.

6.7. Twierdzenie. *Jeżeli grupa G jest produktem prostym wewnętrznym podgrup $M, N \trianglelefteq G$, to G jest izomorficzna z produktem $M \times N$. Odwzorowanie $f : M \times N \to G$ zadane wzorem $f(m, n) = mn$ jest izomorfizmem.*

Dowód. Zaczniemy od wykazania, że $\forall_{x \in M} \forall_{y \in N}\ xy = yx$. Oczywiście $xy = yx \Leftrightarrow xyx^{-1}y^{-1} = 1$. Zauważmy, że

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

Ale $xyx^{-1} \in N$, bo N jest podgrupą normalną. Również $y^{-1} \in N$. Zatem

$$xyx^{-1}y^{-1} \in N. \tag{1}$$

Analogicznie, wykorzystując normalność M, pokazujemy, że

$$x(yx^{-1}y^{-1}) \in M. \tag{2}$$

Zestawiając fakty (1) i (2) wnioskujemy, że $xyx^{-1}y^{-1} \in M \cap N = \mathbf{1}$, czyli $xyx^{-1}y^{-1} = 1$, a więc istotnie $xy = yx$. Teraz już łatwo sprawdzić, że
$f((m_1, n_1)(m_2, n_2)) = f(m_1m_2, n_1n_2) = m_1m_2n_1n_2 = (m_1n_1)(m_2n_2) = f(m_1, n_1)f(m_2, n_2)$, co dowodzi, że f jest homomorfizmem. Zatem jest też izomorfizmem, bo oczywiście jest bijekcją (co wynika z Uwagi 6.3). □

Zauważmy, że dla grup skończonych mamy następujące użyteczne kryterium:

6.8. Wniosek. *Jeżeli $N \trianglelefteq G$, $D \trianglelefteq G$, $N \cap D = 1$ i $|N| \cdot |D| = |G| < \infty$, to G jest produktem prostym wewnętrznym N i D.*

Na koniec zauważmy jeszcze, że prawdziwa jest następująca:

6.9. Uwaga. *Niech $M \leqslant G$, $N \leqslant G$ i zbiór $M \cdot N = G$. Jeżeli dla każdego $x \in M$, każdego $y \in N$, $xy = yx$, to $M \trianglelefteq G$ i $N \trianglelefteq G$.*

Dowód. Niech $g \in G$. Musimy pokazać, że $gMg^{-1} \subset M$. Niech $m \in M$. Mamy $g = xy$, $x \in M$, $y \in N$. Mamy $gmg^{-1} = xymy^{-1}x^{-1}$, ale elementy z M i N są przemienne, więc $x \underbrace{ym}\, y^{-1}x^{-1} = xmx^{-1} \in M$. Dla $N \leqslant G$ rachunek jest analogiczny. □

6.10. Definicja. *Gupa G nazywa się nierozkładalna jeżeli nie jest produktem wewnętrznym swoich podgrup właściwych.*

7. Klasyfikacja skończenie generowanych grup przemiennych

W tym rozdziale zajmiemy się skończenie generowanymi grupami przemiennymi. Zgodnie z tradycją będziemy się posługiwać zapisem addytywnym. Działanie dwuargumentowe oznaczamy przez $+$ ($x+y$ zamiast $x\cdot y$), działanie jednoargumentowe przez $-$ ($-x$ zamiast x^{-1}), element neutralny przez 0 (zamiast 1), a podgrupę trywialną przez $\mathbf{0}$ (zamiast $\mathbf{1}$). Piszemy także nx zamiast x^n.
Przypomnijmy, że grupę nazywamy grupą **skończenie generowaną**, jeżeli posiada skończony zbiór generatorów. Oczywiście skończenie generowane są wszystkie grupy skończone, grupy cykliczne (w tym $\mathbb{Z}$ — grupa cykliczna nieskończona) i skończone produkty grup skończenie generowanych. Nie są grupami skończenie generowanymi na przykład grupy $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Zacznijmy od przypomnienia pewnych faktów dotyczących grup cyklicznych.

7.1. Stwierdzenie. *Grupa cykliczna nieskończona $\mathbb{Z}$ jest nierozkładalna, Każda podgrupa grupy $\mathbb{Z}$ jest postaci $m\mathbb{Z}$, gdzie $m \in \mathbb{N}\cup\{0\}$.*

7.2. Stwierdzenie. *Jeżeli p jest liczbą pierwszą, to grupa cykliczna $\mathbb{Z}_{p^k}$ jest nierozkładalna.*

7.3. Stwierdzenie. *Jeżeli $n = {p_1}^{k_1}\dots{p_m}^{k_m}$, jest rozkładem liczby n na czynniki pierwsze ($p_i \neq p_j$ dla $i \neq j$), to*

$$\mathbb{Z}_n \cong \mathbb{Z}_{{p_1}^{k_1}} \times \mathbb{Z}_{{p_2}^{k_2}} \times \dots \times \mathbb{Z}_{{p_m}^{k_m}},$$

a zatem $\mathbb{Z}_n$ rozkłada się na produkt p–grup[†] cyklicznych nierozkładalnych.

Oznaczenie: Produkt l egzemplarzy tej samej grupy H będziemy dla skrócenia zapisu oznaczać symbolem H^l. Przyjmujemy konwencję, że dla $l = 0$, H^l jest grupą trywialną.

Następujące twierdzenie rozstrzyga całkowicie problem klasyfikacji skończenie generowanych grup przemiennych.

7.4. Twierdzenie (o klasyfikacji grup przemiennych skończenie generowanych). *Każda skończenie generowana grupa przemienna jest izomorficzna ze skończonym produktem (nierozkładalnych) p–grup cyklicznych i grup izomorficznych z (nierozkładalną) grupą cykliczną nieskończoną $\mathbb{Z}$*

$$(\bigstar) \qquad (\mathbb{Z}_{{p_1}^{k_1}})^{v_1} \times (\mathbb{Z}_{{p_2}^{k_2}})^{v_2} \times \dots \times (\mathbb{Z}_{{p_n}^{k_n}})^{v_n} \times \mathbb{Z}^l,$$

gdzie ${p_1}^{k_1}, {p_2}^{k_2}, \dots, {p_n}^{k_n}$ są parami różnymi potęgami liczb pierwszych (niekoniecznie różnych), $l \in \mathbb{N}\cup\{0\}$, zaś $k_1, k_2, \dots, k_n, v_1, v_2, \dots, v_n \in \mathbb{N}\setminus\{0\}$.
Ponadto, czynniki produktu są wyznaczone jednoznacznie, z dokładnością do kolejności.

Na sformułowane powyżej **Twierdzenie o klasyfikacji** składają się dwie dość odrębne rzeczy:
1. możliwość przedstawienia grupy w postaci ($\bigstar$),

[†] sformułowanie p–grupa oznacza tutaj *grupę, której rząd jest potęgą liczby pierwszej* i tylko tyle; por. Uwaga 6.3.

2. jednoznaczność zapisu w postaci (★).

Twierdzenie to pozostawimy bez dowodu. Ograniczymy się do kilku uwag. Zaczniemy od uwagi dotyczącej jednoznaczności zapisu (★). Zobaczmy, że w dowodzie jednoznaczności można *rozdzielić* przypadek produktu p–grup cyklicznych skończonych od przypadku produktu grup cyklicznych izomorficznych z $\mathbb{Z}$. Poniższe twierdzenie wyjaśnia dokładnie sens tego sformułowania.

7.5. Twierdzenie. *Jeżeli*

$$(\mathbb{Z}_{{p_1}^{k_1}})^{v_1} \times \cdots \times (\mathbb{Z}_{{p_n}^{k_n}})^{v_n} \times \mathbb{Z}^l \cong (\mathbb{Z}_{{q_1}^{m_1}})^{w_1} \times \cdots \times (\mathbb{Z}_{{q_s}^{m_s}})^{w_s} \times \mathbb{Z}^t,$$

to

$$\mathbb{Z}^l \cong \mathbb{Z}^t$$

oraz

$$(\mathbb{Z}_{{p_1}^{k_1}})^{v_1} \times \cdots \times (\mathbb{Z}_{{p_n}^{k_n}})^{v_n} \cong (\mathbb{Z}_{{q_1}^{m_1}})^{w_1} \times \cdots \times (\mathbb{Z}_{{q_s}^{m_s}})^{w_s}.$$

Dowód. Niech $S(G)$ będzie podgrupą grupy przemiennej G złożoną ze wszystkich elementów skończonego rzędu (dla grupy przemiennej jest to istotnie podgrupa). Jeżeli $G_1 \cong G_2$, to oczywiście

$$\checkmark \qquad S(G_1) \cong S(G_2),$$
$$\checkmark\checkmark \qquad G_1/S(G_1) \cong G_2/S(G_2).$$

Stąd natychmiast wynika, że

$$\underline{\checkmark} \qquad (\mathbb{Z}_{{p_1}^{k_1}})^{v_1} \times \cdots \times (\mathbb{Z}_{{p_n}^{k_n}})^{v_n} \cong (\mathbb{Z}_{{q_1}^{m_1}})^{w_1} \times \cdots \times (\mathbb{Z}_{{q_s}^{m_s}})^{w_s},$$
$$\underline{\checkmark}\,\underline{\checkmark} \qquad \mathbb{Z}^l \cong \mathbb{Z}^t.$$

□

Przypadek produktu grup cyklicznych izomorficznych z $\mathbb{Z}$ jest bardzo prosty:

7.6. Twierdzenie. *Grupy $\mathbb{Z}^l$ i $\mathbb{Z}^t$ są izomorficzne wtedy i tylko wtedy, gdy $l = t$.*

Dowód. Zauważmy, że dla dowolnej grupy przemiennej G, zbiór $2G = \{2g\colon\ g \in G\}$ jest podgrupą. Ponadto, jeżeli $\varphi : G \to H$ jest izomorfizmem, to $\varphi|_{2G} : 2G \to 2H$ i $\tilde{\varphi} : G/2G \to H/2H$ są izomorfizmami.
Oczywiście $\mathbb{Z}^i/2\mathbb{Z}^i \cong (\mathbb{Z}_2)^i$. Zatem, jeżeli $\mathbb{Z}^l \cong \mathbb{Z}^t$, to $(\mathbb{Z}_2)^l \cong (\mathbb{Z}_2)^t$, a wobec tego $l = t$ (bo już sam warunek równoliczności grup $(\mathbb{Z}_2)^l$ i $(\mathbb{Z}_2)^t$ implikuje $l = t$). □

Przypadek produktu p–grup cyklicznych skończonych nietrudno zredukować do sytuacji, gdy rzędy rozpatrywanych p–grup są potęgami *jednej* ustalonej liczby pierwszej p. i posłużyć się indukcją.

Przechodzimy do uwag dotyczących *możliwości przedstawienia grupy w postaci* (★).
Zauważmy, że na mocy Twierdzenia 7.3 wystarczy udowodnić, że prawdziwe jest następujące twierdzenie.

7.7. Twierdzenie. *Każda skończenie generowana grupa abelowa jest izomorficzna z produktem skończonej liczby grup cyklicznych.*

NastEpujący fakt przyjmijmy na wiarę.

7.8. Lemat. *Jeżeli $H \leqslant \mathbb{Z}^n$, to H jest grupą skończenie generowaną.*

Oznaczenie. Wyróżnijmy w $\mathbb{Z}^n$ wygodny układ generatorów $x_1, \ldots, x_n$ gdzie $x_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (wszystkie współrzędne z wyjątkiem i–tej równe 0).

7.9. Stwierdzenie. *Niech $a_1, \ldots, a_n$ będą dowolnymi elementami przemiennej grupy H. Wówczas istnieje dokładnie jeden homomorfizm $f : \mathbb{Z}^n \longrightarrow H$, taki że $f(x_i) = a_i$ dla $i = 1, \ldots, n$.*

Dowód. Bezpośrednie sprawdzenie. □

7.10. Przykład. Dla dowolnych $1 \leq i, j \leq n,\ i \neq j,\ c \in \mathbb{Z}$ istnieje automorfizm f grupy $\mathbb{Z}^n$, zadany wzorem

$$f(x_k) = \begin{cases} x_k & k \neq j \\ cx_i + x_j & k = j \end{cases}.$$

Stwierdzenie 7.9 gwarantuje istnienie *homomorfizmu* zadanego na generatorach w taki właśnie sposób. O tym, że jest to *automorfizm* przekonujemy się sprawdzając, że istnieje homomorfizm odwrotny f^{-1}, zadany wzorem

$$f^{-1}(x_k) = \begin{cases} x_k & k \neq j \\ -cx_i + x_j & k = j \end{cases}.$$

7.11. Wniosek. *Każda grupa przemienna skończenie generowana jest obrazem homomorficznym pewnej grupy $\mathbb{Z}^n$.*
Zatem każda grupa przemienna skończenie generowana da się przedstawić w postaci $\mathbb{Z}^n/N$, gdzie $N \leqslant \mathbb{Z}^n$. □

Na mocy Lematu 7.8 podgrupa N grupy $\mathbb{Z}^n$ jest zadana przez podanie skończonego układu generatorów. Każdy z tych generatorów można zapisać w postaci wektora $(a_1, \ldots, a_n)$. Zapisując je jeden pod drugim otrzymamy macierz A. Będziemy używać naturalnego i wygodnego zapisu $\mathbb{Z}^n/A$ na oznaczenie ilorazu grupy $\mathbb{Z}^n$ przez podgrupę generowaną przez wiersze macierzy A.

7.12. Przykład. Niech $A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ Wówczas $\mathbb{Z}^3/A \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbf{0} \cong \mathbb{Z}_3 \times \mathbb{Z}_2$.

Powyższy przykład jest oczywiście bardzo szczególny — rozpatrujemy macierz diagonalną, co pozwala na łatwe zidentyfikowanie grupy ilorazowej, w postaci takiej, jakiej oczekujemy (tzn. w postaci produktu grup cyklicznych). Odnotujmy oczywiste stwierdzenie ogólne.

