Grupy, pierścienie i ciała

Mateusz Trubiłowicz
mateusz.trubilowicz@gmail.com

Zadania kwalifikacyjne do moich warsztatów podzieliłem na dwie kategorie: Zadania obowiązkowe i zadania dodatkowe. Pierwsza kategoria zadań jest, jak sama nazwa wskazuje, obligatoryjna. Podczas warsztatów będę uznawał wiadomości zawarte w poleceniach i opisach dodatkowych za już przyswojone. Zadania te będą punktowane zgodnie z liczbami zawartymi w nawiasach. Nie wszystkie zadania są bezpośrednio połączone z tematem warsztatów, niektóre mają za zadanie pokazać przykłady, którym dokładniej będziemy przyglądać się podczas zajęć.

Polecenia drugiej kategorii, „dodatkowe", zawierają pewne przesłanki dotyczące tego, czym będziemy się zajmować podczas warsztatów. Zadania z tej serii nie są bynajmniej trudniejsze a zastanowienie się nad nimi może pomóc zrozumieć treść warsztatów. Punktacja za każde zadanie podana jest w nawiasach. Pierwsza liczba w nawiasie oznacza gwarantowaną liczbę punktów za rozwiązanie zadania. Druga liczba w nawiasie oznacza liczbę punktów dodatkowych za dane zadanie. Ostateczna liczba punktów za zadanie zostanie przyznana zgodnie z następującą formułą: $l=g+g\cdot d/s$, gdzie l-liczba punktów za zadanie, g-liczba zdobytych punktów z puli punktów gwarantowanych, d-liczba punktów dodatkowych za dane zadanie, s-suma punktów gwarantowanych zdobytych za to zadanie przez wszystkich uczestników.

Rozwiązania zadań proszę przesyłać na podany powyżej adres mejlowy. W razie wszelkich pytań lub wątpliwości odnośnie treści zadań można pisać do mnie na moje prywatne, częściej sprawdzane konto: mt394587@students.mimuw.edu.pl Prosiłbym również o napisanie wiadomości na ten adres w przypadku wysłania zadań przed wymaganym terminem.

1. Zadania obowiązkowe

***Definicja*: Grupą** nazywamy obiekt $G=(X,*)$, gdzie X-zbiór, $*$-działanie dwuargumentowe zdefiniowane na zbiorze X spełniające:
1. $\forall\ a,b,c\in X:(a*b)*c=a*(b*c)$ – tę cechę nazywamy **łącznością**
2. $\exists\ e\in X:\forall\ a\in X\ a*e=e*a=a$ – element e nazywamy **elementem neutralnym**
3. $\forall\ a\in X\exists\ b\in X:a*b=b*a=e$ – element b nazywamy **elementem odwrotnym** do a (często oznaczanym przez $-a$ lub a^{-1}).

Jeśli ponadto $\forall\ a,b\in X:a*b=b*a$to grupę G nazywamy **abelową** (przemienną).

Często w zapisie przyjmuje się konwencję, że $\underbrace{a*a*a*\ldots*a}_{n\,razy}=a^n$ (analogicznie

$\underbrace{a^{-1}*a^{-1}*a^{-1}*\ldots*a^{-1}}_{n\,razy}=a^{-n}$

Przykłady grup: $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+),(\mathbb{R}^*,\cdot)$, gdzie $\mathbb{R}^*\stackrel{\text{def}}{=}\mathbb{R}\setminus\{0\}$, $+$ jest standardową operacją dodawania, zaś $\cdot$ standardową operacją mnożenia.
Szczególnym przykładem grupy jest grupa izometrii własnych wielokąta foremnego, nazywana **grupą diedralną** i oznaczana przez D_n, gdzie n - liczba wierzchołków wielokąta.

Zad.1. (1p.) Pokazać, że element neutralny e oraz element odwrotny do wybranego $a\in X$ są określone w sposób jednoznaczny.

Zad.2. (3p.) Uzasadnić, które z poniższych obiektów są grupami oraz z jakich powodów pozostałe nie są:
-$(\mathbb{R}\setminus\{-1\},^{\circ})$, gdzie $a^{\circ}b=a+b+a\cdot b$
-$(\mathbb{R},\nrightarrow)$, gdzie $a\nrightarrow b=|a|\cdot b$
-$(\mathbb{Z}_{15},\otimes)$, gdzie $\mathbb{Z}_{15}\overset{def}{=}\{0,1,\ldots,14\}$ i $a\otimes b=a\cdot b\,(mod\,15)$, analogicznie $\forall n\in\mathbb{N}:\mathbb{Z}_n\overset{def}{=}\{0,1,\ldots,n-1\}$
-$(\mathbb{Z}_{15,}\oplus)$, gdzie $a\oplus b=a+b\,(mod\,15)$
- $(G,\boldsymbol{\cdot})$, gdzie $(G,\star)$ jest grupą, zaś działanie $\boldsymbol{\cdot}$ jest zdefiniowane: $\forall a,b\in G: a\boldsymbol{\cdot}b=b\star a$

