Kolokwium 2

Poniżej przedstawiono zadania jednej z wersji kolokwium. Zadania z drugiego zestawu można rozwiązać analogicznie.

Zadanie 1 (4 punkty)**.** *W zbiorze $\mathbb{Z}$ zdefiniowane są działania*

$$a \oplus b = a + b + 1, \qquad a \odot b = a + b + ab.$$

1. *Sprawdź czy każde z tych działań posiada element neutralny. Jeśli tak, czy każdy element z $\mathbb{Z}$ posiada element odwrotny względem tego działania (lub obu)? Jakiej jest on postaci?*
2. *Jakie dodatkowe warunki powinny być spełnione, żeby $(\mathbb{Z}, \oplus, \odot)$ było pierścieniem przemiennym z jedynką? (Nie musisz sprawdzać tych warunków.)*
3. *Czy jest szansa na to, żeby $(\mathbb{Z}, \oplus, \odot)$ było ciałem? Odpowiedź uzasadnij.*

Rozwiązanie:

1. $e \in \mathbb{Z}$ jest elementem neutralym $\oplus$ jeśli dla każdego $a \in \mathbb{Z}$ mamy:

   $$a \oplus e = e \oplus a = a.$$

   Zauważmy, że $a \oplus e = a + e + 1 = e + a + 1 = e \oplus a$, $a \in \mathbb{Z}$. Ponadto, dla $a \in \mathbb{Z}$:

   $$e \oplus a = a \quad \Leftrightarrow \quad e + a + 1 = a \quad \Leftrightarrow \quad e = -1.$$

   Zatem $e = -1$ jest elementem neutralym $\oplus$.
   Wyznaczymy element odwrotny do $a \in \mathbb{Z}$ względem $\oplus$:

   $$a \oplus b = e \quad \Leftrightarrow \quad a + b + 1 = -1 \quad \Leftrightarrow \quad b = -a - 2.$$

   Zatem dla każdego $a \in \mathbb{Z}$ element odwrotny istnieje i jest postaci $-a - 2$.

   Podobnie postępujemy dla $\odot$. Ustalmy $a \in \mathbb{Z}$. Wtedy $\tilde{e} \in \mathbb{Z}$ jest elementem neutralym $\odot$ jeśli $a \odot \tilde{e} = \tilde{e} \odot a = a$. Zauważmy, że $a \odot \tilde{e} = a + \tilde{e} + a\tilde{e} = \tilde{e} + a + \tilde{e}a = \tilde{e} \odot a$. Ponadto:

   $$\tilde{e} \odot a = a \quad \Leftrightarrow \quad \tilde{e} + a + \tilde{e}a = a \quad \Leftrightarrow \quad \tilde{e}(1 + a) = 0.$$

   Ponieważ a jest dowolną liczbą całkowitą, ostatnia równość zachodzi wtedy i tylko wtedy gdy $\tilde{e} = 0$. Zatem $\tilde{e} = 0$ jest elementem neutralym $\odot$. Wyznaczymy teraz element odwrotny do $a \in \mathbb{Z}$ względem $\odot$ (o ile istnieje):

   $$a \odot b = \tilde{e} \quad \Leftrightarrow \quad a + b + ab = 0 \quad \Leftrightarrow \quad b(1 + a) = -a \quad \Leftrightarrow \quad b = \frac{-a}{1 + a},$$

   przy czym ostatnia równość zachodzi tylko dla $a \neq -1$ (łatwo również sparwdzić, że element odwrotny do $a = -1$ nie istnieje). Dodatkowo, ponieważ szukamy elementu odwrotnego w $\mathbb{Z}$, $b = \frac{-a}{1+a}$ jest elementem odwrotnym do a wtedy i tylko wtedy gdy $b \in \mathbb{Z}$, to jest, $1 + a | a$. To jest możliwe tylko wtedy gdy $1 + a = \pm 1$ lub $a = 0$, tzn. gdy $a = 0$ lub $a = -2$. Pozostałe liczby calkowite nie mają elementu odwrotnego względem $\odot$.