7.13. Stwierdzenie. *Jeżeli A jest macierzą diagonalną o wyrazach $a_1, \ldots, a_n$ na przekątnej, to $\mathbb{Z}^n/A$ jest izomorficzne z produktem grup $\mathbb{Z}_{a_i}$ (stosujemy tu konwencję, że $\mathbb{Z}_1 = \mathbf{0}$, $\mathbb{Z}_0 = \mathbb{Z}$).*

Ustaliliśmy, że rozpatrywana grupa przemienna skończenie generowana jest postaci $\mathbb{Z}^n/A$. Chcemy teraz pokazać, że macierz A może być zastąpiona macierzą diagonalną. Jest to możliwe dzięki następującemu lematowi.

7.14. Lemat. *Następujące operacje na macierzy A nie zmieniają klasy izomorfizmu grupy ilorazowej:*
(a) Zamiana dwóch wierszy (albo kolumn) miejscami
(b) Pomnożenie wiersza (lub kolumny) przez -1
(c) Dodanie do i–tego wiersza (kolumny) wielokrotności j–tego wiersza (kolumny), dla $i \neq j$.
(d) Usunięcie/dodanie wiersza zerowego.

Dowód. Dopuszczalność operacji na wierszach jest we wszystkich czterech przypadkach oczywista — wiersze zmodyfikowanej macierzy opisują dokładnie tę samą podgrupę. W przypadku operacji kolumnowych ((a),(b),(c)) wyjaśnienie jest nieco bardziej skomplikowane. Na przykład dla operacji typu (c): rozpatrywaliśmy automorfizm f grupy $\mathbb{Z}^n$, zadany wzorem

$$f(x_k) = \begin{cases} x_k & k \neq j \\ cx_i + x_j & k = j \end{cases} .$$

Jest jasne, że $\mathbb{Z}^n/N \cong \mathbb{Z}^n/f(N)$. Łatwo sprawdzić, że macierz opisująca podgrupę $f(N)$ to właśnie zmodyfikowana macierz A (do j–tej kolumny dodano i–tą kolumnę pomnożoną przez stałą c). □

Pozostaje pokazać, że dopuszczalne operacje pozwalają od dowolnej macierzy przejść do macierzy diagonalnej.

7.15. Lemat. *Każdą macierz całkowitoliczbową można za pomocą operacji (a)–(d) sprowadzić do postaci diagonalnej.*

Dowód (a zarazem opis algorytmu).
Szukamy w macierzy A niezerowego wyrazu c o najmniejszej wartości bezwzględnej. Jeżeli się da, to dodajemy odpowiednio dobraną wielokrotność jego wiersza lub kolumny do innego odpowiednio dobranego wiersza (kolumny), tak aby uzyskać wyraz niezerowy o mniejszej wartości bezwzględnej.
Jeżeli się *nie da*, to oznacza to, że wszystkie wyrazy w kolumnie i wierszu wyrazu c są podzielne przez c. Wówczas dodając wielokrotności wiersza i kolumny wyrazu c do pozostałych wierszy i kolumn doprowadzamy do takiej sytuacji, że w wierszu i kolumnie wyrazu c są same zera (poza wyrazem c.)
Przestawiając wiersze i kolumny doprowadzamy do tego, żeby wyraz c znalazł się w lewym górnym rogu.
Powtarzamy całą procedurą dla mniejszej macierzy, powstałej przez skreślenie pierwszego wiersza i kolumny. Tak naprawdę pracujemy dalej z tą dużą macierzą, tylko że pierwszy wierszy i kolumna nie podlegają już żadnym modyfikacjom. Ostatecznie otrzymujemy macierz diagonalną (być może konieczne będzie dopisanie lub usunięcie pewnej liczby wierszy zerowych), co kończy dowód lematu. □
Kończy to także dowód *możliwości przedstawienia grupy w postaci* (★).

Warto jeszcze wspomnieć o często stosowanej notacji dotyczącej grup przemiennych skończenie generowanych.
7.16. Przykład. Zapis: grupa przemienna G zadana przez generatory i relacje

$$\langle\, x, y, z, w \mid x + 2y - 2z = 0,\ 2x - 5y = 0,\ 3x = 0 \,\rangle$$

lub krócej

$$\langle\, x, y, z, w \mid x + 2y - 2z,\ 2x - 5y,\ 3x \,\rangle$$

jest równoważny naszemu zapisowi $G = \mathbb{Z}^3/A$, gdzie $A = \begin{pmatrix} 1 & 2 & -2 & 0 \\ 2 & -5 & 0 & 0 \\ 3 & 0 & 0 & 0 \end{pmatrix}$.

Zobaczmy, co to za grupa. Przekształcamy macierz A w podany poniżej sposób:

$$\begin{pmatrix} 1 & 2 & -2 & 0 \\ 2 & -5 & 0 & 0 \\ 3 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & -2 & 0 \\ 0 & -9 & 4 & 0 \\ 0 & -6 & 6 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -9 & 4 & 0 \\ 0 & -6 & 6 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 4 & 0 \\ 0 & 6 & 6 & 0 \end{pmatrix} \to$$

$$\to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 4 & 0 \\ 0 & 0 & 30 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 30 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 30 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 30 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Jak widać $\mathbb{Z}^4/A \cong Z_1 \times \mathbb{Z}_1 \times \mathbb{Z}_{30} \times \mathbb{Z}_0 = \mathbf{0} \times \mathbf{0} \times \mathbb{Z}_{30} \times \mathbb{Z} = \mathbb{Z}_{30} \times \mathbb{Z} = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}$.

Twierdzenie Sylowa

Przytoczymy teraz twierdzenie Sylowa, na które można patrzeć jak na odwrócenie twierdzenia Lagrange'a dla pewnych dzielników rzędu grupy. Jeżeli G jest grupą rzędu n i $n = {p_1}^{k_1} \dots {p_s}^{k_s}$ jest przedstawieniem n w postaci iloczynu potęg różnych liczb pierwszych, to twierdzenie Sylowa mówi, że dla każdego p_i istnieje w G podgrupa rzędu ${p_i}^{k_i}$ i podaje ograniczenia na liczbę takich podgrup.

7.17. Definicja. *Niech $|G| = p^k \cdot r$, gdzie p jest liczbą pierwszą i $(p, r) = 1$. Podgrupę $H \leqslant G$ nazywamy p–**podgrupą Sylowa** grupy G jeżeli $|H| = p^k$.*

7.18. Twierdzenie Sylowa. *Niech $|G| = p^k \cdot r$, gdzie p jest liczbą pierwszą i $(p, r) = 1$. Wówczas:*

a) Istnieje p–podgrupa Sylowa w G.

b) Jeżeli H jest p–podgrupą Sylowa w G, a $K \leqslant G$ dowolną p-podgrupą, to istnieje element $g \in G$ dla którego $K \leqslant gHg^{-1}$. W szczególności, każda p–podgrupa grupy G jest zawarta w pewnej p–podgrupie Sylowa.

c) Każde dwie p–podgrupy Sylowa są sprzężone.

d) Jeżeli s_p oznacza liczbę p–podgrup Sylowa grupy G, to $s_p \mid r$ i $s_p \equiv 1 \pmod{p}$.

TEORIA PIERŚCIENI

8. Własności elementów pierścienia

Przypominamy, że przez pierścień rozumiemy pierścień przeminenny z 1.

8.1. Definicja. *Niech R będzie pierścieniem, zaś $A \subseteq R$ dowolnym podzbiorem. Podpierścieniem pierścienia R generowanym przez A nazywamy najmniejszy podpierścień zawierający zbiór A. Oznaczamy go symbolem $\langle A \rangle$.*

Jest jasne, że część wspólna podpierścieni pierścienia R jest podpierscieniem, zatem podpierścień generowany przez A istnieje i jest nim część wspólna wszystkich podpierścieni R zawierających zbiór A. Jest także jasne, ze $\langle A \rangle = \langle A \cup \{1\} \rangle$.

8.2. Przykład. Niech $d \in \mathbb{Z}$ będzie liczbą całkowitą, $d \neq 1$, która nie jest podzielna przez kwadrat liczby naturalnej różnej od 1 — taką liczbę nazywamy bezkwadratową. Oznaczmy przez $\mathbb{Z}[\sqrt{d}]$ podpierścień ciała liczb zespolonych generowany przez $\sqrt{d}$ — jego elementami są liczby postaci $a + b\sqrt{d}$, $a, b \in \mathbb{Z}$.
Zbiór liczb tej postaci jest podpierścieniem również wtedy, gdy opuścimy założenie, że liczba d jest bezkwadratowa, jednak przykłady spełniające to założenie będą dla nas bardziej interesujące.

8.3. Definicja. *Element $x \in R$ nazywamy* **dzielnikiem zera** *wtedy i tylko wtedy, gdy istnieje element niezerowy $y \in R$, dla którego $xy = 0$.*
Element $x \in R$ nazywamy **odwracalnym** *wtedy i tylko wtedy, gdy istnieje element $y \in R$, zwany* **odwrotnością** *elementu x, dla którego $xy = 1$.*
Element $x \in R$ nazywamy **nilpotentnym** *jeżeli istnieje liczba całkowita dodatnia n, dla której $x^n = 0$.*

8.4. Uwaga. W pierścieniu niezerowym 0 *jest* dzielnikiem zera. W każdym pierścieniu 0 jest elementem nilpotentnym.
8.5. Uwaga. Można skracać przez elementy, które nie są dzielnikami zera, to znaczy: jeżeli x nie jest dzielnikiem zera i $xy = xz$ to $y = z$.
8.6. Uwaga. Element odwracalny nie jest dzielnikiem zera. Jego odwrotność jest wyznaczona jednoznacznie. Zbiór elementów odwracalnych, z jedynką jako elementem neutralnym, jest grupą ze względu na mnożenie.
8.7. Przykład. W pierścieniu $\mathbb{Z}_n$ dzielnikami zera są te liczby k, dla których $(k, n) > 1$. Pozostałe elementy są odwracalne.

Ten ostatni przykład łatwo uogólnić do następującego stwierdzenia.

8.8. Stwierdzenie. *W pierścieniu skończonym, element nie będący dzielnikiem zera jest odwracalny.*

Dowód. Niech $0, x_1, \ldots, x_n$ będzie listą elementów rozpatrywanego pierścienia. Rozpatrzmy element x, który nie jest dzielnikiem zera. Z założenia o elemencie x i Uwagi 8.5 wynika, że iloczyny $xx_1, \ldots, xx_n$ są parami różne i że żaden z nich nie jest zerem. Zatem rozpatrywane iloczyny, to wszystkie niezerowe elementy pierścienia. Wobec tego któryś z nich jest jedynką, czyli istotnie x jest odwracalny. □

8.9. Definicja. *Niezerowy pierścień przemienny z jedynką, który nie ma niezerowych dzielników zera, nazywamy* **dziedziną całkowitości**, *albo po prostu* **dziedziną**.

Z Uwagi 8.5 i ze Stwierdzenia 8.8 natychmiast wynikają następujące fakty.

8.10. Stwierdzenie. *W dziedzinie całkowitości obowiązuje prawo skracania (przez elementy niezerowe) dla mnożenia.*

8.11. Stwierdzenie. *Skończona dziedzina całkowitości jest ciałem.*

9. Homomorfizmy i ideały.

Niech $\varphi : R \to P$ będzie homomorfizmem.

9.1. Definicja. *Jądrem homomorfizmu $\varphi : R \to P$ nazywamy zbiór*

$$ker\,\varphi = \{x \in R\colon \varphi(x) = 0\}.$$

Jądro homomorfizmu ma następujące własności:
a) jest podgrupą grupy addytywnej pierścienia R
b) $\forall_{x\in R}\forall_{a\in ker\,\varphi}\ a \cdot x \in ker\,\varphi$.

9.2. Definicja. **Ideałem** *pierścienia R nazywamy taką podgrupę I grupy addytywnej tego pierścienia, która spełnia warunek:*
$\forall_{x\in R\ a\in I}\ a \cdot x \in I$.
Używamy oznaczenia $I \trianglelefteq R$.

9.3. Przykłady.
1) Jądro dowolnego homomorfizmu jest ideałem.
2) $\{0\} \trianglelefteq R$ jest ideałem, który nazywamy ideałem zerowym.
3) Dla elementu $a \in R$ zbiór $\{ax \mid x \in R\}$ jest ideałem. Ideał ten oznaczamy symbolem (a).
3) W pierścieniu liczb całkowitych $\mathbb{Z}$, podgrupy grupy addytywnej są postaci, $n\mathbb{Z}$, dla pewnego $n \in \mathbb{N}$. Każda z nich jest ideałem, gdyż jest jądrem homomorfizmu $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(x) = x \pmod n$.
4) $R \trianglelefteq R$ — ten ideał nazywamy niewłaściwym. Jest on jądrem homomorfizmu trywialnego w pierścień zerowy.

Ideał nazywamy **właściwym**, jeżeli jest różny od całego pierścienia. Odnotujmy przydatne, choć oczywiste, stwierdzenie:

9.4. Stwierdzenie. *Ideał jest właściwy wtedy i tylko wtedy, gdy nie zawiera* 1.

Dowód. Jeżeli ideał zawiera 1, to $\forall_{x\in R}\ x \cdot 1 = x \in I$, czyli $I = R$. □
Wobec powyższego, ideał właściwy nie jest podpierścieniem pierścienia przemiennego z jedynką.

Używając pojęcia ideału można podać wygodną charakteryzację tych pierścieni, które są ciałami.

9.5. Stwierdzenie. *Pierścień jest ciałem wtedy i tylko wtedy, gdy jest niezerowy i jedynymi jego ideałami są ideał zerowy i cały pierścień.*

Dowód. $\Rightarrow$ Jeżeli $\{0\} \neq I \trianglelefteq R$, to istnieje $x \neq 0$, $x \in I$. Wówczas $x \cdot x^{-1} = 1 \in I$, zatem $I = R$.
$\Leftarrow$ Jeżeli $x \neq 0$, to $\{0\} \neq (x)$, więc $(x) = R$ i $1 \in (x)$ — co oznacza, że istnieje y, dla którego $xy = 1$. □

Odnotujmy jeszcze następujące, łatwe do udowodnienia, własności ideałów (analogiczne do odpowiednich własności podgrup normalnych):
1) Jeżeli $\varphi : R \longrightarrow P$ jest homomorfizmem i $J \trianglelefteq P$, to $\varphi^{-1}(J) \trianglelefteq R$.
2) Jeżeli $\varphi : R \longrightarrow P$ jest epimorfizmem i $I \trianglelefteq R$, to $\varphi(I) \trianglelefteq P$.
Jeżeli o przekształceniu φ zakładamy tylko tyle, że jest homomorfizmem, to w każdym razie możemy twierdzić, że $\varphi(I) \trianglelefteq \mathrm{im}\,(\varphi)$.

