Приклади розв'язування задач

1. Доведіть, що $a \cdot 0 = 0 \cdot a = 0$ для будь-якого елемента a кільця R.

Розв'язування:

Використовуючи дистрибутивність множення відносно додавання, маємо $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Додамо тепер до обох частин цієї рівності $-a \cdot 0$ і отримаємо $0 = a \cdot 0$.

2. Чи будуть кільцями зі звичайними операціями додавання та множення числові множини: а) Z; б) nZ; в) $Z\left[\sqrt{2}\,\right] = \left\{a + b\sqrt{2}: \ a, b \in Z\right\}$?

Розв'язування:

а) По-перше, відносно операції додавання Z є абелевою групою: всім зі школи добре відомо, що додавання цілих чисел асоціативне і комутативне, $0 + a = a + 0 = a$ для будь-якого цілого a і для кожного цілого числа a протилежне до нього $-a$ є єдиним розв'язком рівняння $a + x = 0$. Далі, відносно операції множення Z є комутативною півгрупою: множення цілих чисел, очевидно, асоціативне і комутативне. Крім того, множення цілих чисел дистрибутивне відносно додавання і число 1 є нейтральним елементом відносно множення. Отже, Z є комутативним кільцем з одиницею.

Аналогічно встановлюється, що множина Q всіх раціональних чисел відносно додавання і множення є комутативним кільцем з одиницею. Із властивостей додавання і множення дійсних чисел випливає, що комутативним кільцем з одиницею є множина всіх дійсних чисел R, звідки неважко вивести аналогічне твердження про множину C усіх комплексних чисел.

б) Можна просто перевірити аксіоми кільця: так само, як і у попередньому прикладі. Але досить зауважити, що сума і добуток двох чисел із nZ належать до nZ і для $a \in nZ$ очевидно, що $-a \in nZ$. Сказане означає, що nZ є замкненою відносно додавання, множення та взяття протилежного елемента. Враховуючи попередній приклад і те, що $nZ \subset Z$, всі аксіоми кільця для nZ виконуються автоматично. Зауважимо, що для $n > 1$ на відміну від кільця Z кільце nZ не істить одиниці.

в) Покажемо, що $Z\left[\sqrt{2}\,\right]$ – комутативне кільце. Для числа $a + b\sqrt{2} \in Z\left[\sqrt{2}\right]$ назвемо a його першою координатою, а b – другою. Асоціативність і комутативність додавання є фактично наслідками того, що додавання в $Z\left[\sqrt{2}\right]$ є покоординатним, а додавання координат (цілих чисел) асоціативне і комутативне. Розпишемо в деталях доведення асоціативності додавання. Візьмемо $a + b\sqrt{2},\ c + d\sqrt{2},\ e + f\sqrt{2} \in Z\left[\sqrt{2}\right]$. Маємо:

$$\left(\left(a+b\sqrt{2}\right) + \left(c+d\sqrt{2}\right)\right) + \left(e+f\sqrt{2}\right) = \left((a+c) + (b+d)\sqrt{2}\right) +$$
$$+ \left(e+f\sqrt{2}\right) = (a+c+e) + (b+d+f)\sqrt{2} = \left(a + b\sqrt{2}\right) +$$
$$+ \left((c+e) + (d+f)\sqrt{2}\right) = \left(a+b\sqrt{2}\right) + \left(\left(c+d\sqrt{2}\right) + \left(e+f\sqrt{2}\right)\right).$$

Нейтральним елементом при додаванні є, очевидно, число $0 = 0+0\sqrt{2}$, а (єдиним) протилежним елементом для $a+b\sqrt{2}$ є $-a-b\sqrt{2}$. Для встановлення асоціативності множення візьмемо $a + b\sqrt{2}, c + d\sqrt{2},\ e + f\sqrt{2} \in Z\left[\sqrt{2}\right]$. Маємо:

$$\left(\left(a+b\sqrt{2}\right)\cdot\left(c+d\sqrt{2}\right)\right)\cdot\left(e+f\sqrt{2}\right)=$$
$$=\left(\left(ac+2bd\right)+\left(ad+bc\right)\sqrt{2}\right)\cdot\left(e+f\sqrt{2}\right)=$$
$$=\left(\left(ac+2bd\right)e\right)+\left(2\left(ad+bc\right)\right)f+\left(\left(ac+2bd\right)f+\left(ad+bc\right)e\right)\sqrt{2}=$$
$$=\left(ace+2\left(bde+adf+bcf\right)\right)+\left(\left(acf+ade+bde\right)+2bdf\right)\sqrt{2}.$$

Розкриваючи дужки у виразі $\left(a+b\sqrt{2}\right)\cdot\left(\left(c+d\sqrt{2}\right)\cdot\left(e+f\sqrt{2}\right)\right)$, легко переконаємось, що праві частини останніх двох записів збігаються, а отже, і ліві частини, що доводить асоціативність множення. Операція множення буде до того ж комутативною. Це випливає з того, що переставивши місцями у виразі $\left(ac+2bd\right)+\left(ad+bc\right)\sqrt{2}$ відповідно a та c і b та d, ми одержимо той самий вираз. Останній штрих – доведення дистрибутивності – лишаємо читачеві. Отже, $Z\left[\sqrt{2}\right]=\left\{a+b\sqrt{2}:\ a,\ b\in Z\right\}$ – кільце.

3. Визначте, які з наступних множин є полями відносно дій додавання та множення дійсних чисел: а) $A=\left\{a+b\sqrt{2}:\ a,b\in Q\right\}$;
б) $B=\left\{a+b\sqrt[3]{2}:\ a,b\in Q\right\}$; в) $C=\left\{a+b\sqrt[3]{2}+c\sqrt[3]{4}:a,b,c\in Q\right\}$.

