Faktoryzacja
WWW8

Tadek Krassowski
Maciek Malinowski

25 maja 2012

1 Grupy

Nie przekręcaj nazwy mojej grupy (...)
Płomień 81, "Kiedy powiem na osiedlu"

Definicja 1.1. Mówimy, że $(G, *)$ jest grupą, jeśli G jest zbiorem, $*$ jest działaniem dwuargumentowym określonym na G i zachodzą następujące warunki:

1. Jeśli $a, b \in G$, to $a * b \in G$. (G jest zamknięty ze względu na $*$)
2. Jeśli $a, b, c \in G$, to $(a * b) * c = a * (b * c)$. ($*$ jest łączne)
3. Istnieje element $e \in G$, taki że $e * a = a = a * e$ dla każdego $a \in G$. (istnienie elementu neutralnego)
4. Jeśli $a \in G$, to istnieje element $a^{-1} \in G$, taki że $a * a^{-1} = e$. (istnienie elementu odwrotnego)

Jeśli zbiór G jest skończony, to jego moc $|G|$ nazywany rzędem grupy. W przeciwnym razie mówimy, że rząd grupy wynosi nieskończoność.
Uwaga! Dla $a, b \in (G, *)$ często stosujemy notację $ab = a * b$.

Definicja 1.2. Grupę $(G, *)$ nazywamy abelową (lub przemienną), jeżeli $a*b = b * a$ dla dowolnej pary elementów $a, b \in G$.

Lemat 1.1. Niech $(G, *)$ będzie grupą.

1. Element neutralny e jest wyznaczony jednoznacznie.
2. Jeśli $a \in G$, to $a^{-1}*a = e$ oraz element a^{-1} jest wyznaczony jednoznacznie.

Dowód.

1. Przypuśćmy, że $e, f \in G$ są elementami neutralnymi. Wtedy $e = e*f = f$.
2. Dowód pozostawiamy jako ćwiczenie.

□

Definicja 1.3. Niech $(G, *)$ będzie grupą i niech $g \in G$. Najmniejszą liczbę naturalną k, taką że $g^k = e$ nazywamy rzędem g i oznaczamy $\mathrm{o}(g)$ lub $\mathrm{ord}(g)$. Jeśli taka liczba k nie istnieje, mówimy, że rząd g wynosi nieskończoność.

Definicja 1.4. Niech $(G, *)$ będzie grupą. Podzbiór H zbioru G nazywamy podgrupą $(G, *)$, jeśli $(H, *)$ jest grupą i piszemy $H \leqslant G$. Jeśli $H \neq G$ to piszemy $H < G$. Indeksem $|G/H|$ grupy H w G nazywamy liczbę $\frac{|G|}{|H|}$.

Definicja 1.5. Niech H i K będą grupami. Wtedy iloczynem tych grup nazywamy zbiór $H \times K = \{(h,k) : h \in H, k \in K\}$. Tworzy on grupę z działaniem określonym przez $(h_1,k_1) * (h_2,k_2) = (h_1 *_H h_2, k_1 *_K k_2)$.

Definicja 1.6. Niech $(G,*)$ będzie grupą i niech $|G| = n$. Jeśli istnieje element $g \in G$, taki że $\mathrm{ord}(g) = n$, to G nazywamy grupą cykliczną generowaną przez g i piszemy $G =< g >$. Ogólniej, jeśli $g_1, g_2, ..., g_m \in G$ to grupą $< g_1, g_2, ..., g_m >$ generowaną przez $g_1, g_2, ..., g_m$ nazywamy najmniejszą podgrupę G zawierającą $g_1, g_2, ..., g_m$.

Przykłady grup.