3) Jeżeli $I_k \trianglelefteq R$ dla $k \in K$ to $\bigcap_{k\in K} I_k \trianglelefteq R$.

Pierścień ilorazowy

Niech $I \trianglelefteq R$ będzie ideałem.

9.6. Definicja. *Niech $I \trianglelefteq R$ będzie ideałem. Wówczas* **pierścieniem ilorazowym** *nazywamy zbiór warstw R/I z działaniami:*

$$(x+I)+(y+I) = (x+y)+I$$
$$(x+I)\cdot(y+I) = x\cdot y + I$$
$$-(x+I) = -x+I$$

i warstwami: $1+I$ jako jedynką, I jako zerem.
Przekształcenie $\pi : R \to R/I$ zadane wzorem $\pi(x) = x+I$ jest epimorfizmem, $ker\,\pi = I$.

9.7. Uwaga Należy sprawdzić, że powyższa definicja jest dobra - to znaczy, że działania są dobrze określone (nie zależą od wyboru reprezentantów warstw) i spełniają aksjomaty pierścienia przemiennego z 1. To, że ideał jest podgrupą przemiennej grupy addytywnej pierścienia zapewnia poprawność dodawania warstw, zaś to że ideał jest "pułapką" na mnożenie poprawność mnożenia warstw. Spełnienie aksjomatów jest oczywiste.

Konstrukcja pierścienia ilorazowego pozwala na analizę homomorfizmów.

9.8. Twierdzenie o homomorfizmie. *Jeżeli $\varphi : R \to P$ jest homomorfizmem, to istnieje dokładnie jeden homomorfizm $\tilde{\varphi} : R/ker\,\varphi \to P$, taki że $\varphi = \tilde{\varphi}\circ\pi$, gdzie $\pi : R \to R/ker\,\varphi$. Homomorfizm $\tilde{\varphi} : R/ker\,\varphi \to \varphi(R)$ jest izomorfizmem i istnieje wzajemnie jednoznaczna odpowiedniość między ideałami pierścienia $\varphi(R)$ a ideałami R zawierającymi $ker\,\varphi$.*

Dowód. Szukanym homomorfizmem jest $\tilde{\varphi}(x+ker\,\varphi) = \varphi(x)$. Sprawdzenia wymaga tylko to, że $\tilde{\varphi}$ jest dobrze określone. □

9.9. Przykład. Rozpatrzmy homomorfizm $\varphi : \mathbb{Z}[X] \to \mathbb{C}$, $\varphi(X) = \sqrt{d}$, gdzie d jest liczba bezkwadratową. Jego jądro $\ker\varphi = \{f \in \mathbb{Z}[X]\colon f(\sqrt{d}) = 0\}$. Wyłączając $X^2 - d$ przed nawias możemy dowolny wielomian przedstawić w postaci $f = (x^2 - d)g + aX + b$. Zatem $\ker\varphi = \{(X^2-d)f, f \in \mathbb{Z}[X]\}$. Jest jasne, że $\mathrm{im}\,\varphi = \mathbb{Z}[\sqrt{d}]$ a więc $\mathbb{Z}[X]/(X^2-d) \cong \mathbb{Z}[\sqrt{d}]$.

Wróćmy do własności ideałów. Z faktu, że część wspólna rodziny ideałów jest ideałem, wynika, że dla każdego podzbioru $A \subseteq R$ istnieje najmniejszy ze względu na zawieranie ideał pierścienia R zawierający zbiór A — oznacza się go przez (A) i nazywa **ideałem generowanym** przez A. Nietrudno znaleźć postać elementów ideału (A).

9.10. Stwierdzenie. *Jeżeli $A \subseteq R$, $A \neq \emptyset$, to*

$$(A) = \{a_1x_1 + \cdots + a_jx_j : j \in \mathbb{N},\ a_i \in A,\ x_i \in R\}.$$

Dowód. Łatwo sprawdzić, że każdy ideał zawierający zbiór A zawiera powyższy zbiór i że zbiór ten *jest* ideałem. □

9.11. Przykład. Jeżeli $i \trianglelefteq R$ oraz $J \trianglelefteq R$ to zgodnie z powyższym stwierdzeniem $(I \cup J) = \{x+y\colon x \in I,\ y \in J\}$. Ideał ten będziemy więc nazywali suma ideałów I i J oznaczając go symbolem $I + J$.

9.12. Definicja. *Ideał $I \trianglelefteq R$ nazywamy* **ideałem głównym** *wtedy i tylko wtedy, gdy istnieje element $a \in R$, taki że $I = (a) = \{ax : x \in R\}$.*

9.13. Stwierdzenie. *W pierścieniu $\mathbb{Z}$ i w pierścieniu $k[X]$ (wielomianów nad ciałem k każdy ideał jest główny.*

Dowód. Dla niezerowego ideału w pierścieniu $\mathbb{Z}$ generatorem jest liczba całkowita o najmniejszym module spośród liczb różnych od zera należących do ideału. W przypadku pierścienia wielomianów należy wziąć wielomian najmniejszego stopnia spośród niezerowych wielomianów należących do ideału. □

Powyższa własność jest na tyle istotna, że wyodrębnia się klasę pierścieni,które ją posiadają.

9.14. Definicja. *Dziedzinę całkowitości nazywamy* **dziedziną ideałów głównych** *wtedy i tylko wtedy, gdy każdy jej ideał jest główny.*

W zależności od własności pierścienia ilorazowego będziemy wyróżniać pewne ideały.

9.15. Definicja. *Ideał $I \trianglelefteq R$ nazywamy* **ideałem pierwszym** *wtedy i tylko wtedy, gdy R/I jest dziedziną całkowitości.*
Ideał $I \trianglelefteq R$ nazywamy **ideałem maksymalnym** *wtedy i tylko wtedy, gdy R/I jest ciałem.*

9.16. Uwaga. *W pierścieniu R ideał zerowy jest pierwszy wtedy i tylko wtedy, gdy R jest dziedziną całkowitości.*

Zauważmy, że ideały pierwsze i maksymalne są z definicji ideałami właściwymi. Oczywiście, każdy ideał maksymalny jest pierwszy.

Podamy warunki równoważne tym z definicji i wówczas będzie widać dlaczego używa się nazw — pierwszy i maksymalny.

9.17. Stwierdzenie. *Ideał $I \trianglelefteq R$ jest pierwszy wtedy i tylko wtedy, gdy $I \neq R$ oraz dla dowolnych $x, y \in R$, jeżeli $xy \in I$, to $x \in I$ lub $y \in I$.*
Ideał $I \trianglelefteq R$ jest maksymalny wtedy i tylko wtedy, gdy jest elementem maksymalnym, ze względu na zawieranie, w zbiorze właściwych ideałów R (oznacza to, że $I \neq R$ oraz jeżeli $J \trianglelefteq R$ i $I \subseteq J$, to $I = J$ lub $J = R$).

Dowód. W obydwu wypadkach możemy ograniczyć rozważania do sytuacji, gdy I jest ideałem właściwym. W przeciwnym razie iloraz jest pierścieniem zerowym, a więc nie jest ani dziedziną całkowitości, ani ciałem. Zakładamy zatem, że $I \neq R$.

Pierścień R/I jest dziedziną całkowitości wtedy i tylko wtedy, gdy z równości $(x + I) \cdot (y + I) = xy + I = 0 + I$ wynika, że $(x + I = 0 + I \ \vee \ y + I = 0 + I)$,
a zatem wtedy i tylko wtedy, gdy z $xy \in I$ wynika, że $(x \in I \ \vee \ y \in I)$.

Pierścień R/I jest ciałem wtedy i tylko wtedy, gdy jego jedynymi ideałami są ideał zerowy oraz cały pierścień R/I, a zatem (wobec wzajemnie jednoznacznej odpowiedniości między ideałami pierścienia ilorazowego R/I a ideałami pierścienia R zawierającymi I) wtedy i tylko wtedy, gdy z $I \subseteq J \trianglelefteq R$ wynika $(I = J \vee J = R)$.
□

9.18. Twierdzenie. *Każdy ideał właściwy I jest zawarty w pewnym ideale maksymalnym.*

Dowód. Rozpatrzmy zbiór ideałów właściwych zawierających I, z częściowym porządkiem wyznaczonym przez zawieranie. Łańcuchami† są wówczas wstępujące rodziny ideałów. Każdy łańcuch ma zatem ograniczenie górne, bo suma wstępującej rodziny ideałów właściwych jest ideałem właściwym (nie zawiera jedynki, bo nie zawiera jej żaden z sumowanych składników). Na mocy lematu Zorna w zbiorze tym istnieje więc element maksymalny. □

9.19. Wniosek. *Każdy niezerowy pierścień można odwzorować epimorficznie na pewne ciało.* □

9.20. Przykłady.

1) Niech X będzie przestrzenią topologiczną, a $C(X)$ pierścieniem funkcji ciągłych o wartościach rzeczywistych. Niech $x_0 \in X$. Ideał $\{f\colon f(x_0) = 0\} = I_{x_0}$ jest jądrem epimorfizmu $\phi : C(X) \to R$, określonego wzorem $\phi_f(x_0) = f(x_0)$, a więc jest maksymalny.

Następne dwa przykłady ilustrują ważną metodę otrzymywania interesujących ciał jako pierścieni ilorazowych pierścienia wielomianów nad ciałem.

2) Ideał $(x^2 + 1) \trianglelefteq \mathbb{R}[X]$ jest maksymalny, i $\mathbb{R}[X]/(x^2 + 1) \cong \mathbb{C}$. Izomorfizm jest wyznaczony przez przyporządkowanie warstwie $x + (x^2 + 1)$ liczby i.
3) Łatwo sprawdzić, że $\mathbb{Z}_2[X]/(X^2 + X + 1)$ jest ciałem o czterech elementach, więc ideał $(X^2 + X + 1)$ jest maksymalny.
1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ jest pierścieniem skończonym. Zatem ideał główny (n) jest maksymalny wtedy i tylko wtedy, gdy jest pierwszy, a więc wtedy i tylko wtedy, gdy n jest liczbą pierwszą.

   Własność ta przysługuje dziedzinom ideałów głównych.

9.21. Twierdzenie. *Jeżeli pierścień jest dziedziną całkowitości, to w zbiorze właściwych ideałów głównych ideały pierwsze różne od zerowego, są maksymalne ze względu na zawieranie.*

Dowód. Niech $I = (a)$, $a \neq 0$ będzie ideałem pierwszym i niech $I \subseteq J$, gdzie $J = (b)$. Zatem $a = bc$ i z tego, że ideał I jest pierwszy wynika, że $b \in I$ lub $c \in I$.

W pierwszym przypadku $(b) \subseteq I$, co dowodzi równości $(a) = I = J = (b)$.

Jeżeli $c \in I$, to $c = ad$, więc $a = bad$ i $a(bd - 1) = 0$. Pierścień R jest dziedziną, $a \neq 0$, więc $bd = 1 \in J$ i $J = R$. □

Jako wniosek otrzymujemy następujące ważne twierdzenie.

9.22. Twierdzenie. *W dziedzinie ideałów głównych każdy niezerowy ideał pierwszy jest maksymalny.*

Twierdzenie chińskie o resztach.

Ustalenie z jakim pierścieniem jest izomorficzny dany pierścień ilorazowy bywa trudne. W wielu sytuacjach w sukurs przychodzi "chińskie twierdzenie o resztach." Zacznijmy od definicji:

9.23. Definicja. *Ideały $I_1 \trianglelefteq R$, $I_2 \trianglelefteq R$ nazywamy względnie pierwszymi wtedy i tylko wtedy, gdy $I_1 + I_2 = R$.*

Zauważmy, że ideały $I_1 \trianglelefteq R$, $I_2 \trianglelefteq R$ są względnie pierwsze jeżeli istnieją elementy $x \in I_1$, $y \in I_2$, dla których $x + y = 1$.

† tzn. podzbiorami liniowo uporządkowanymi.

9.24. Twierdzenie chińskie o resztach. *Niech $I_1, \ldots, I_n$ będą parami względnie pierwszymi ideałami pierścienia R. Niech*

$$\varphi : R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

będzie homomorfizmem danym wzorem:

$$\varphi(x) = (x + I_1, x + I_2, \ldots, x + I_n).$$

Wówczas:
a) homomorfizm φ jest epimorfizmem.
b) $\ker \varphi = I_1 \cap I_2 \cap \cdots \cap I_n$
Zatem:

$$R/(I_1 \cap I_2 \cap \cdots \cap I_n) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n.$$

Zanim przystąpimy do dowodu twierdzenia przeanalizujmy przykład. Niech $R = \mathbb{Z}$, $I_1 = (3), I_2 = (10), I_3 = (7)$. Założenia są spełnione. Spróbujmy znaleźć element $x \in \mathbb{Z}$, taki że $\varphi(x) = (2 + (3), 3 + (10), 2 + (7))$. Oznacza to, że szukamy liczby całkowitej x, której reszta przy dzieleniu przez 3 wynosi 2, przez 10 wynosi 3, a przez 7 wynosi 2. Z tego, że $3, 10, 7$ są parami względnie pierwsze mamy:

$$\begin{array}{ccccc} 3 \cdot 7 & + & (-2) \cdot 10 & = & 1 \\ (-3) \cdot 3 & + & 10 & = & 1 \\ 7 & + & (-2) \cdot 3 & = & 1. \end{array}$$

Zatem liczba $a_2 = 3 \cdot 7 \cdot (-3) \cdot 3 = (1 - (-2) \cdot 10)(1 - 10)$ daje resztę 1 przy dzieleniu przez 10 oraz reszte 0 przy dzieleniu przez 3 i przez 7, zaś $3a_2$ daje resztę 3 przy dzieleniu przez 10 oraz reszte 0 przy dzieleniu przez 3 i przez 7. Postępując analogicznie znajdujemy $a_1 = 70$, $a_3 = 120$. Ostatecznie $x = 2a_1 + 3a_2 + 2a_3$ jest szukaną liczbą całkowitą. Dowód twierdzenia w postaci ogólnej przebiega podobnie.
Dowód. Teza punktu b) jest oczywista i prawdziwa dla dowolnego ciągu ideałów $I_1, \ldots, I_n$.