2. $(\mathbb{Z}, \oplus, \odot)$ jest pierścieniem przemiennym z jedynką jeśli ($\oplus$ i $\odot$ są działaniami w $\mathbb{Z}$ oraz):
   - $\oplus$ jest łączne i przemienne (powyżej pokazaliśmy już istnienie elementu neutralnego i elementów odwrotnych)
   - $\odot$ jest łączne i przemienne (powyżej pokazaliśmy już istnienie elementu neutralnego)
   - $\odot$ jest rozdzielne względem $\oplus$.
3. $(\mathbb{Z}, \oplus, \odot)$ nie może być ciałem ponieważ, jak pokazaliśmy powyżej, tylko $a = 0$ i $a = -2$ mają elementy odwrotne względem $\odot$.

$\square$

Zadanie 2 (1 punkt)**.** *Jakiej postaci są elementy pierścienia $\mathbb{Z}[\sqrt{2}, \sqrt{5}]$?*

Rozwiązanie:
$\mathbb{Z}[\sqrt{2}, \sqrt{5}]$ jest pierścieniem generowanym przez $\sqrt{2}, \sqrt{5}$ nad $\mathbb{Z}$, a więc:

$$\mathbb{Z}[\sqrt{2}, \sqrt{5}] = \{a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10} : a, b, c, d \in \mathbb{Z}\}.$$

(Wykład: Wniosek 6.2.(2).)

$\square$

Zadanie 3 (2,5 punkta)**.**

1. *Wyznacz wszystkie ideały pierścienia $\mathbb{Z}_{10}$. W każdym przypadku rozstrzygnij czy są one pierwsze lub maksymalne.*
2. *Wyznacz elementy pierścienia ilorazowego $\mathbb{Z}_{10}/(5)$.*

Rozwiązanie:

1. Najlepiej wyznaczyć wszystkie ideały $\mathbb{Z}_{10}$ generując je różnymi elementami zbioru $\mathbb{Z}_{10}$. Oczywiście:
$$(0) = \{0\}, \qquad (1) = \mathbb{Z}_{10}.$$
Ponadto, jeśli a jest elementem odwracalnym, tzn. $a \in U(\mathbb{Z}_{10})$, to istnieje $b \in \mathbb{Z}_{10}$ takie, że $ab = 1$. A ponieważ $(a) = \{ax : x \in \mathbb{Z}_{10}\}$, to w szególności $1 \in (a)$, a więc $(a) = \mathbb{Z}_{10}$. Wystarczy więc rozważyć ideały generowane przez elementy nieodwracalne:
$$(2) = \{2x : x \in \mathbb{Z}_{10}\} = \{0, 2, 4, 6, 8\} = (4) = (6) = (8),$$
$$(5) = \{0, 5\}.$$
Musimy również rozważyć ideały generowane przez dwa elementy lub więcej, tzn. np.:
$$(a, b) = \{ax + by : x, y \in \mathbb{Z}_{10}\}$$
(Zauważmy, że w szczególności $(a) \subseteq (a, b)$.) Ale ponieważ ideały generowane przez $2, 4, 6$ lub 8 są równe, dodanie 0 jako generatora nic nie wnosi, a dodanie elementu odwracalnego jako generatora dałoby całe $\mathbb{Z}_{10}$, to zostaje nam tylko rozważenie
$$(2, 5) = \{2x + 5y : x, y \in \mathbb{Z}_{10}\} = \{0, 2, 4, 6, 8, 5, 2 + 5, \ldots\} = \mathbb{Z}_{10}.$$