1. Grupa trywialna, $\{e\}$.
2. Grupa liczb całkowitych z działaniem dodawania, $(\mathbb{Z}, +)$.
3. Grupa liczb wymiernych bez zera z działaniem mnożenia, $(\mathbb{Q} \setminus \{0\}, \cdot)$.
4. Grupa liczb całkowitych nieujemnych mniejszych niż n z działaniem dodawania modulo n, $(\{0,1,2,...,p-1\}, + \pmod n)$ (grupa cykliczna C_n o rzędzie n).
5. Grupa liczb całkowitych dodatnich mniejszych niż p, z działaniem mnożenia modulo p, dla p pierwszego, $(\{1,2,...,p-1\}, \cdot \pmod p)$.
6. Grupa permutacji ciągu $(1,2,...,n)$ z działaniem złożenia funkcji, S_n.
7. Grupa diedralna izometrii płaszczyzny przekształcających n-kąt foremny na samego siebie z działaniem złożenia funkcji, D_{2n}.
8. Grupa macierzy $n \times n$ o współczynnikach zespolonych i wyznaczniku różnym od zera z działaniem mnożenia macierzy, $\mathrm{GL}_2(\mathbb{C})$.

Ćwiczenie. Udowodnić, że powyższe przykłady są grupami. Jakie są ich elementy neutralne? Które z nich są abelowe? Jakie są ich rzędy? Jakie są w nich możliwe rzędy elementów? Jakie są ich możliwe podgrupy?

Definicja 1.7. Niech G będzie grupą, a H jej podgrupą. Wtedy lewą warstwę $g \in G$ względem H definiujemy jako $gH = \{g * h : h \in H\}$. Analogicznie definiujemy prawą warstwę.

Twierdzenie 1.1. (Lagrange'a) Jeśli grupa H jest podgrupą grupy G, to $|H| \,|\, |G|$.
Dowód. Udowodnimy, że zbiór lewych warstw względem H stanowi partycję G. Istotnie, jeśli $g \in G$, to $g \in gH$. Przypućmy teraz, że $a, b \in G$ oraz $aH \cap bH \neq \emptyset$ i niech $c \in aH \cap bH$. Wtedy $c = ah_1$ dla pewnego $h_1 \in H$, a więc dla każdego $h \in H$ mamy $ch = ah_1h \in aH$, a więc $cH \subseteq aH$. Ale mamy również $ch_1^{-1} = a$, a więc podobnie $aH \subseteq cH$. Stąd $aH = cH$. Podobnie dowodzimy, że $bH = cH$, a

więc $aH = bH$. Zatem różne warstwy względem H mają albo puste przecięcia, albo są tą samą warstwą i pokrywają G w całości, więc tworzą partycję G. Ale funkcja $\theta : H \to gH$, taka że $\theta(h) = gh$ jest bijekcją dla każdego g, a więc wszystkie warstwy względem H mają rozmiar $|H|$, skąd $|H| \,|\, |G|$.

□

Definicja 1.8. Niech $(G, *_G)$ oraz $(H, *_H)$ będą grupami. Funkcja $\theta : G \to H$ jest homomorfizmem, jeżeli $\theta(a *_G b) = \theta(a) *_H \theta(b)$ dla każdych $a, b \in G$. Obrazem $\theta(G)$ homomorfizmu nazywamy zbiór $\{\theta(g) : g \in G\}$, a jego jądrem $\ker \theta$ zbiór $\{g \in G : \theta(g) = e_H\}$. Funkcja $\psi : G \to H$ jest izomorfizmem, jeśli jest homomorfizmem i bijekcją. Grupy G i H nazywamy izomorficznymi, jeśli istnieje izomorfizm $\psi : G \to H$ i piszemy $G \simeq H$.

Lemat 1.2. Niech $\theta : G \to H$ będzie homomorfizmem, wtedy

1. $\theta(e_G) = e_H$.
2. $\theta(g)^{-1} = \theta(g^{-1})$.

Dowód. Dowód pozostawiamy jako ćwiczenie.

□

Definicja 1.9. Podgrupę H grupy G nazywamy normalną i piszemy $H \lhd G$ jeśli $gH = Hg$ dla każdego $g \in G$. Równoważnie, $H \lhd G$ jeśli $gHg^{-1} = H$ dla każdego $g \in G$, gdzie $gHg^{-1} = \{ghg^{-1} : h \in H\}$.

Twierdzenie 1.2. Niech G będzie grupą i niech $H \lhd G$. Zbiór $G/H = \{gH : g \in G\}$ tworzy grupę z działaniem mnożenia $(g_1H) \cdot (g_2H) = g_1g_2H$.
Dowód.