Aby dowieść surjektywności odwzorowania φ wystarczy pokazać, że wszystkie elementy postaci $(0, \ldots, 0, y + I, 0, \ldots, 0)$ *są w obrazie* odwzorowania φ. Wynika to z faktu, że $\varphi(R)$ jest podpierścieniem w rozpatrywanym produkcie, a podpierścień generowany przez tego rodzaju elementy jest równy całemu produktowi. W celu dalszego uproszczenia rozpatrywanej sytuacji zauważmy, że jeżeli $\varphi(x) = (0, \ldots, 0, 1 + I, 0, \ldots, 0)$, to $\varphi(x \cdot y) = (0, \ldots, 0, y + I, 0, \ldots, 0)$. Wystarczy zatem pokazać, że w obrazie odwzorowania φ są wszystkie elementy postaci $(0, \ldots, 0, 1+I, 0, \ldots, 0)$. Nie ograniczając ogólności rozważań (a zyskując na przejrzystości zapisu) możemy zająć się przypadkiem elementu $(1+I, 0, \ldots, 0)$. Naszym celem jest wskazanie elementu a, takiego że $1 - a \in I_1$, a dla $i > 1$ zachodzi $a \in I_i$. Ale taki element łatwo wskazać:

Z założenia że ideały I_1 oraz I_i są względnie pierwsze wynika, że istnieją elementy $x_i \in I_1$ oraz $y_i \in I_i$, dla których $x_i + y_i = 1$. Wówczas element a zdefiniowany jako

$$a = \prod_{i \neq 1} (1 - x_i)$$

lub równoważnie

$$a = \prod_{i \neq 1} y_i$$

spełnia warunki:

$$a - 1 \in I_1 \quad \text{(to ze względu na pierwszy zapis)}$$

oraz:

$$a \in I_i \quad \text{dla } i \neq 1, \text{ (to ze względu na drugi zapis)},$$

co właśnie chcieliśmy uzyskać.

Kończy to dowód punktu a) a wraz z twierdzeniem o izomorfizmie dowód całego twierdzenia. □

Praktyczne zastosowanie twierdzenia chińskiego o resztach wymaga przedstawienia ideału I w postaci części wspólnej skończonej liczby ideałów względnie pierwszych. Okaże sie, że dla pewnej klasy pierścieni będziemy umieli to zrobić.

10. Dziedziny z jednoznacznością rozkładu

W pierścieniu liczb całkowitych $\mathbb{Z}$ podstawowym twierdzeniem jest zasadnicze twierdzenie arytmetyki mówiące, że każdą liczbę całkowitą można przedstawić w postaci iloczynu liczb całkowitych pierwszych i że przedstawienie to jest jednoznaczne z dokładnością do kolejności czynników i ich znaku. Ważnym i naturalnym problemem jest pytanie dla jakich pierścieni możemy udowodnić podobne twierdzenie. Zaczniemy od wprowadzenia słownika potrzebnych pojęć. **W rozdziale tym zakładamy, że rozpatrywane pierścienie są dziedzinami całkowitości.**

10.1. Definicja. *Niech R bedzie dziedziną całkowitości.Mówimy, że:*

a) *Element $a \in R \setminus \{0\}$ dzieli element b (co oznaczamy symbolem $a|b$) wtedy i tylko wtedy gdy istnieje element c, taki że $b = ca$ lub równoważnie $(b) \subseteq (a)$.*
b) *Elementy $a, b \in R \setminus \{0\}$ są* **stowarzyszone** *(co oznaczamy symbolem $a \sim b$ tylko wtedy gdy istnieje odwracalny element $u \in R$ dla którego $a = bu$ lub równoważnie $(a) = (b)$.*
c) *Element $a \in R \setminus \{0\}$ nieodwracalny jest* **nierozkładalny** *wtedy i tylko wtedy, gdy z równości $a = bc$ wynika, że b lub c jest elementem odwracalnym lub równoważnie (a) jest elementem maksymalnym ze względu na zawieranie w zbiorze właściwych ideałów głównych.*
d) *Element $a \in R \setminus \{0\}$ nieodwracalny jest* **pierwszy** *wtedy i tylko wtedy, gdy z tego, że $a|bc$ wynika, że $a|b$ lub $a|c$ lub równoważnie ideał (a) jest niezerowym ideałem pierwszym.*

10.2. Stwierdzenie. *W dziedzinie całkowitości element pierwszy jest nierozkładalny.*

Dowód. Teza stwierdzenia jest równoważnym sformułowaniem Twierdzenia 9.21. □

Zauważmy, że w dziedzinie ideałów głównych elementy pierwsze i nierozkładalne pokrywaja się.

10.3. Stwierdzenie. *Jeżeli R jest DIG, to każdy element nierozkładalny jest pierwszy.*

Dowód. Jeżeli a jest elementem nierozkładalnym, to (a) jest elementem maksymalnym ze względu na zawieranie w zbiorze właściwych ideałów głównych, ale ten w DIG jest równy zbiorowi wszystkich właściwych ideałów, a zatem (a) jest ideałem maksymalnym. Każdy ideał maksymalny jest pierwszy, a więc a jest elementem pierwszym. □

10.4. Przykłady.

1. W pierścieniu liczb całkowitych $\mathbb{Z}$ zbiór elementów pierwszych jest równy zbiorowi elementów nierozkładalnych i składa się z liczb pierwszych.
2. Liczba 2 nie jest elementem pierwszym w pierścieniu $\mathbb{Z}[\sqrt{d}]$, dla dowolnej liczby bezkwadratowej d. Mamy bowiem $2|d(d-1) = (d+\sqrt{d})(d-\sqrt{d})$, ale $2 \nmid (d+\sqrt{d})$ i $2 \nmid (d-\sqrt{d})$.
3. Liczba 2 jest elementem nierozkładalnym w pierścieniu $\mathbb{Z}[\sqrt{-3}]$ więc pierścień ten nie jest DIG.

Sformułujmy teraz główną definicję tego rozdziału.

10.5. Definicja. *Dziedzina całkowitości R nazywa sie* **dziedziną z jednoznacznością rozkładu (DJR)** *wtedy i tylko wtedy, gdy*

a) każdy element $a \in R \setminus \{0\}$ *może być przedstawiony w postaci iloczynu*

$$a = up_1 \dots p_k,$$

gdzie u jest elementem odwracalnym, zaś $p_1, \dots, p_k$ *są elementami nierozkładalnymi.*

b) rozkład ten jest jednoznaczny z dokładnością do stowarzyszenia, to znaczy ze jeżeli $a = up_1 \dots p_k = vq_1 \dots q_l$ *są rozkładami,* u, v *są elementami odwracalnymi, zaś* $p_1, dots, p_k, q_1, \dots, q_l$ *nierozkładalnymi, to* $k = l$ *i po ewentualnym przenumerowaniu* p_i *jest stowarzyszone z* q_i*,* $1 \leq i \leq k$*.*

Grupując nierozkładalne elementy stowarzyszone możemy dowolny niezerowy element zapisać jednoznacznie (z dokładnością do kolejności i stowarzyszenia) w postaci:

$$a = up_1^{k_1} \dots p_s^{k_s},$$

gdzie p_i *nie jest stowarzyszone z* p_j*, dla* $i \neq j$*.*

Zauważmy, ze w DJR jest tak, jak w pierścieniu liczb całkowitych, to znaczy

10.6. Stwierdzenie. *Jeżeli R jest dziedzina z jednoznacznością rozkładu, to*

a) każdy element nierozkładalny jest pierwszy;

b) każdy ciąg ideałów głównych

$$(\bigstar) \qquad (a_1) \subseteq (a_2) \subseteq \dots \subseteq (a_n) \subseteq \dots$$

stabilizuje się, to znaczy że od pewnego miejsca jest stały.

Dowód.

a) Niech a będzie elementem nierozkładalnym i niech $a|bc$. Zatem $ad = bc$, dla pewnego elementu d. Elementy b, c, d przedstawiamy w postaci iloczynu czynników nierozkładalnych. Z jednoznaczności rozkładu wynika, że po prawej stronie musi znaleźć się czynnik stowarzyszony z a.

b) Dla każdego i, $(a_i) \subseteq (a_{i+1})$ oznacza, że $a_{i+1}|a_i$ a zatem czynniki nierozkładalne a_{i+1} (liczone z wielokrotnością), ponieważ są elementami pierwszymi, to są czynnikami a_i , a więc i a_1. Wynika z tego, że począwszy od pewnego miejsca rozkłady a_i oraz a_{i+1} są takie same z dokładnością do stowarzyszenia. □

Warunek ★ nazywa się **ACC dla ideałów głównych**, gdzie ACC jest skrótem od angielskiego terminu "ascending chain condition".

Na to by dana dziedzina była dziedziną z jednoznacznością rozkładu muszą być spełnione dwa warunki :

✓ każdy element daje się przedstawić w postaci iloczynu elementów nierozkładalnych;

✓ przedstawienie to jest jednoznaczne z dokładnością do stowarzyszenia i permutacji czynników.

Przyjrzyjmy się temu pierwszemu warunkowi.

10.7. Stwierdzenie. *Jeżeli dziedzina całkowitości R spełnia ACC dla ideałów głównych, to każdy element nieodwracalny jest iloczynem elementów nierozkładalnych.*

Dowód. Przypuśćmy, że $a \in R$ jest elementem, którego nie można przedstawić w postaci iloczynu elementów nierozkładanych. Wynika z tego, że a nie jest nierozkładalny i $a = bc$, gdzie b i c nie są odwracalne. Element b lub c nie jest iloczynem

elementów nierozkładalnych, gdyż w przeciwnym razie a dałoby się tak przedstawić. Powiedzmy, że b nie jest iloczynem nierozkładalnych. Kładąc $b = a_1$ mamy $(a) \subsetneqq (a_1)$. Powtarzając indukcyjnie to rozumowanie otrzymujemy nieskończony ciąg $(a)) \subsetneqq (a_1)) \subsetneqq (a_2)) \subsetneqq \dots$ wbrew założeniu. □

A teraz drugi warunek:

10.8. Stwierdzenie. *Jeżeli w dziedzinie całkowitości R każdy element nierozkładalny jest pierwszy, to przedstawienie dowolnego elementu w postaci iloczynu elementów nierozkładalnych jest jednoznaczne z dokładnością do stowarzyszenia i permutacji czynników.*

Dowód. Niech $a_1 a_2 \dots a_n = b_1 b_2 \dots b_m$ i niech a_i, $1 \geq i \geq n$ oraz b_j, $1 \geq j \geq m$ będą nierozkładalne. Dowodzimy przez indukcję ze względu na n. Będziemy korzystać z tego, że elementy $a_1, \dots a_n$ jako nierozkładalne są pierwsze. Jeżeli $n = 1$, to a_1 jako element pierwszy dzieli pewne b_j, po przenumerowaniu można założyć, że $j = 1$ i z nierozkładalności b_1 mamy $b_1 = a_1 u_1$, gdzie u_1 jest odwracalny. Po skróceniu otrzymujemy $1 = u_1 b_2 \dots b_m$. Oznacza to, że $b_2, \dots b_m$ są odwracalne, co jest sprzeczne i $m = 1$. Rozumowanie w kroku indukcyjnym jest analogiczne. □

10.9. Twierdzenie. *Dziedzina ideałów głównych jest dziedziną z jednoznacznością rozkładu.*

Dowód. Wiemy już że w DIG elementy nierozkładalne są pierwsze - Stwierdzenie 10.2. Musimy pokazać warunek ACC dla ideałów. Niech

$$(a_1) \subseteq (a_2) \subseteq \dots \subseteq (a_n) \subseteq \dots$$

będzie wstępującym ciągiem ideałów. Wówczas $\bigcup_{i=1}^{\infty}(a_i)$ jest ideałem i jest on postaci (b). Dla pewnego $i \in \mathbb{N}$, $b \in (a_i)$ i od tego miejsca ciąg musi się stabilizować. □

Największy Wspólny Dzielnik.

Wzorem pierścienia liczb całkowitych wprowadzimy definicję.

10.10. Definicja. *Niech R bedzie dziedziną całkowitości i niech $\emptyset \neq A \subset R$. Powiemy, że element $d \in R$ jest największym wspólnym dzielnikiem (oznaczamy go symbolem NWD(A)) jeżeli*

a) dla każdego $x \in A$, $d|x$,

b) jeżeli $e|x$ dla każdego $x \in A$, to $e|d$.

Jeżeli NWD$(A) = 1$*, to mówimy że zbiór A jest względnie pierwszy.*

Zauważmy, ze z definicji wynika natychmiast, że jeżeli $NWD(A)$ istnieje, to jest wyznaczony jednoznacznie z dokładnością do stowarzyszenia.

10.11. Przykład. Nie istnieje $NWD(4, 2 + 2\sqrt{-3})$.

W szkole podstawowej znajdowało się największy wspólny dzielnik podzbioru A zbioru licz całkowitych w ten sposób, że należało rozłożyć wszystkie liczby ze zbioru A na czynniki pierwsze i największy wspólny dzielnik był iloczynem tych (z uwzględnieniem krotności), które występują w każdej liczbie ze zbioru A. Dokładnie to samo rozumowanie prowadzi do dowodu następującego faktu.