Ostatnia równość wynika z tego, że $(2,5)$ zawiera $2+5=7$, który jest elementem odwracalnym, a więc automatycznie generuje cały pierścień $\mathbb{Z}_{10}$.
Zatem, jedyne ideały w $\mathbb{Z}_{10}$ to:

$$(0), \qquad (2), \qquad (5), \qquad \mathbb{Z}_{10}.$$

- Z definicji, $\mathbb{Z}_{10}$ nie jest ani ideałem pierwszym ani maksymalnym.
- (0) nie jest ideałem pierwszym, bo $2\cdot 5 \in (0)$, ale $2 \notin (0)$ oraz $5 \notin (0)$. (Równoważnie: (0) nie jest ideałem pierwszym, bo $\mathbb{Z}_{10}/(0) \cong \mathbb{Z}_{10}$, a $\mathbb{Z}_{10}$ nie jest pierścieniem całkowitym.) Zatem (0) nie jest też ideałem maksymalnym. (To wynika również z tego, że $(0) \subseteq (5) \subseteq \mathbb{Z}_{10}$ oraz $(0) \neq (5) \neq \mathbb{Z}_{10}$.)
- (5) jest ideałem maksymalnym ponieważ jedyny ideał w którym ideał (5) jest zawarty to (5) lub $\mathbb{Z}_{10}$. (Równoważnie: (5) jest ideałem maksymalnym ponieważ $\mathbb{Z}_{10}/(5) \cong \mathbb{Z}_5$, które jest ciałem.) W szczególności, (5) jest również ideałem pierwszym.
- (2) jest ideałem maksymalnym ponieważ jedyny ideał w którym ideał (2) jest zawarty to (2) lub $\mathbb{Z}_{10}$. (Równoważnie: (2) jest ideałem maksymalnym ponieważ $\mathbb{Z}_{10}/(2) \cong \mathbb{Z}_2$, które jest ciałem.) W szczególności, (2) jest również ideałem pierwszym.

2. $\mathbb{Z}_{10}/(5) = \{0+(5), 1+(5), 2+(5), 3+(5), 4+(5)\}$

(Wykład: Wniosek 7.1., Twierdzenie 7.14., Twierdzenie 7.15.)

$\square$

Zadanie 4 (4,5 punkta)**.**

1. *Wykaż, że* $\mathbb{Z}_{17}[X]/(X^2-2) \cong \mathbb{Z}_{17} \times \mathbb{Z}_{17}$.
   (Jeśli masz problem z $\mathbb{Z}_{17}$*, wykaż, że* $\mathbb{R}[X]/(X^2-2) \cong \mathbb{R} \times \mathbb{R}$
   ($0,5$ *pkt mniej).)*
2. *Wyznacz dzielniki zera w* $\mathbb{Z}_{17} \times \mathbb{Z}_{17}$.
3. *Czy ideał* (X^2-2) *pierścienia* $\mathbb{Z}_{17}[X]$ *jest pierwszy lub maksymalny?*

Rozwiązanie:

1. Wiemy, że $X^2-2 = (X-\sqrt{2})(X+\sqrt{2})$. Ponieważ w $\mathbb{Z}_{17}$ mamy $\sqrt{2} = \pm 6$ (skoro $(\pm 6)^2 = 36 = 2$), więc $X^2-2 = (X-6)(X+6)$. Dlatego zdefiniujmy

$$\phi\colon \mathbb{Z}_{17}[X] \to \mathbb{Z}_{17} \times \mathbb{Z}_{17}, \qquad \phi(f) = (f(6), f(-6)).$$

   - ϕ jest homomorfizmem pierścieni: dla $f, g \in \mathbb{Z}_{17}[X]$ mamy

$$\begin{aligned}\phi(f+g) &= ((f+g)(6), (f+g)(-6)) = (f(6)+g(6), f(-6)+g(-6)) \\ &= (f(6), f(-6)) + (g(6), g(-6)) = \phi(f) + \phi(g)\end{aligned}$$

     oraz

$$\begin{aligned}\phi(f\cdot g) &= ((f\cdot g)(6), (f\cdot g)(-6)) = (f(6)\cdot g(6), f(-6)\cdot g(-6)) \\ &= (f(6), f(-6)) \cdot (g(6), g(-6)) = \phi(f)\cdot\phi(g)\end{aligned}$$