Zad.3. (2p.)Wypisać wszystkie $z\in\mathbb{C}: z^{15}=1\wedge\forall n\in\mathbb{Z}_{15}\setminus\{0\}\, z^n\neq 1$. Pokazać, że zbiór pierwiastków n-tego stopnia z jedynki dla dowolnego $n\in\mathbb{N}$ wraz z działaniem mnożenia w liczbach zespolonych jest grupą (często oznaczaną przez C_n)

Definicja: Niech $G=(X,*)$ - grupa. Mówimy, że $H=(Y,*)$ jest **podgrupą** G , jeśli:
- $\forall a\in H: a^{-1}\in H$
- $\forall a,b\in H: a*b\in H$

Definicja: Niech $G=(X,\blacklozenge), H=(Y,\boldsymbol{\cdot})$ - grupy. Funkcję $f: G\to H$ nazywamy **homomorfizmem**, jeśli $\forall a,b\in X: f(a\blacklozenge b)=f(a)\boldsymbol{\cdot}f(b)$. Jeśli ponadto funkcja f jest różnowartościowa, nazywamy ją zanurzeniem grupy G w grupę H . Jeśli f jest homomorfizmem oraz bijekcją (różnowartościowa i „na"), to nazywamy ją **izomorfizmem** i mówimy, że grupy G i H są **izomorficzne**.

Zad.4. (1p.) Niech $G=(X,*)$ Zdefiniujmy $f: G\to G$ dane wzorem: $f(x)=x^2$. Uzasadnij, że f jest homomorfizmem $\Leftrightarrow$ G jest przemienna

Zad. 5. (1p.) Niech G - grupa, $P(G)$ - zbiór wszystkich podgrup grupy G. Uzasadnij, że relacja $\cong$ zdefiniowana na $P(G)$ w następujący sposób: $\forall A,B\in G: A\cong B\Leftrightarrow A\,i\,B\,są\,izomorficzne$ jest relacją równoważności.

Zad.6. (2p.) Które z grup z zadania 2. są izomorficzne z grupami: C_{15} , $(\mathbb{R}^*,\cdot)$?

Definicja: **Permutacją** nazywamy dowolną bijekcję $\sigma: X\to X$. Niech $X=\{a,b,c,d\}$ oraz $\sigma(a)=b,\sigma(b)=a,\sigma(c)=d,\sigma(d)=c$. Trzy podstawowe formy zapisu takiej permutacji to:

$$\begin{pmatrix}a & b & c & d\\ b & a & d & c\end{pmatrix};(a,b)(c,d),\begin{pmatrix}0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$$ (w ostatniej macierzy zapisujemy w kolumnie, na który element przechodzi element odpowiadający numerowi wiersza).

Zad.7. (3p.) Niech $X=\{1,2,3,4,5\}$. oraz $\sigma: X\to X$ dana jest wzorem:
$\sigma(x)=2\otimes(x-1)+1=2\cdot(x-1)(mod\,5)+1$, zaś $\tau: X\to X$ jest określona następująco:
$(1,5)(2,3)(4)$ (ostatni nawias można pominąć, wpisałem go dla jasności i wytłumaczenia, że się tego nie robi). Zapisz σ na wszystkie trzy wymienione powyżej sposoby oraz na jeden, wybrany przez siebie, sposób zapisz $\sigma\circ\tau: X\to X$ oraz $\tau\circ\sigma^{-1}: X\to X$, gdzie $\circ$ oznacza złożenie funkcji, zaś σ^{-1} taką funkcję, że $\sigma\circ\sigma^{-1}=id_X$. Następnie udowodnij, że zbiór wszystkich permutacji wraz z działaniem składania funkcji tworzy grupę (oznaczaną często przez S_5 lub Σ_5 .

Definicja: Rzędem grupy $G=(X,*)$ nazywamy $|X|$, czyli ilość elementów w grupie G. Jeśli $|X|<\infty$, to mówimy, że grupa G jest skończona.

Zad. 8. (1p.) Niech $G=(X,*), \emptyset \neq Y \subseteq X$. oraz Z jest częścią wspólną wszystkich podzbiorów X zawierających Y. Udowodnij, że $H=(Z,*)$ jest podgrupą G.

Definicja: H z powyższego zadania nazywamy ***podgrupą generowaną przez*** Y i oznaczamy często $H=\langle Y \rangle$.

Rzędem elementu $a \in X$ nazywamy $|\langle \{a\} \rangle|$

Zad. 9. (1p.) Oblicz rząd elementu $-i$ w grupie C_8.