10.12. Stwierdzenie. *W każdej dziedzinie z jednoznacznością rozkładu istnieje* NWD(A)*, dla dowolnego niepustego podzbioru $A \subset R$.*

10.13. Stwierdzenie. *Jeżeli R jest dziedziną ideałów głównych, to $d = NWD(A)$, $\emptyset \neq A \subset R$ wtedy i tylko wtedy, gdy $(A) = (d)$.*

Dowód. Równość $(d) = (A)$ zachodzi wtedy i tylko wtedy, gdy po pierwsze $A \subset (d)$ i po drugie (d) jest najmniejszym ideałem zawierającym A, czyli jeżeli $A \subseteq (e)$, to $(d) \subseteq (e)$. Pierwszy z tych warunków jest równoważny temu, że dla każdego $x \in A$, $d|x$, Drugi temu, że jeżeli $e|x$ dla każdego $x \in A$, to $e|d$. □

10.14. Wniosek. *Jeżeli w dziedzinie ideałów głównych elementy a i b są względnie pierwsze, to istnieją elementy k i l, dla których $ak + bl = 1$*

10.15. Przykład. Zauważmy, że w powyższym stwierdzeniu założenie, że R jest dziedziną ideałów głównych jest istotne. W pierścieniu $\mathbb{Z}[X]$, $NWD(X, 3) = 1$, ale $(3, X) \neq \mathbb{Z}[X]$.

Wróćmy jeszcze do chińskiego twierdzenia o resztach.

Niech R będzie DIG a $I \trianglelefteq R$ ideałem. Wówczas $I = (x)$ i element x ma rozkład $x = a_1^{k_1} \cdot \ldots a_n^{k_n}$, gdzie elementy a_i są nierozkładalne i nie stowarzyszone. Wynika z tego, ze :

ideały $I_i = (a_i^{k_i})$ oraz $I_j = (a_j^{k_j})$ są względnie pierwsze dla $i \neq j$,

$I = I_1 \cap \cdots \cap I_n$.

Zatem stosując twierdzenie chińskie o resztach otrzymujemy następujący wniosek:

10.16. Wniosek. *Niech R będzie dziedziną ideałów głównych, $(x) \trianglelefteq R$ ideałem, oraz $x = a_1^{k_1} \cdot \ldots a_n^{k_n}$, gdzie elementy a_i są nierozkładalne i nie stowarzyszone. Wówczas*

$$R/(x) \cong R/(a_1^{k_1}) \times \cdots \times R/(a_n^{k_n}).$$

10.17. Przykład. Czy pierścienie $\mathbb{Q}[X]/((X-1)(X+1))$ oraz $\mathbb{Q}[X]/((X-3)X)$ są izomorficzne?

Mamy:

$$\mathbb{Q}[X]/((X-1)(X+1)) \cong \mathbb{Q}[X]/(X+1) \times \mathbb{Q}[X]/(X-1) \cong \mathbb{Q} \times \mathbb{Q}$$

i analogicznie

$$\mathbb{Q}[X]/((X-3)X) \cong \mathbb{Q}[X]/(X-3) \times \mathbb{Q}[X]/(X) \cong \mathbb{Q} \times \mathbb{Q},$$

a więc są izomorficzne.

11. Dziedziny Euklidesowe

11.1. Definicja. *Dziedziną Euklidesową nazywamy parę (R, v), gdzie R jest dziedziną całkowitości a $v : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ funkcją zwaną waluacją, która spełnia następujące warunki:*
1. *dla dowolnych $a, b \in R \setminus \{0\}$, $v(ab) \geq v(a)$,*
2. *dla dowolnych $a \in R$ oraz $b \in R \setminus \{0\}$ istnieja elementy $q, r \in R$, takie że*

$$a = bq + r \quad oraz \quad r = 0 \quad lub \quad v(r) < v(b).$$

11.2. Twierdzenie. *Każda dziedzina euklidesowa jest dziedziną ideałów głównych.*

Dowód. Niech R będzie dziedzina euklidesową z waluacją v. Niech $I \lhd R$ będzie niezerowym ideałem. Niech $x \in I$ będzie niezerowym elementem, takim że $v(x) = \min\{v(y) : \quad y \in I \setminus \{0\}\}$. Pokażemy, że $I = (x)$. Niech $y \in I$. Wówczas $y = xq + r$, gdzie $r = 0$ lub $v(r) < v(x)$. Zauważmy, że skoro $y, x \in I$, to $r \in I$. Ponieważ waluacja x jest minimalna, to $r = 0$ i $y = qx$, a zatem $I = (x)$. □

Klasa pierścieni będących dziedzinami ideałów głównych jest szersza od klasy pierścieni euklidesowych. Na tym wykładzie wszystkie omawiane przykłady dziedzin ideałów głównych będą pierścieniami euklidesowymi. Zanim omówimy przykłady dziedzin euklidesowych odnotujmy pewne proste własności waluacji.

11.3. Stwierdzenie. *Niech $v : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ będzie waluacją. Wówczas,*
a) dla każdego $a \in R \setminus \{0\}$, $v(a) \geq v(1)$.
b) dla dowolnych $a, b \in R \setminus \{0\}$, $v(ab) = v(b)$ wtedy i tylko wtedy, gdy a jest elementem odwracalnym.
c) dla dowolnego $a \in R \setminus \{0\}$, $v(a) = v(1)$ wtedy i tylko wtedy, gdy a jest elementem odwracalnym.

Dowód. punkt a) jest oczywistym wnioskiem z definicji, zaś punkt c) wynika z punktu b). Tak więc udowodnimy punkt b). Jeżeli $v(ab) = v(b)$, to z dowodu poprzedniego twierdzenia wynika, że $(ab) = (b)$. W szczególności $b \in (ab)$ i istnieje $c \in R$, dla którego $b = abc$. Ponieważ $b \neq 0$ i R jest dziedzina całkowitości, to $ac = 1$. Odwrotnie, jeżeli a jest elementem odwracalnym i c elementem odwrotnym, to $v(b) = v(cab) \geq v(ab)$. Nierówność $v(ab) \geq v(b)$ wynika z definicji. Punkt c) jest wnioskiem z b) jeżeli weźmiemy $b = 1$. □

Przykładami dziedzin euklidesowych są : pierścień liczb całkowitych $\mathbb{Z}$, gdzie waluacją jest wartość bezwzględna oraz pierścień wielomianów $K[X]$ nad ciałem K, gdzie waluacja jest stopień wielomianu.

Niech $d \in \mathbb{Z}$ będzie liczba całkowitą,$d \neq 1$, bezkwadratową. Niech

$$v : \mathbb{Z}[\sqrt{d}] \to \mathbb{N} \qquad v(a + b\sqrt{d}) = |a^2 - b^2 d|.$$

Wprowadźmy oznaczenia: $\alpha = a + b\sqrt{d}$, $\bar{\alpha} = a - b\sqrt{d}$. Wówczas $v(\alpha) = |\alpha\bar{\alpha}|$. Łatwy rachunek przekonuje nas o tym, że $v(\alpha\beta) = v(\alpha)v(\beta)$ oraz, że α jest elementem odwracalnym wtedy i tylko wtedy, gdy $v(\alpha) = 1$ i wówczas $\bar{\alpha}$ jest elementem odwrotnym.

11.4. Stwierdzenie. *Funkcja* $v(a+b\sqrt{d}) = |a^2 - b^2 d|$ *jest waluacją euklidesową na* $\mathbb{Z}[\sqrt{d}]$ *dla* $d \in \{-2, -1, 2, 3\}$

Dowód. Jest oczywiste, że $v(a+b\sqrt{d}) \geq 1$, gdyż $v(a+b\sqrt{d}) = 0$ oznaczałoby, że $d = (\frac{a}{b})^2$, wbrew założeniu, że d jest liczba bezkwadratową. Stąd i z multyplilkatywności funkcji v wynika, że warunek pierwszy jest spełniony dla dowolnego d.

Pokażemy, że dla wymienionych wartości d w pierścieniu $\mathbb{Z}[\sqrt{d}]$ można dzielić z resztą. Dowód dostarcza także algorytm wykonywania takiego dzielenia. Niech $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$, $\beta \neq 0$. Wówczas $\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$. Niech $r, s \in \mathbb{Z}$ będą liczbami całkowitymi takimi, że $|x - r| \leq \frac{1}{2}$ i $|y - s| \leq \frac{1}{2}$. Niech $\gamma = r + s\sqrt{d}$, zaś $\delta = ((x - r) + (y - s)\sqrt{d})\beta$. Zauważmy, że $\alpha = \beta\gamma + \delta$ przy czym $\alpha, \beta, \gamma \in \mathbb{Z}[\sqrt{d}]$. Zatem także $\delta \in \mathbb{Z}[\sqrt{d}]$. Wystarczy teraz pokazać, ze $v(\delta) < v(\beta)$ lub $\delta = 0$. Przypuśćmy, że $\delta \neq 0$. Mamy $v(\delta) = v(\beta)|(x-r)^2 - (y-s)^2 d| \leq v(\beta)(\frac{1}{4} + \frac{1}{4}|d|)$. Dla $d =\in \{-2, -1, 2\}$, $\frac{1}{4} + \frac{1}{4}|d| < 1$ i $v(\delta) < v(\beta)$. Jeżeli $d = 3$, to $|(x-r)^2 - (y-s)^2 3| \leq \frac{1}{4} + \frac{1}{4}3 = 1$. Równość może wystąpić tylko wtedy, gdy $x - r = y - s = \frac{1}{2}$, jednak wówczas $v(\frac{1}{2} + \frac{1}{2}\sqrt{3}) = \frac{1}{2} < 1$, co dowodzi, że dla $d = 3$ waluacja także jest euklidesowa. □

11.5. Przykład. Liczba 2 nie jest elementem pierwszym, ale jest elementem nierozkładalnym w pierścieniu $\mathbb{Z}[\sqrt{d}]$, dla $d \leq -3$. Przypuśćmy przeciwnie, że $2 = \alpha\beta$, gdzie α, β nieodwracalne. Wówczas $v(2) = 4 = v(\alpha)v(\beta)$. Z nieodwracalności $v(\alpha) \neq 1$ i $v(\beta) \neq 1$, a więc $v(\alpha) = v(\beta) = 2$.Jeżeli $\alpha = x + y\sqrt{d}$, to $|x^2 - y^2 d| = 2$, ale dla $d \leq -3$, to nie jest mozliwe. Bowiem $|x^2 - y^2 d| \geq x^2 + 3y^2 > 2$ dla $y \neq 0$, ale $y \neq 0$, bo w przeciwnym razie 2 byłaby kwadratem liczby naturalnej.

11.6. Wniosek. *Dziedzina* $\mathbb{Z}[\sqrt{d}]$ *nie jest dziedziną euklidesową dla* $d \leq -3$.

Algorytm Euklidesa

Niech R będzie dziedziną Euklidesową z waluacją v. Pokażemy algorytm, który pozwoli na znajdowanie największego wspólnego dzielnika dwóch elementów bez konieczności rozkładania ich na iloczyn czynników nierozkładalnych.

Niech $a_1, a_2 \in R \setminus \{0\}$. Mamy:

$$\begin{array}{lllllll} a_1 & = & a_2 q_1 + a_3 & \text{gdzie} & a_3 = 0 & \text{lub} & v(a_3) < v(a_2) \\ a_2 & = & a_3 q_2 + a_4 & \text{gdzie} & a_4 = 0 & \text{lub} & v(a_4) < v(a_3) \\ a_3 & = & a_4 q_3 + a_5 & \text{gdzie} & a_5 = 0 & \text{lub} & v(a_5) < v(a_4) \\ .. & & & & & & \end{array}$$

jest jasne, że ten proces musi się skończyć i w końcu

$$a_{n-1} = a_n q_{n-1} + 0$$

11.7. Stwierdzenie. $a_n = NWD(a_1, a_2)$

Dowód. Wiemy, że $NWD(a_1, a_2)$ jest generatorem ideału (a_1, a_2). Pokażemy przez indukcję, że $(a_i, a_{i+1}) = (a_{i+1}, a_{i+2})$. Mamy:

$$xa_i + ya_{i+1} = x(a_{i+1}q_i + a_{i+2}) + ya_{i+1} \in (a_{i+1}, a_{i+2})$$

$$ra_{i+1} + sa_{i+2} = ra_{i+1} + s(a_i - a_{i+1}qi) \in (a_i, a_{i+1})$$

co dowodzi żądą równość. Zatem $(a_1, a_2) = (a_{n-1}, a_n)$. Wszakże $a_{n-1} = a_n q_{n-1}$ i $(a_1, a_2) = (a_{n-1}, a_n) = (a_n)$, co wobec Stwierdzenia 10.12 dowodzi tezy. □

Pierścień $\mathbb{Z}[i]$ liczb Gaussa.

Zacznijmy od ustalenia jak wyglądają elementy nierozkładalne w pierścieniu $\mathbb{Z}[i]$. Poprzedzimy je oczywistymi uwagami:

1) Elementami odwracalnymi w $\mathbb{Z}[i]$ są $1, -1. i. - i$.
1) Jeżeli $\alpha \in \mathbb{Z}[i]$ i $v(\alpha)$ jest liczbą pierwszą, to α jest elemetem nierozkładalnym.
2) Element α jest nierozkładalny wtedy i tylko wtedy, gdy nierozkładalny jest element $\bar{\alpha}$.

11.8. Stwierdzenie. *Element nierozkładalny dziedziny $\mathbb{Z}[i]$ jest dzielnikiem liczby całkowitej pierwszej.*

Dowód. Niech $\alpha \in \mathbb{Z}[i]$ będzie elementem nierozkładalnym. Wówczas $\alpha\bar{\alpha} = n$ jest rozkładem liczby całkowitej n na czynniki nierozkładalne w $\mathbb{Z}[i]$. Gdyby n nie było liczbą pierwszą i $n = rs$, $r, s \in \mathbb{N} \setminus \{1\}$, to rozkładając r i s na czynniki nierozkładalne w $\mathbb{Z}[i]$ otrzymalibyśmy inny rozkład n, a więc sprzeczność. □

11.9. Stwierdzenie. *Liczba całkowita pierwsza p jest rozkładalna w pierścieniu $\mathbb{Z}[i]$ wtedy i tylko wtedy, gdy można ją przedstawić w postaci sumy kwadratów liczb całkowitych. Jeżeli $a^2 + b^2 = p$, to*

a) $\alpha\bar{\alpha} = p$, gdzie $\alpha = a + bi$ jest jej rozkładem na czynniki nierozkładalne w pierścieniu $\mathbb{Z}[i]$;
b) przedstawienie $a^2 + b^2 = p$ jest jednoznaczne.

