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.