Definicja: **Pierścieniem** nazywamy $R=(X,+,\cdot)$ takie, że:
- $(R,+)$ jest grupą abelową (przemienną),
- $\cdot$ jest łączne na R (tzn. $\forall a,b \in R: (a \cdot b) \cdot c = a \cdot (b \cdot c)$)
- $\forall a,b,c \in R: a \cdot (b+c) = a \cdot b + a \cdot c$
- $\forall a,b,c \in R: (b+c) \cdot a = b \cdot a + c \cdot a$

Jeśli $\forall a,b \in R: a \cdot b = b \cdot a$ to mówimy, że R jest **przemienny**
Jeśli $\exists e \in R \, \forall a \in R: e \cdot a = a \cdot e = e$ to mówimy, że R jest **pierścieniem z 1** i oznaczamy $e=1$.
Przykłady:
- $\mathbb{Z}$
- $n\mathbb{Z} = \{n \cdot z : z \in \mathbb{Z}\}$
- $\mathbb{R}$
-zbiór wielomianów o współczynnikach z $\mathbb{R}$
- $\mathbb{Z}[i] = \{a + b \cdot i : a,b \in \mathbb{Z}\} \subset \mathbb{C}$
Ze standardowymi działaniami dodawania i mnożenia.

Zad.10. (2p.) Niech $X \neq \emptyset$, $P(X)$ – zbiór wszystkich podzbiorów X .
Dla $A,B \in P(X)$ zdefiniujmy: $A \boxplus B = (A \setminus B) \cup (B \setminus A); A \boxtimes B = A \cap B$.
Pokaż, że $(P(X), \boxplus, \boxtimes)$ jest pierścieniem przemiennym z jedynką.

Definicja: Jeśli R – pierścień przemienny z 1, t.że $(R \setminus \{0\}, \cdot)$ jest grupą, to R nazywamy **ciałem**.
Przykłady:
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ze standardowymi działaniami dodawania i mnożenia,
- $\mathbb{Z}_p$, gdzie p – liczba pierwsza, z działaniami $(\oplus, \otimes)$

Zad.11. (2p.)Podziel z resztą wielomian $x^5+2x^4+x^3+4x^2$ przez x^3-2x+2 nad $\mathbb{R}$ oraz nad $\mathbb{Z}_5$ (czyli odpowiednie działania trzeba wykonywać zgodnie z tym, jak są zdefiniowane w danym ciele).

Zad.12. (2p.) Policz, korzystając wyłącznie z kalkulatora prostego, NWW liczb 20 227 oraz 17 363.

2. Zadania dodatkowe

Zad. A. (2p. 10p.) Ania ma 71 koleżanek, które wszystkie mają urodziny tego samego dnia. Postanowiła zrobić im dwa różne rodzaje prezentów: bransoletki i paczki cukierków. Nie byle jakie zresztą. Ponieważ miała bardzo dużo czasu i pieniędzy, kupiła koraliki w 67 kolorach i ułożyła z nich wszystkie możliwe łańcuszki zgodne z następującymi zasadami:
-każde dwa łańcuszki są różne (zakładamy, że łańcuszki są równe wtedy i tylko wtedy, gdy koraliki były nawlekane w tej samej kolejności. W szczególności odbicia symetryczne typu „a,b" i „b,a" są różnymi łańcuszkami),
-wszystkie łańcuszki mają po 67 koralików,
-dowolne dwa koraliki w jednym łańcuszku są różnego koloru.
Poza tym kupiła cukierki o 112 smakach i powkładała je do tubek na wszystkie możliwe sposoby zgodne z

następującymi zasadami:
-w każdej tubce jest 211 cukierków (niekoniecznie różnych),
-każde dwie tubki są różne (jak powyżej, zakładamy, że tubki są równe wtedy i tylko wtedy, gdy cukierki były wrzucane w tej samej kolejności).
Obładowana tymi prezentami poszła na wspólne przyjęcie urodzinowe wszystkich swoich koleżanek gdzie wręczyła każdej z nich dokładnie tyle samo podarunków (niekoniecznie tego samego rodzaju). Wychodząc z imprezy, miała już mniej niż 71 prezentów. Ile dokładnie ich jej zostało?

Zad. B. (1p. 6p.) Ania poszła kupić koraliki do sklepu, w którym nie przyjmują monet jednogroszowych. Chciała tam kupić koralik kosztujący 1 gr. W tym celu dała sprzedawcy monetę pięciogroszową i otrzymała dwie monety dwugroszowe reszty. Z cukierkami miała większy problem. Okazało się, że w sklepie przyjmują jedynie monety 403-groszowe oraz 713-groszowe i żadnych innych nominałów. Ile co najmniej kosztujących 3 grosze cukierków musi kupić Ania, by być w stanie rozliczyć się ze sprzedawcą tak, by nikt nie był nikomu winny choć grosika? (Zakładamy, ze chce kupić przynajmniej jeden cukierek).

Zad. C. (1p. 6p.) Niech G -niepusty zbiór, zaś $*$ - łączne działanie dwuargumentowe, t. że: $\forall a,b\in G\,\exists x,y\in G: a*x=b\wedge y*a=b$. Czy to wystarczy, by $(G,*)$ było grupą? Uzasadnij swoją odpowiedź.

Zad. D. (2p. 10p.) Wypisz (z dokładnością do izomorfizmu) wszystkie grupy sześcioelementowe.

Zad. E. (1p. 6p.) Niech F,H – skończone podgrupy grupy G , $FH=\{f*h: f\in F, h\in H\}$. Pokaż, że $|FH|=\frac{|F|\cdot|H|}{|F\cap H|}$