Dowód. Jeżeli $p = \alpha\beta$ jest rozkładem liczby pierwszej na czynniki nierozkładalne w pierścieniu $\mathbb{Z}[i]$, to żaden z czynników tego rozkładu nie jest stowarzyszony z liczbą całkowitą. Korzystając z multyplikatywności waluacji otrzymujemy $p^2 = v(\alpha)v(\beta)$. Ponieważ α i β są czynnikami nieodwracalnymi, to ich waluacje są różne od 1 i jedyną możliwością jest $v(\alpha) = v(\beta) = p$. Jeżeli $\alpha = a + bi$, to $v(\alpha) = a^2 + b^2 = p$, $a \neq 0$, $b \neq 0$.

Przedstawienie liczby p w postaci $p = a^2 + b^2$, oznacza, że w pierścieniu $\mathbb{Z}[i]$, $p = \alpha\bar{\alpha}$, gdzie $\alpha = a + bi$ Oba czynniki są nierozkładalne, gdyż ich waluacja jest liczbą pierwszą. Pierścień $\mathbb{Z}[i]$ jest dziedziną z jednoznacznością rozkładu, więc rozkład p jest jedyny z dokładnością do stowarzyszenia, a zatem przedstawienie $p = a^2 + b^2$ o ile istnieje to jest jedyne. □

11.10. Wniosek. *Elementami nierozkładalnymi pierścienia $\mathbb{Z}[i]$ są liczby całkowite pierwsze, które nie dają się przedstawić w postaci sumy dwóch kwadratów oraz liczby $a \pm bi$, gdzie $a^2 + b^2$ jest liczbą pierwszą.*

Pozostaje pytanie, jakie liczby pierwsze można przedstawić w postaci sumy kwadratów liczb całkowitych. Oczywiście $2 = 1^2 + 1^2$. Ponieważ kwadrat dowolnej liczby całkowitej przytsaje do 0 lub do 1 *mod* 4, to warunkiem koniecznym na to by takie przedstawienie istniało jest by liczba pierwsza była postaci $p = 4k + 1$, $k \in \mathbb{Z}$. To, że jest to warunek dostateczny jest treścią twierdzenia Fermata. Jego dowód poprzedzimy lematem.

11.11. Lemat. *Jeżeli liczba pierwsza $p \in \mathbb{N}$ jest postaci $4k + 1$, to istnieje liczba całkowita m, dla której $p \mid m^2 + 1$.*

Dowód. Przypomnijmy twierdzenie Wilsona, ktore było zastosowaniem do grupy multyplikatywnej $\mathbb{Z}_p^*$ łatwego faktu, iż w grupie przemiennej skończonej iloczyn wszystkich elementów jest równy iloczynowi elementów rzędu dwa. Twierdzenie to mówi więc, że dla liczby pierwszej p, $(p-1)! \equiv -1 (\mathrm{mod}\, p)$. Mamy $p-l \equiv -l (\mathrm{mod}\, p)$ i jeżeli $p = 4k+1$, to $(p-1)! \equiv (-1)^{2k}((2k)!)^2 (\mathrm{mod}\, p)$. Zatem przyjmując $m = (2k)!$ mamy $m^2 \equiv -1 (\mathrm{mod}\, p)$. □

11.12. Twierdzenie Fermata o sumie dwóch kwadratów. *Jeżeli p jest liczbą pierwszą postaci $4k+1$, to istnieją liczby całkowite a i b dla których $p = a^2 + b^2$.*

Dowód. Wiemy, że $p \mid m^2 + 1$ dla pewnej liczby całkowitej m. W pierścieniu $\mathbb{Z}[i]$, $m^2 + 1 = (m+i)(m-i)$ zatem $p \mid (m+i)(m-i)$. Jest jednak jasne, że $p \nmid m+i$ i $p \nmid m-i$, zatem p nie jest elementem pierwszym, czyli nierozkładalnym. Ze stwierdzenia 11.9 wynika więc, że p jest sumą kwadratów dwóch liczb całkowitych i to dokładnie na jeden sposób. □

Autorzy skryptu nie mogą nie ulec pokusie, by przedstawić Państwu zupełnie inny, nie korzystający z teorii rozkładu w pierścieniu $\mathbb{Z}[i]$ tylko z teorii działań grup, dowód twierdzenia Fermata. Autorem tego nowego (sprzed kilkunastu lat) dowodu jest Don Zagier.

Dowód. (Don Zagier). Niech p będzie liczbą pierwszą postaci $4k+1$ i niech $X = \{(x,y,z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$. Zbiór X jest oczywiście skończony i działa na nim grupa $\mathbb{Z}_2$ tak że generator odwzorowuje (x,y,z) na (x,z,y). Twierdzenie Fermata jest równoważne stwierdzeniu że działanie to ma punkty stałe. Na zbiorze X istnieje także inne działanie grupy $\mathbb{Z}_2$. Jeżeli przez φ oznaczymy bijekcję zdefiniowaną przez generator, to

$$\varphi(x,y,z) = \begin{cases} (x+2z, z, y-x-z), & \text{jeżeli} \quad x < y-z \\ (2y-x, y, x-y=z), & \text{jeżeli} \quad y-z < x < 2y \\ (x-2y, x-y+z, y), & \text{jeżeli} \quad x > 2y \end{cases} .$$

Proste sprawdzenie pokazuje, że to ostatnie działanie ma dokładnie jeden punkt stały i jest nim $(1,1,k)$. Wynika z tego, że moc X jest liczbą nieparzystą a zatem pierwsze działanie także musi mieć punkty stałe. □

12. Jednoznaczność rozkładu w pierścieniach wielomianów.

Celem tego rozdziału jest udowodnienie twierdzenia Gaussa, które mówi, że pierścień wielomianów nad dziedziną z jednoznacznoćią rozkładu jest także dziedziną z jednoznacznością rozkładu.

Rozważania poprzedzimy opisem konstrukcji, która danej dziedzinie całkowitości przyorz'adkowuje ciało, tę dziedzinę całkowitości zawierające jako podpierścień.

Ciało ułamków.

Załóżmy, że R jest dziedziną całkowitości. Obowiązuje wówczas, tak jak w ciele, prawo skracania (przez elementy niezerowe) dla mnożenia:

$$\forall_{x\neq 0}\forall_{y,z}\ xy = xz \Leftrightarrow y = z.$$

Jednak, inaczej niż w ciele, niektóre niezerowe elementy mogą nie mieć odwrotności. Okazuje się, że dziedzina R, choć sama nie musi być ciałem, jest zawsze *zawarta* w pewnym ciele. Istnieje prosta konstrukcja, która to gwarantuje, tzw. konstrukcja ciała ułamków $Q(R)$ dziedziny R. W szczególnym przypadku, gdy $R = \mathbb{Z}$ otrzymujemy dobrze znane ciało liczb wymiernych: $Q(\mathbb{Z}) = \mathbb{Q}$.

Niech R będzie dziedziną całkowitości. Na zbiorze par uporządkowanych $R \times (R \setminus \{0\})$ określamy relację równoważności $\sim$ wzorem
$(x, y) \sim (z, v) \Leftrightarrow xv = yz$. Klasę równoważności tej relacji nazywamy ułamkiem i oznaczamy symbolem $\frac{x}{y}$ (tak więc $\frac{x}{y} = \frac{z}{v} \Leftrightarrow xv = yz$). Zbiór wszystkich ułamków oznaczamy symbolem $Q(R)$.

12.1. Definicja. **Ciałem ułamków** *dziedziny całkowitości R nazywamy zbiór $Q(R)$ z ułamkiem $\frac{0}{1}$ jako zerem, ułamkiem $\frac{1}{1}$ jako jedynką i działaniami określonymi wzorami:*

$$\frac{x}{y} + \frac{p}{q} = \frac{xq + py}{yq}$$
$$\frac{x}{y} \cdot \frac{p}{q} = \frac{xp}{yq}$$
$$-\frac{p}{q} = \frac{-p}{q}$$

Łatwo sprawdzić, że takie działania są dobrze określone i że definiują ciało. Odwzorowanie $i : R \hookrightarrow Q(R)$ zadane wzorem $i(x) = \frac{x}{1}$ jest monomorfizmem pierścieni. Zatem istotnie, każda dziedzina całkowitości jest podpierścieniem pewnego ciała.

12.2. Przykład. Niech $R = k[X]$ będzie pierścieniem wielomianów ciała k. Ciało ułamków $Q(k[X])$ oznaczamy symbolem $k(X)$ i nazywamy **ciałem funkcji wymiernych nad** k. Dla $k = \mathbb{Z}_p$ konstrukcja ta dostarcza przykładu ciała nieskończonego charakterystyki p.

Konstrukcję ciała ułamków rozumiemy jako operację dodania do dziedziny całkowitości pewnych brakujących elementów. Zauważmy, że oczywiście

12.3. Uwaga. Jeżeli dziedzina całkowitości R jest ciałem, to $Q(R) \cong R$.

Ciało ułamków jest scharakteryzowane przez następujące stwierdzenie.

12.4. Stwierdzenie. *Jeżeli R jest dziedziną całkowitości, a $j : R \hookrightarrow F$ włożeniem w ciało F, to istnieje dokładnie jedno włożenie $k : Q(R) \hookrightarrow F$ dla którego $ki = j$, gdzie $i : R \hookrightarrow Q(R)$.*

Dowód tego twierdzenia jest oczywisty.

Twierdzenie Gaussa.

12.5. Twierdzenie Gaussa. *Jeżeli R jest dziedziną z jednoznacznością rozkładu, to pierścień wielomianów $R[X]$ jest także dziedziną z jednoznacznością rozkładu.*

W dalszych rozważaniach zakładamy, że R jest dziedziną z jednoznacznością rozkładu. Pierścień R jest zawarty w $R[X]$ jako wielomiany stopnia 0. Ponieważ R jest dziedziną całkowitości, to $\deg fg = \deg f + \deg g$. Ta prosta obserwacja pozwala na scharakteryzowanie odwracalnych i nierozkładalnych elementów dziedziny całkowitości $R[X]$.

12.6. Uwaga. *Element $R[X]$ jest odwracalny wtedy i tylko wtedy, gdy jest odwracalnym elementem R.*

12.7. Definicja. *Zawartością niezerowego wielomianu $f = a_0 + a_1X + \cdots + a_nX^n$ nazywamy $\mathrm{NWD}(a_0, a_1, \ldots, a_n)$ i oznaczamy ją symbolem $\mathrm{cont}(f)$. Zawartość wielomianu jest wyznaczona jednoznacznie z dokładnością do stowarzyszenia w R. Wielomian $f \in R[X] \setminus \{0\}$, nazywa się* **pierwotny** *jeżeli $\mathrm{cont}(f) = 1$.*

12.8. Stwierdzenie. *Każdy niezerowy wielomian możemy zapisać w postaci $f = \mathrm{cont}(f)f_1$, gdzie f_1 jest wielomianem pierwotnym.*

12.9. Stwierdzenie. *Elementami nierozkładalnymi dziedziny $R[X]$ są:*
nierozkładalne elementy pierścienia R
wielomiany pierwotne stopnia większego od zera, których nie można przedstawić w postaci iloczynu wielomianów mniejszego stopnia.

Dowód. Jest jasne, że nierozkładalne wielomiany stopnia 0, to dokładnie nierozkładalne elementy pierścienia R. Jeżeli $\deg f > 0$ i f nierozkładalny, to f musi być pierwotny i nie być iloczynem wielomianów mniejszego stopnia. W przeciwnym bowiem razie $f = \mathrm{cont}(f)f_1$ lub $f = gh$, $\deg g > 0$ i $\deg h > 0$ byłyby przedstawieniem f w postaci iloczynu elementów nieodwracalnych. Odwrotnie, przypuśćmy że f , $\deg f > 0$ jest wielomianem pierwotnym którego nie można przedstawić w postaci iloczynu wielomianów mniejszego stopnia. Jeżeli $f = gh$, to stopień jednego z wielomianów np. g jest równy 0. Zatem $g = a \in R$ i $a \mid \mathrm{cont}(f)$. Ponieważ $cont(f) = 1$, to a jest elementem odracalnym, a więc f jest nierozkładalny. □

Łatwo widać, że każdy wielomian można przedstawić w postaci iloczynu nierozkładalnych elementów $R[X]$.

12.10. Stwierdzenie. *Każdy element dziedziny $R[X]$ może być przedstawiony w postaci iloczynu elementów nierozkładalnych.*

Dowód. Wielomian $f \in R[X]$ przedstawiamy w postaci $f = \mathrm{cont}(f)f_1$, gdzie f_1 jest wielomianem pierwotnym. Element $\mathrm{cont}(f) \in R$ przedstawiamy w postaci iloczunu nierozkładalnych elementów R, gdyż R jest DJR - elementy nierozkładalne R są też elementami nierozkładalnymi $R[X]$. Wielomian pierwotny f_1 jeśli nie jest nierozkładalny, to $f_1 = g_1h_1$, przy czym $\deg g_1 < \deg f_1$ i $\deg h_1 < \deg f_1$ i

oczywiście oba wielomiany g_1 i h_1 są pierwotne. Powtarzamy procedurę w odniesieniu do wielomianów g_1 i h_1. Po skończonej liczbie kroków otrzymamy iloczyn pierwotnych wielomianów nierozkładalnych dodatniego stopnia, gdyż za każdym krokiem stopień wielomianu zmniejsza się. □

W celu zakończenia dowodu należy wykazać jednoznaczność rozkładu dowodząc (Stwierdzenie 10.7), że elementy nierozkładalne dziedziny $R[X]$ są pierwsze.