- $\ker\phi = (X^2-2)$:

$$\begin{aligned}\ker\phi &= \{f\in\mathbb{Z}_{17}[X] : \phi(f)=(0,0)\} = \{f\in\mathbb{Z}_{17}[X] : (f(6),f(-6))=(0,0)\}\\ &= \{f\in\mathbb{Z}_{17}[X] : f(6)=0 \text{ i } f(-6)=0\} = \{f\in\mathbb{Z}_{17}[X] : (X-6)|f \text{ i } (X+6)|f\}\\ &= \{f\in\mathbb{Z}_{17}[X] : (X-6)(X+6)|f\} = \{(X-6)(X+6)g(X) : g\in\mathbb{Z}_{17}[X]\}\\ &= ((X-6)(X+6)) = (X^2-2)\end{aligned}$$

- $\operatorname{Im}\phi = \mathbb{Z}_{17}\times\mathbb{Z}_{17}$:
  Ustalmy $(a,b)\in\mathbb{Z}_{17}\times\mathbb{Z}_{17}$. $\phi(f)=(a,b)$ wtedy i tylko wtedy gdy $f(6)=a$ i $f(-6)=b$, tzn. szukamy wielomianu f, którego wykres przechodzi przez dwa punkty: $(6,a)$ i $(-6,b)$. W związku z tym, jeśli $a\neq b$, nie może to być wielomian stały, lecz przynajmniej pierwszego stopnia: np. $f(X)=a_0+a_1X$. Z warunków $f(6)=a$, $f(-6)=b$ dostajemy układ równań, który musimy rozwiązać:

$$\begin{cases} f(6)=a\\ f(-6)=b\end{cases} \Leftrightarrow \begin{cases} a_0+6a_1=a\\ a_0-6a_1=b\end{cases} \Leftrightarrow \begin{cases} a_0=-6a_1+a\\ -6a_1+a-6a_1=b\end{cases} \Leftrightarrow \begin{cases} a_0=-6a_1+a\\ -12a_1=b-a\end{cases}$$

$$\Leftrightarrow \begin{cases} a_1=(a-b)\cdot 12^{-1}\\ a_0=-6(a-b)\cdot 12^{-1}+a\end{cases}$$

  Nawet nie musimy wyliczać 12^{-1} w $\mathbb{Z}_{17}$, ważne że istnieje. W ten sposób otrzymaliśmy wielomian

$$f(X)=-6(a-b)\cdot 12^{-1}+a+(a-b)\cdot 12^{-1}X\,,$$

  który spełnia warunki $f(6)=a$, $f(-6)=b$.

Na mocy twierdzenia o izomorfizmie: $\mathbb{Z}_{17}[X]/(X^2-2)\cong\mathbb{Z}_{17}\times\mathbb{Z}_{17}$.

2. $(a,b)\in\mathbb{Z}_{17}\times\mathbb{Z}_{17}$ jest dzielnikiem zera wtedy i tylko wtedy gdy istnieje para $(x,y)\in\mathbb{Z}_{17}\times\mathbb{Z}_{17}$ różna od $(0,0)$ taka, że $(a,b)\cdot(x,y)=(0,0)$. Ponieważ

$$(a,b)\cdot(x,y)=(0,0) \quad\Leftrightarrow\quad (ax,by)=(0,0) \quad\Leftrightarrow\quad \begin{cases} ax=0\\ by=0\end{cases} \quad\Leftrightarrow\quad \begin{cases} a=0 \text{ lub } x=0\\ b=0 \text{ lub } y=0\end{cases},$$

więc $(a,b)\cdot(x,y)=(0,0)$ dla $(x,y)\neq(0,0)$ wtedy i tylko wtedy gdy $a=0$ lub $b=0$, tzn. dzielnikami zera w $\mathbb{Z}_{17}\times\mathbb{Z}_{17}$ są elementy zbioru