1. Mnożenie w G/H jest dobrze zdefiniowane - istotnie, jeśli $g_1H = f_1H$ i $g_2H = f_2H$, to $f_2^{-1}f_1^{-1}g_1g_2 = f_2^{-1}h_1g = h_2f_2^{-1}g_2 = h_2h_3 \in H$, dla pewnych $h_1, h_2, h_3 \in H$, więc $g_1g_2H = f_1f_2H$.
2. G/H spełnia aksjomaty grupy - pozostawiamy do udowodnienia jako ćwiczenie.

□

Twierdzenie 1.3. (o izomorfizmie) Niech $\theta : G \to H$ będzie homomorfizmem grup. Wtedy

1. $\theta(G) \leqslant H$.
2. $\ker \theta \lhd G$.
3. $G/\ker \theta \simeq \theta(G)$.

Dowód.

1. Pozostawiamy jako ćwiczenie.
2. Pozostawiamy jako ćwiczenie.
3. Niech $\overline{\theta} : G/\ker\,\theta \to \theta(G)$ będzie funkcją, taką że $\overline{\theta}(g\ker\,\theta) = \theta(g)$ dla każdego $g \in G$. Wykażemy, że $\overline{\theta}$ jest izomorfizmem. Jest to dobrze zdefiniowana funkcja, bo $g_1\ker\,\theta = g_2\ker\,\theta \Leftrightarrow g_1^{-1}g_2 \in \ker\,\theta \Leftrightarrow \theta(g_1^{-1}g_2) = e \Leftrightarrow \theta(g_1) = \theta(g_2) \Leftrightarrow \overline{\theta}(g_1\ker\,\theta) = \overline{\theta}(g_2\ker\,\theta)$. Przejście tymi implikacjami w drugą stronę, wykazuje różnowartościowość $\overline{\theta}$, więc $\overline{\theta}$ jest bijekcją. Ponadto $\overline{\theta}$ jest homomorfizmem, bo $\overline{\theta}(g_1\ker\,\theta \cdot g_2\ker\,\theta) = \overline{\theta}(g_1g_2\ker\,\theta) = \theta(g_1g_2) = \theta(g_1)\theta(g_2) = \overline{\theta}(g_1\ker\,\theta)\overline{\theta}(g_2\ker\,\theta)$.

□

2 Pierścienie

Ciało ma jedynie trywialne ideały.
Paulo Coelho

Definicja 2.1. Mówimy, że $(R, +, \cdot, 0)$ jest pierścieniem, jeśli R jest zbiorem, $+, \cdot$ są działaniami dwuargumentowymi określonymi na R i zachodzą następujące warunki:

1. $(R, +)$ jest grupą abelową z elementem neutralnym 0.
2. $\cdot$ jest łączne i rozdzielne względem dodawania, to znaczy $x(y+z) = xy+xz$ oraz $(y + z)x = yx + zx$ dla każdych $x, y, z \in R$.

Jeśli $x\cdot y = y\cdot x$ dla każdych $x, y \in R$, to R nazywamy pierścieniem przemiennym. Jeśli istnieje element $1 \in R$, taki że $1 \cdot x = x = x \cdot 1$ dla każdego $x \in R$, to R nazywamy pierścieniem z jedynką. W tym skrypcie rozważamy tylko pierścienie przemienne z jedynką.

Definicja 2.2. Pierścień przemienny z jedynką R nazywamy ciałem, jeżeli dla każdego elementu $x \in R$ istnieje element $y \in R$ spełniający $xy = 1$.

Przykłady pierścieni.

1. $\mathbb{Z}$ z intuicyjnymi działaniami.
2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
3. $\mathbb{Z}_n$ dla każdej liczby naturalnej n.
4. $\mathbb{R}[X]$ - zbiór wielomianów o współczynnikach rzeczywistych.
5. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ (gęsty podzbiór $\mathbb{R}$).

6. $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ - wszystkie punkty na płaszczyźnie zespolonej o całkowitych częściach rzeczywistej i urojonej.