12.11. Stwierdzenie. *Jeżeli $a \in R$ jest elementem nierozkładalnym, to a jest elementem pierwszym dziedziny $R[X]$.*

Dowód. Jeżeli a jest elementem nierozkładalnym dziedziny z jednoznacznością rozkładu R, to a jest elementem pierwszym, czyli ideał (a) jest pierwszy i $R/(a)$ jest dziedziną całkowitości. Homomorfizm $\pi : R \to R/(a)$ wyznacza homomorfizm $\pi_*: R[X] \to R/(a)[X]$. Niech $a \mid fg$ w $R[X]$. Zatem $fg = ah$ w $R[X]$ i $\pi_*(f)\pi_*(g) = \pi_*(a)\pi_*(h)$ w pierścieniu $R/(a)[X]$. Ale $\pi_*(a) = 0$, więc w dziedzinie całkowitości $R/(a)[X]$, $\pi_*(f)\pi_*(g) = 0$, co oznacza. że $\pi_*(f) = 0$ lub $\pi_*(g) = 0$, co jest równoważne $a \mid f$ lub $a \mid g$. □

Pokazanie, że nierozkładalny wielomian pierwotny f dodatniego stopnia w $R[X]$ jest elementem pierwszym w $R[X]$ jest bardziej skomplikowane i stanowi główną trudność dowodu twierdzenia Gaussa. Pierścień $R[X]$ rozpatrujemy jako podpierścień pierścienia wielomianów $Q(R)[X]$ nad ciałem ułamków R. Wnioskowanie jest następujące:

1. nierozkładalny wielomian pierwotny f dodatniego stopnia w $R[X]$ jest elementem nierozkładalnym w $Q(R)[X]$,
2. ponieważ $Q(R)[X]$ jest DJR jako dziedzina euklidesowa, to wielomian f jest elementem pierwszym w $Q(R)[X]$,
3. jeżeli f jest elementem pierwszym w $Q(R)[X]$, to jest też elementem pierwszym w $R[X]$.

Do udowodnienia punktu 1. potrzebny jest:

12.12. Lemat Gaussa. *Dla wielomianów $f, g \in R[X] \setminus \{0\}$,*

$$\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$$

Dowód. Wystarczy pokazać, że iloczyn wielomianów pierwotnych jest wielomianem pierwotnym. Załóżmy nie wprost, że $f, g \in R[X] \setminus \{0\}$ są wielomianami pierwotnymi, a fg nie jest pierwotny. Ponieważ R jest DJR, to istnieje element pierwszy p, taki że $p \mid \operatorname{cont}(fg)$. Niech $f = a_0 + a_1X + \cdots + a_nX^n$, $g = b_0 + b_1X + \cdots + b_mX^m$ i niech a_r i b_s będą najniższymi współczynnikami, których nie dzieli p. Element p dzieli współczynnik c_{r+s} iloczynu fg, który jest równy

$$c_{r+s} = \underbrace{a_0b_{r+s} + \cdots + a_{r-1}b_{s+1}} + a_rb_s + \underbrace{a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0}$$

Element p dzieli te składniki sumy, które są ujęte w klamry, a więc dzieli także a_rb_s. Ponieważ p jest elementem pierwszym, to $p \mid a_r$ lub $p \mid b_s$ - sprzeczność. □

12.13. Uwaga Niech teraz $Q(R)$ będzie ciałem ułamków dziedziny R z jednoznacznością rozkładu. Jest jasne, że wielomian $f \in Q(R)[X] \setminus \{0\}$ można przedstawić w postaci

$$f = \frac{a}{b}\tilde{f},$$

gdzie $\tilde{f} \in R[X]$, $\deg \tilde{f} = \deg f$ jest wielomianem pierwotnym (o współczynnikach z R), zaś $\frac{a}{b} \in Q(R)$. Ponieważ zawartość wielomianu jest wyznaczona jednoznacznie z dokładnością do stowarzyszenia w R, to wielomian $\tilde{f}$ jest wyznaczony jednoznacznie z dokładnością do mnożenia przez element odwracalny pierścienia R, czyli do stowarzyszenia w $R[X]$.

Możemy teraz podać dowód punktu 1.

12.14. Lemat. *Niech $f \in R[X]$ będzie wielomianem nierozkładalnym w $R[X]$, $\deg f > 0$. Wówczas f jest wielomianem nierozkładalnym w $Q(R)[X]$.*

Dowód. Z założenia wynika, że wielomian f jest pierwotny. Przypuśćmy, ze f jest rozkładalny w $Q(R)[X]$. Wynika z tego, że $f = gh$, gdzie $g, h \in Q(R)[X]$ nieodwracalne, a zatem $\deg g > 0$ i $\deg h > 0$. Przedstawiając wielomiany g i h zgodnie z uwagą poprzedzającą lemat, otrzymujemy

$$f = \frac{a}{b}\,\tilde{g}\,\tilde{h} \quad a, b \in R,$$

przy czym wielomiany $\tilde{g}, \tilde{h} \in R[X]$ są pierwotne dodatniego stopnia. Z lematu Gaussa wynika, że $\tilde{g}\tilde{h}$ jest także wielomianem pierwotnym, więc poprzedniego lematu wnioskujemy, że f i $\tilde{g}\tilde{h}$ są stowarzyszone w pierścieniu $R[X]$, co przeczy nierozkładalności f. □

12.15. Stwierdzenie. *Niech $f \in R[X]$ będzie wielomianem pierwotnym nierozkładalnym w $R[X]$, $\deg f > 0$. Wówczas f jest elementem pierwszym dziedziny $R[X]$.*

Dowód. Musimy pokazać, że ideał generowany przez wielomian f w pierścieniu $R[X]$ jest pierwszy. Oznaczmy go przez $(f)_{R[X]}$. Z poprzedniego lematu wynika, że wielomian f rozpatrywany jako element $Q(R)[X]$ jest nierozkładalny, a więc pierwszy. Oznaczmy przez $(f)_{Q(R)[X]}$ ideał generowany przez wielomian f w pierścieniu $Q(R)[X]$ – jest on ideałem pierwszym. Mamy $(f)_{R[X]} = i_*^{-1}((f)_{Q(R)[X]})$, gdzie $i_* : R[X] \to Q(R)[X]$ jest włożeniem. Zatem $(f)_{R[X]}$ jest pierwszy jako przeciwobraz ideału pierwszego. □

Możemy teraz zrekapitulować dowód twierdzenia Gaussa.

Dowód Twierdzenia Gaussa Ze stwierdzenia 12.10 wynika, że każdy element jest iloczynem elementów nierozkładalnych. Ze stwierdzeń 12.11 i 12.15 wynika, że rozkład ten jest jednoznaczny. □

12.16. Wniosek. *Jeżeli R jest dziedziną z jednoznacznością rozkładu, to dla każdej liczby naturalnej n , $R[X_1, X_2, \ldots, X_n]$ jest dziedziną z jednoznacznością rozkładu.*

Kryterium Eisensteina

Wiedząc, że pierścienie wielomianów skończonej liczby zmiennych nad ciałem są dziedzinami z jednoznacznością rozkładu, naturalnym jest pytanie o kryterium rozkładalności wielomianu. Odpowiedź na to pytanie jest trudna i nie dysponujemy warunkiem koniecznym i dostatecznym, który by te kwestie rozstrzygał. Niekiedy pomocny jest następujący warunek dostateczny.

12.17. Twierdzenie Kryterium Eisensteina. *Niech R będzie dziedziną z jednoznacznością rozkładu i niech $f \in R[X]$.*

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

Jeżeli istnieje element pierwszy dziedziny R, taki że
$p \nmid a_n$
$p \mid a_i$ *dla* $0 \leq i \leq n-1$
$p^2 \nmid a_0$.
Wówczas f jest elementem nierozkładalnym w $Q(R)[X]$. Jeżli f jest wielomianem pierwotnym, to f jest elementem nierozkładalnym w $R[X]$.

Dowód. Przypuśćmy, że f jest rozkładalny w $Q(R)[X]$. Z lematu 2.14 wynika, że $f = gh$ w $R[X]$, $\deg g > 0$ i $\deg h > 0$. Niech $\pi : R \to R/(p)$ będzie epimorfizmem na dziedzinę całkowitości $R/(p)$, zaś $\pi_* : R[X] \to R/(p)[X]$ homomorfizmem indukowanym. Z warunków zadania wynika, że $\pi_*(g)\pi_*(h) = \pi_*(f) = \pi(a_n)X^n$, $\pi(a_n) \neq 0$. Jeśli popatrzymy na tę równość jak na mającą miejsce w pierścieniu $Q(R/(p))[X]$, to z jednoznaczności rozkładu w $Q(R/(p))[X]$, wynika że $\pi_*(g)$ jest stowarzyszone w nim z X^k a $\pi_*(h)$ z X^l dla pewnych $k, l \in \mathbb{N}$, $k + l = n$. Mamy $k = \deg \pi_*(g) \leq \deg g$ i podobnie $l = \deg \pi_*(h) \leq \deg h$. Ponieważ $n = k + l \leq \deg g + \deg h = \deg f = n$, to $k = \deg g > 0$ i $l = \deg h > 0$. Wynika z tego, że wyraz wolny wielomianu g i wielomianu h jest podzielny przez p, co z kolei pociąga $p^2 \mid a_0$. Sprzeczność. □

13. Ciała. Rozszerzenia ciał.

Z rozważań poprzedniego paragrafu wynika, że jeżeli wielomian f o współczynnikach w ciele K jest nierozkładalny, to pierścień ilorazowy $K[X]/(f)$ jest ciałem zawierającym ciało K. Przytoczmy ponownie szczególne przykłady tej konstrukcji.

13.1. Przykłady.

1. $\mathbb{Z}_2 \subseteq \mathbb{Z}_2[X]/(X^2+X+1)$ jest ciałem czteroelementowym zawierającym $\mathbb{Z}_2$.
2. Rozważmy homomorfizm $\Phi\colon \mathbb{Q}[X] \to \mathbb{R}$, $\Phi(X) = \sqrt{2}$, którego jądrem jest (X^2-2) zaś obrazem podciało ciała liczb rzeczywistych $\{a+b\sqrt{2}\colon a,b \in \mathbb{Q}\}$. Oznaczamy je symbolem $\mathbb{Q}(\sqrt{2})$. Mamy więc $\mathbb{Q} \subseteq \mathbb{Q}[X]/(x^2-2) \cong \mathbb{Q}(\sqrt{2})$. W ciele $\mathbb{Q}(\sqrt{2})$ wielomian X^2-2 jest iloczynem $(X-\sqrt{2})(X+\sqrt{2})$.
3. Rozważmy homomorfizm $\Phi\colon \mathbb{R}[X] \to \mathbb{C}$, $\Phi(X) = i$, którego jądrem jest (X^2+1) zaś obrazem ciało liczb zespolonych. Mamy więc $\mathbb{R} \subseteq \mathbb{R}[X]/(x^2+1) \cong \mathbb{C}$. W ciele $\mathbb{C}$ wielomian $X^2+1 = (X+i)(X-i)$.

Przypomnijmy i uzupełnijmy podstawowe definicje i fakty dotyczące ciał.

13.2. Definicja. *Charakterystyką ciała K nazywamy najmniejszą liczbę naturalną $n \in N$, dla której* $\underbrace{1+\cdots+1}_{n-\text{ razy}} = 0$.

Jeżeli taka liczba nie istnieje, to mówimy, że ciało ma charakterystykę 0. *Charakterystykę ciała K oznaczamy symbolem $\chi(K)$.*

Nietrudno sprawdzić, że charakterystyka ciała, o ile jest różna od zera, musi być liczbą pierwszą.

13.3. Przykłady. Ciałami charakterystyki p są $\mathbb{Z}_p$, $\mathbb{Z}_p[X]/(f)$, gdzie f jest wielomianem nierozkładalnym w $\mathbb{Z}_p[X]$, ciało funkcji wymiernych $Q(\mathbb{Z}_p[X]) = \mathbb{Z}_p(X)$.

Twierdzenie Bézout i grupa multyplikatywna ciała

Niech K będzie ciałem i niech $f \in K[X]$ będzie niezerowym wielomianem. Mówimy, że $a \in K$ jest pierwiastkiem wielomianu f, $f = a_0+a_1X+\cdots+a_nX^n$ jeżeli $f(a) = a_0 + a_1a + \cdots + a_na^n = 0$.

13.4. Twierdzenie Bézout. *Niech K będzie ciałem i niech $f \in K[X]$ i $f \neq 0$. Wówczas*

a) dla $a \in K$, $f(a) = 0$ wtedy i tylko wtedy gdy $(x-a) \mid f$ w $K[X]$;

b) liczba pierwiastków wielomianu f jest mniejsza równa od stopnia $\deg f$.

Dowód. Pierścień $K[X]$ jest dziedziną euklidesową, więc $f = g(X-a)+c$, gdzie $c \in K$ jest wielomianem stopnia 0. Jest jasne, że $f(a) = 0 \iff c = 0$, co dowodzi punktu a). Punkt b) łatwo dowodzimy przez indukcję korzystając z a). □

13.5. Wniosek. *Niech K będzie całem a K^* jego grupą multyplikatywną. Wówczas dowolna skończona podgrupa $G \leqslant K^*$ jest cykliczna.*

Dowód. Skorzystamy z charakteryzacji grup cyklicznych zawartej w Stwierdzeniu 3.4. Niech $k||G|$. Wówczas dla elementu $a \in G$, $o(a)|k$ wtedy i tylko wtedy, gdy $a^k = 1$, czyli wtedy i tylko wtedy, gdy a jest pierwiastkiem wielomianu X^k-1. Z twierdzenia Bézout wynika, że liczba tych pierwiastków jest nie większa od k, zatem G zawiera co najwyżej jedną podgrupę rzędu k, co dowodzi że G jest cykliczna. □

13.6. Wniosek. *Grupa $Aut(\mathbb{Z}_p)$ jest izomorficzna z $\mathbb{Z}_{p-1}$.*

Badanie homomorfizmów ciał zacznijmy od łatwej uwagi:
13.7. Uwaga Niech K będzie ciałem, a $\varphi : K \to L$ homomorfizmem pierścieni. Wówczas dla dowolnego $a \neq 0$, $a \in K$ mamy $\varphi(aa^{-1}) = \varphi(1) = 1 = \varphi(a)\varphi(a^{-1})$, więc $\varphi(a) \neq 0$ i φ jest monomorfizmem. Jeżeli L jest ciałem, to φ jest homomorfizmem ciał.
13.8. Przykład. Niech K będzie ciałem charakterystyki p. Wówczas przekształcenie zadane wzorem $\Phi(x) = x^p$ jest endomorfizmem tego ciała zwanym endomorfizmem Frobeniusa. Jeśli $|K| < \infty$ to endomorfizm Frobeniusa jest automorfizmem. Dla ciała $\mathbb{Z}_p$ jest on identycznością. Dla ciała czteroelementowego z Przykładu 13.1, 1) jest on nietrywialną inwolucją.