$$\{(a,0),(0,b) : a,b\in\mathbb{Z}_{17}\}.$$

3. Zadanie to można rozwiązać na kilka sposobów.
   <u>I sposób:</u>
   Jak zauważyliśmy powyżej: $\mathbb{Z}_{17}[X]/(X^2-2)$ jest izomorficzne z $Z_{17}\times\mathbb{Z}_{17}$, które ma nietrywialne dzielniki zera. To oznacza, że $Z_{17}\times\mathbb{Z}_{17}$ nie jest pierścieniem całkowitym, a więc (X^2-2) nie jest ideałem pierwszym. W związku z tym nie może być też ideałem maksymalnym.
   <u>II sposób:</u>
   Jak zauważyliśmy powyżej, X^2-2 jest wielmonianem rozkładalnym w $\mathbb{Z}_{17}$:

$$X^2-2=(X-6)(X+6)\,.$$

Zatem $X - 6 \notin (X^2 - 2)$ oraz $X + 6 \notin (X^2 - 2)$ podczas gdy $(X - 6)(X + 6) \in (X^2 - 2)$. W związku z tym $(X^2 - 2)$ nie jest ideałem pierwszym. Tu można od razu wywnioskować jak powyżej, że nie może być też ideałem maksymalnym. Można też zauważyć, że

$$(X^2 - 2) \subseteq (X - 6, X + 6) \subseteq \mathbb{Z}_{17}[X]$$

oraz wszystkie te zawierania są właściwe, tzn. powyższe ideały nie są równe. To oznacza, że ideał $(X^2 - 2)$ nie jest maksymalny.

(Wykład: Twierdzenie 7.13., Twierdzenie 7.14., Twierdzenie 7.15.)

$\square$

Zadanie 5 (3 punkty)**.** *Niech $(P, +, \cdot)$ będzie pierścieniem przemiennym z jedynką, a $I \triangleleft P$ jego ideałem. Wykaż, że zbiór*

$$I[X] = \{a_0 + a_1X + \ldots + a_nX^n : a_0, a_1, \ldots, a_n \in I, n \in \mathbb{N} \cup \{0\}\}$$

jest ideałem pierścienia $P[X]$.

Rozwiązanie:

1) Ustalmy $f, g \in I[X]$, tzn. niech $f(X) = a_0 + a_1X + \ldots + a_nX^n$, $g(X) = b_0 + b_1X + \ldots + b_mX^m$ dla pewnych $a_0, a_1, \ldots, a_n \in I, n \in \mathbb{N} \cup \{0\}$ oraz $b_0, b_1, \ldots, b_m \in I, m \in \mathbb{N} \cup \{0\}$. Bez straty ogólności możemy przyjąć, że $n \geqslant m$. Wtedy

$$f(X) - g(X) = a_0 - b_0 + (a_1 - b_1)X + \ldots + (a_m - b_m)X^m + a_{m+1}X^{m+1} \ldots + a_nX^n,$$

gdzie $a_i - b_i \in I$ dla $i = 0, \ldots, m$ ponieważ I jest ideałem oraz, oczywiście, $a_{m+1}, \ldots, a_n \in I$. Zatem, $f(X) - g(X) \in I[X]$.

2) Niech $f(X) = a_0 + a_1X + \ldots + a_nX^n \in I[X]$ oraz $g(X) = b_0 + b_1X + \ldots + b_mX^m \in P[X]$. Wtedy

$$f(X) \cdot g(X) = a_0b_0 + (a_0b_1 + a_1b_0)X + \ldots = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_ib_{k-i} \right) X^k,$$

gdzie $\sum_{i=0}^{k} a_ib_{k-i} \in I$ ponieważ I jest ideałem, a więc $f(X) \cdot g(X) \in I[X]$.

Zatem $I[X]$ jest ideałem pierścienia $P[X]$.

$\square$