7. Zbiór funkcji z $\mathbb{R}$ w $\mathbb{R}$ z działaniami dodawania i mnożenia określonymi punktowo - $(f + g)(x) = f(x) + g(x)$, $(f \cdot g)(x) = f(x) \cdot g(x)$.

8. C$[0, 1]$ - zbiór funkcji ciągłych z $[0, 1]$ w $\mathbb{R}$.

9. $\mathbb{P}(X)$ - zbiór wszystkich pozdbiorów dowolnego zbioru X z działaniami $A + B = (A \setminus B) \cup (B \setminus A)$, $A \cdot B = A \cap B$.

10. $R = \{0\}$ - pierścień trywialny.

Ćwiczenie. Udowodnij, że podane przykłady są pierścieniami. Jakie są w nich elementy neutralne dodawania i mnożenia? Które z nich są ciałami?

Lemat 2.1. Niech R będzie pierścieniem przemiennym z jedynką.

1. $0 \cdot x = 0$ dla każdego $x \in R$.

2. $(-x)y = -xy$ dla każdych $x, y \in R$.

Dowód. Dowód pozostawiamy jako ćwiczenie.

□

Definicja 2.3. Podzbiór S pierścienia R nazywamy podpierścieniem R jeśli jest pierścieniem z tymi samymi operacjami i tym samym elementem neutralnym mnożenia.
Przykład.
$\mathbb{Z}$ w $\mathbb{Q}$,
R w $R[X]$ dla dowolnego pierścienia R (definicja 2.4).
Uwaga! $2\mathbb{Z}$ nie jest podpierścieniem $\mathbb{Z}$, ponieważ nie zawiera elementu neutralnego mnożenia. Podobnie $\{0\}$ nie jest podpierścieniem w $\mathbb{Z}$.

Definicja 2.4. Niech R, S będą pierścieniami. Ich sumą prostą nazywamy zbiór $R \oplus S = \{(x, y) : x \in R, y \in S\}$, który tworzy pierścień z operacjami $(x, y) + (x', y') = (x +_R x', y +_S y')$ i $(x, y) \cdot (x', y') = (x \cdot_R x', y \cdot_S y')$. Element neutralny dodawania to $(0_R, 0_S)$, element neutralny mnożenia to $(1_R, 1_S)$.
Przykład.
$\mathbb{Z} \oplus \mathbb{Z} = \mathbb{Z}^2$.

Definicja 2.5. Niech R będzie pierścieniem. Zbiór wielomianów, o współczynnikach w R definiujemy jako $R[X] = \{(a_0, a_1, a_2, ...) : a_n \in R \ \forall n$ i $a_i = 0 \ \forall i \geqslant N$ dla pewnego N$\}$. Stopniem wielomianu nazywamy największe d spełniające $a_d \neq 0$, przy czym wielomian zerowy $(0, 0, ...)$ nie ma stopnia. Wielomiany zazwyczaj zapisujemy jako $\sum_{i=0}^{n} a_i X^i$. $R[X]$ tworzy pierścień z działaniami $(\sum_{i=0}^{n} a_i X^i) + (\sum_{i=0}^{n} b_i X^i) = \sum_{i=0}^{n} (a_i + b_i) X^i$ i $(\sum_{i=0}^{n} a_i X^i) \cdot (\sum_{i=0}^{n} b_i X^i) =$

$\sum_{i=0}^{2n}(\sum_{j=0}^{i} a_j b_{i-j})X^i$. Przy danym $f = \sum a_i X^i \in R[X]$ możemy rozważyć funkcję $\overline{f} : R \to R$ taką że $\overline{f}(x) = \sum a_i x^i$.
Uwaga! W pierścieniu $\mathbb{Z}_2[X]$ mamy wielomian $f = X^2 + X$ spełniający $f \neq 0$ (bo stopień f wynosi 2), ale $\overline{f}(x) = 0$ dla każdego $x \in \mathbb{Z}_2$.

Definicja 2.6. Podzbiór I pierścienia R nazywamy ideałem, gdy jest podgrupą $(R, +)$ oraz $xr \in I$ dla każdych $x \in I$, $r \in R$.
Przykład.
$2\mathbb{Z}$ jest ideałem w $\mathbb{Z}$.