Rozszerzenia ciał.

Niech K będzie ciałem a R pierścieniem i niech $K \leqslant R$. Wówczas R ma strukturę przestrzeni liniowej nad K z dodawaniem wektorów i mnożeniem wektorów przez skalary z K zdefiniowanym przez mnożenie w pierścieniu R. Wymiar tej przestrzeni liniowej oznaczamy symbolem $|R : K|$.

13.9. Stwierdzenie. *Niech $f \in K[X]$ będzie wielomianem. Wówczas wymiar $|K[X]/(f) : K|$ pierścienia $K[X]/(f)$ jako przestrzeni liniowej nad K jest równy $deg f$.*

Dowód. Jest oczywiste, że warstwy $1 + (f)$, $X + (f)$, $\ldots$, $X^{n-1} + (f)$ są bazą $K[X]/(f)$ nad K. □

13.10. Stwierdzenie. *Niech K będzie ciałem zawartym w dziedzinie całkowitości R. Jeżeli $|R : K| < \infty$, to R jest ciałem.*

Dowód. Niech $a \in R$, $a \neq 0$. Przekształcenie $\phi_a : R \to R$, $\phi_a(r) = ar$ jest K liniowe i jest monomorfizmem, gdyż R jest dziedziną całkowitości. Jeżeli wymiar R nad K jest skończony to jest epimorfizmem i dla pewnego $r \in R$, $ar = 1$. □

13.11. Definicja. *Jeżeli $K \subseteq L$, gdzie K jest podciałem ciała L, to mówimy, że ciało L jest* **rozszerzeniem** *ciała K. Wymiar $|L : K|$ nazywamy* **stopniem rozszerzenia**.

13.12. Uwaga Jeżeli $K \subseteq L$ jest rozszerzeniem, to $\chi(K) = \chi(L)$.
13.13. Przykład. Jeżeli $\chi(K) = p$, to K jest rozszerzeniem ciała $\mathbb{Z}_p$. Jeżeli $|K : \mathbb{Z}_p| = n$, to ciało K ma p^n elementów. Jeżeli $\chi(K) = 0$, to $\mathbb{Q} \subseteq K$. Ciała $\mathbb{Z}_p$ i $\mathbb{Q}$ nie mają podciał właściwych i nazywamy je ciałami prostymi.

13.14. Wniosek. *Niech $f \in K[X]$ będzie wielomianem nierozkładalnym. Rozszerzenie $K \subseteq K[X]/(f)$ jest stopnia $deg f$.*

13.15. Przykłady. Rozszerzenia $\mathbb{Z}_2 \subseteq \mathbb{Z}_2[X]/(X^2 + X + 1)$, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$, $\mathbb{R} \subseteq \mathbb{C}$ są rozszerzeniami stopnia 2. Rozszerzenia $\mathbb{Q} \subseteq \mathbb{R}$, $K \subseteq K(X)$ są rozszerzeniami nieskończonego stopnia.

13.16. Stwierdzenie. *Niech $K \subseteq L \subseteq M$ będzie ciągiem rozszerzeń. Rozszerzenie $K \subseteq M$ jest skończone wtedy i tylko wtedy, gdy rozszerzenia $K \subseteq L$ i $L \subseteq M$ są skończone. Wówczas*

$$|M : K| = |M : L| \cdot |L : K|.$$

Dowód. Jest oczywiste, że jeżeli $|M : K| < \infty$ to $|L : K| < \infty$ i $|M : L| < \infty$. Niech $|L : K| = n$ i $l_1, \ldots, l_n$ będzie bazą L nad K. Podobnie niech $|M : L| = r$ i $m_1, \ldots, m_r$ będzie bazą M nad L. Łatwo sprawdzić, że $\{l_i m_j\}_{0 \leq i \leq n, 0 \leq j \leq r}$ jest liniowo niezależnym zbiorem generatorów M jako przestrzeni liniowej nad K. □

13.17. Definicja. *Niech $K \subseteq L$ będzie rozszerzeniem. Element $a \in L$ nazywamy algebraicznym nad K wtedy i tylko wtedy, gdy istnieje wielomian $f \in K[X]$ taki, że $f(a) = 0$. Element $a \in L$, ktory nie jest algebraiczny nad K nazywamy elementem przestępnym nad K.*

Niech $K \subseteq L$ będzie rozszerzeniem. Dla elementu $a \in L$, zdefiniujmy

$$K[a] = \{f(a) \mid f \in K[X]\} \leqslant L,$$

$$K(a) = \{\frac{u}{v} \in L \mid u, v \in K[a], v \neq 0\} \leqslant L.$$

Jest jasne, że $K(a)$ jest ciałem ułamków $K[a]$ i najmniejszym podciałem L zawierającym $K \cup \{a\}$ – nazywamy je ciałem generowanym przez a nad K.

13.18. Lemat. *Niech $K \subseteq L$ będzie rozszerzeniem i niech $a \in L$.*
1. *Jeżeli a jest elementem przestępnym nad K, to $K[a] \cong K[X]$ oraz $K(a) \cong K(X)$.*
2. *Jeżeli a jest elementem algebraicznym nad K, to $|K[a] : K| \leq \deg f$, gdzie f jest dowolnym niezerowym wielomianem dla którego $f(a) = 0$.*

Dowód. Niech $\Theta : K[X] \to K[a]$ będzie zadane wzorem $\Theta(f) = f(a)$. Jest jasne, że

$$K[X]/\ker\Theta \cong K[a].$$

Jeżeli a jest elementem przestępnym, to $\ker\Theta = 0$, i $K[X] \cong K[a]$, co dowodzi punktu 1.
Jeżeli a jest elementem algebraicznym i $f(a) = 0$, to $(f) \leqslant \ker\Theta$ i mamy epimorfizm $\pi : K[X]/(f) \twoheadrightarrow K[X]/\ker\Theta \cong K[a]$ przestrzeni liniowych nad K. Zatem zbiór $\{1, a, \ldots, a^{n-1}\}$, $n = \deg f$, generuje przestrzeń $K[a]$ nad K gdyż jest obrazem bazy $1 + (f), X + (f), \ldots, X^{n-1} + (f)$ przestrzeni liniowej $K[X]/(f)$ nad K przy epimorfizmie π. □

13.19. Stwierdzenie. *Niech $K \subseteq L$ będzie rozszerzeniem i niech $a \in L$. Następujące warunki są równoważne:*
1. *a jest elementem algebraicznym;*
2. *$|K[a] : K| < \infty$;*
3. *$K[a] = K(a)$.*

Dowód. Implikacja 1. $\implies$ 2. wynika z poprzedniego stwierdzenia.
2. $\implies$ 3. Pierścień $K[a]$ jako podpierścień ciała jest oczywiście dziedziną całkowitości więc ze Stwierdzenia 13.10 wynika, że $K[a]$ jest ciałem, a zatem jest równy swojemu ciału ułamków $K(a)$.
3. $\implies$ 1. Gdyby a było elementem przestępnym, to ze Stwierdzenia 13.18 zachodziłoby $K[a] \cong K[X]$, ale $K[X]$ nie jest ciałem, więc $K[a]$ byłoby różne od swojego ciała ułamków. □

13.20. Definicja. *Niech $K \subseteq L$ będzie rozszerzeniem i niech $a \in L$ będzie elementem algebraicznym nad K. Stpień rozszerzenia $|K(a) : K|$ nazywamy* **stopniem elementu** *a nad K.*

Przyjrzymy się teraz czemu jest równy stopień elementu algebraicznego.

13.21. Stwierdzenie. *Niech $K \subseteq L$ będzie rozszerzeniem i niech $a \in L$ będzie elementem algebraicznym nad K. Następujące liczby naturalne są równe:*
1. *stopień elementu a nad K;*
2. *stopień nierozkładalnego wielomianu $f \in K[X]$ dla którego $f(a) = 0$;*
3. *najmniejszy stopień takiego niezerowego wielomianu $f \in K[X]$, że $f(a) = 0$.*

Dowód. Jak wiemy $K[a] \cong K[X]/\ker\Theta$, gdzie $\Theta : K[X] \to K[a]$ jest epimorfizmem zadanym wzorem $\Theta(f) = f(a)$. Z poprzedniego stwierdzenia, jeżeli a jest elementem algebraicznym to $K(a) = K[a]$ i stopień elementu a jest równy $|K[a] : K|$. Pierścień $K[X]$ jest dziedziną euklidesową z waluacją będącą stopniem wielomianu. Niech $(f) = \ker\Theta \lhd K[X]$. Wielomian f jest wyznaczony jednoznacznie z dokładnością do stowarzyszenia i jest on wielomianem minimalnego stopnia spośród należących do $\ker\Theta$. Ponieważ $K[X]/\ker\Theta \cong K[a] = K(a)$ jest ciałem, to (f) jest maksymalny. Zatem f jest elementem pierwszym, a więc nierozkładalnym, Jest to jedyny z dokładnością do stowarzyszenia wielomian nierozkładalny w ideale (f), gdyż każdy inny jest postaci $f \cdot g$ dla pewego $g \in K[X]$. Z wniosku 13.14 wynika, że $|K[X]/(f) : K| = \deg f$.

□

13.22. Definicja. *Niech $K \subseteq L$ będzie rozszerzeniem i niech $a \in L$ będzie elementem algebraicznym nad K. Nierozkładalny w $K[X]$ wielomian f, taki że $f(a) = 0$ nazywamy* **wielomianem minimalnym elementu** *a.*

13.23. Definicja. *Mówimy, że rozszerzenie $K \subseteq L$ jest algebraiczne jeżeli każdy element ciała L jest algebraiczny nad K.*

Ze Stwierdzenia 13.19 wynika następujący

13.24. Wniosek. *Rozszerzenie skończonego stopnia jest algebraiczne.*

Stwierdzenie odwrotne nie jest prawdziwe.

13.25. Stwierdzenie. *Niech $K \subseteq L$ będzie rozszerzeniem. Wówczas zbiór A wszystkich elementów L algebraicznych nad K jest podciałem L.*

Dowód. Niech $a, b \in A$. Rozpatrzmy rozszerzenie $K \subseteq K(a)$ – jest ono skończone. Jeżeli $b \in L$ jest algebraiczne nad K, to jest algebraiczne nad $K(a)$, więc rozszerzenie $K(a) \subseteq K(a)(b) = K(a, b)$ też jest skończone. Mamy ciąg rozszerzeń:

$$K \subseteq K(a) \subseteq K(a, b).$$

Wynika z tego, że rozszerzenie $K \subseteq K(a, b)$ jest skończone a więc algebraiczne. Zatem elementy $a + b$, $a - b$, $a - b$, a^{-1} jako należące do $K(a, b)$ są algebraiczne.

□

13.26. Przykład. Rozważmy rozszerzenie $\mathbb{Q} \subseteq \mathbb{C}$ i niech A oznacza liczby $\mathbb{C}$ algebraiczne nad $\mathbb{Q}$ – nazywamy je liczbami algebraicznymi. Rozszerzenie algebraiczne $\mathbb{Q} \subseteq A$ jest nieskończonego stopnia. Niech $p \in \mathbb{N}$ będzie liczbą pierwszą. Wielomian $X^n - p$ jest nierozkładalny w $\mathbb{Q}[X]$ z kryterium Eisensteina i jest wielomianem minimalnym dla $\sqrt[n]{p} \in A$. Zatem $|A : \mathbb{Q}| \geq n$ dla każdego $n \in \mathbb{N}$ i $|A : \mathbb{Q}| = \infty$.

Na koniec przyjrzyjmy się ponownie rozszerzeniu $K \subseteq K[X]/(f) = L$, gdzie $f \in K[X]$ jest wielomianem nierozkładalnym. Niech $a = X + (f)$. Wielomian f jako wielomian $L[X]$ jest już rozkładalny, bo a jest jego pierwiastkiem. Tak więc możemy uważać, że L powstało z K przez dodanie pierwiastka a.

13.27. Definicja. *Ciało K nazywa się* **algebraicznie domknięte** *jeżeli każdy wielomian dodatniego stopnia ma w ciele K co najmniej jeden pierwiastek.*

Nietrudno zauważyć,że ciało K jest algebraicznie domknięte jeżeli każdy wielomian o współczynnikach z K dodatniego stopnia jest iloczynem wielomianów stopnia 1. Podstawowe twierdzenie algebry mówi, że ciało liczb zespolonych $\mathbb{C}$ jest algebraicznie domknięte.

Możemy mając dane ciało K próbować skonstruować ciało algebraicznie domknięte dołączając kolejno pierwiastki wielomianów.

13.28. Definicja. *Rozszerzenie $K \subseteq L$ nazywamy algebraicznym domknięciem ciała K wtedy i tylko wtedy, gdy rozszerzenie to jest algebraiczne i L jest ciałem algebraicznie domkniętym.*

13.29. Przykłady.1. $\mathbb{Q} \subseteq A$ jest algebraicznym domknięciem ciała liczb wymiernych.

2. $\mathbb{R} \subseteq \mathbb{C}$ jest algebraicznym domknięciem ciała liczb rzeczywistych.

13.30. Twierdzenie. *Dla każdego ciała K istnieje algebraiczne domknięcie $K \subseteq L$ i jest ono wyznaczone jednoznacznie z dokładnością do izomorfizmu.*

KONIEC