Розв'язування:

Оскільки A, B, C є підмножинами поля R, то асоціативність та комутативність додавання і множення, а також дистрибутивний закон автоматично виконуються для елементів множин A, B, C. Кожна із заданих множин містить 0 та 1 – нейтральні елементи для додавання і множення в R, отже 0 та 1 виконують ролі нейтральних елементів для додавання та множення для кожної із заданих множин. Крім цього, очевидно, що всі три множини замкнені відносно додавання та взяття протилежного елемента. Нам лишається дослідити A, B, C а замкненість відносно множення та на оборотність всіх ненульових елементів.

а) A замкнена відносно множення, оскільки для $\left(a+b\sqrt{2}\right)$ і $\left(c+d\sqrt{2}\right)$ з A маємо: $\left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right)=\left(ac+2bd\right)+\left(ad+bc\right)\sqrt{2}\in A$. Далі візьмемо ненульвий елемент $\left(a+b\sqrt{2}\right)\in A$. Для нього:

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}.$$

Відзначимо, що $a^2-2b^2\neq 0$ для $a,b\in Q$, оскільки $\sqrt{2}\notin Q$. Отже, $(a+b\sqrt{2})^{-1}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\in A$. Таким чином, кожний ненульовий елемент із A є оборотним, а отже, A є полем.

б) Намагаючись довести замкненість відносно множення аналогічно попередньому пункту візьмемо два довільних елементи $\left(a+b\sqrt[3]{2}\right)$ і $\left(c+d\sqrt[3]{2}\right)$ із A, перемножуючи які отримаємо: $\left(a+b\sqrt[3]{2}\right)\left(c+d\sqrt[3]{2}\right)=ac+\left(bc+ad\right)\sqrt[3]{2}+bd\sqrt[3]{4}$, а $\sqrt[3]{4}\notin B$. Отримана суперечність означає, що множина B не замкнена відносно множення, тому не є полем.

в) Так само, як у пункті а), легко перевірити, що множина C є замкненою відносно множення. Лишається перевірити, чи кожен ненульовий елемент $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4} \in C$ є оборотним. Дамо можливість читачеві самому це зробити за аналогією до попереднього пункту.

Отже, ненульовий елемент α є оборотним в C, звідки випливає, що C є полем.

4. Перевірте, чи утворює поле відносно звичайних матричних операцій множина матриць вигляду $M_p^n = \left\{ \begin{pmatrix} x & y \\ ny & x \end{pmatrix} :\ x, y \in Z_p \right\}$, де n – фіксований елемент із Z_p, для $p = 2, 3, 5, 7$.

Розв'язування:

Замкненість відносно додавання і взяття протилежної матриці випливають безпосередньо із означення M_p^n. Нехай $A = \begin{pmatrix} x & y \\ ny & x \end{pmatrix}$, $B = \begin{pmatrix} u & v \\ nv & u \end{pmatrix} \in M_p^n$. Тоді $A \cdot B = B \cdot A = \begin{pmatrix} xu + nyv & xv + yu \\ nvx + nuy & nvy + xu \end{pmatrix} \in M_p^n$. Отже, M_p^n замкнена відносно множення матриць і будь-які дві матриці із M_p^n переставновочні.

Припустимо, що $A = \begin{pmatrix} x & y \\ ny & x \end{pmatrix} \in M_p^n$ – оборотна в $M_n(Z_p)$. Тоді $d = det\, A = x^2 - ny^2 \neq 0$ і $A^{-1} = \begin{pmatrix} xd^{-1} & -yd^{-1} \\ -nyd^{-1} & xd^{-1} \end{pmatrix} \in M_p^n$.

Лишилось дослідити, при яких цілих n кожна ненульова матриця із M_p^n є оборотною, тобто при яких цілих n нерівність $x^2 - ny^2 \neq 0$ виконується для будь-яких одночасно не рівних нулю $x, y \in Z_p$.

Нехай $y = 0$. Тоді $d = x^2 \neq 0$, оскільки $x \neq 0$ і в полі Z_p відсутні дільники нуля. Нехай тепер $y \neq 0$. Виконання нерівності $x^2 - ny^2 \neq 0$ для всіх $x \in Z_p, y \in Z_p \backslash \{0\}$ еквівалентне виконанню нерівності $\left(\frac{x}{y}\right)^2 - n \neq 0$ для всіх $x \in Z_p, y \in Z_p \backslash \{0\}$, що в свою чергу рівносильне виконанню нерівності $z^2 - n \neq 0$ для всіх $z \in Z_p$ (в силу того, що $\left\{ \frac{x}{y} : x \in Z_p, y \in Z_p \backslash \{0\} \right\} = Z_p$).

Отже, для знаходження потрібних значень n потрібно виписати квадрати всіх елементів із Z_p для кожного конкретного p і взяті ті n, які серед виписаних квадратів не зустрілися.

1) $p=2$: $0^2=0$, $1^2=1$. Всі елементи із Z_2 є квадратами певних елементів із Z_2. Отже, при жодному $n\in Z_2$ M_p^2 не є полем.

2) $p=3$: $0^2=0$, $2^2=1$. В списку квадратів не зустрівся лише елемент 2, тому M_p^3 є полем тоді й лише тоді, коли $n=2$.

3) $p=5$: $0^2=0$, $1^2=1$, $2^2=4$, $3^2=4$, $4^2=1$. В списку квадратів не зустрілися елементи 2, 3, тому M_p^5 є полем тоді й лише тоді, коли $n=2,3$.

4) $p=7$: $0^2=0$, $1^2=1$, $2^2=4$, $3^2=2$, $4^2=2$, $5^2=4$, $6^2=1$. В списку квадратів не зустрілися елементи 3, 5, 6, тому M_p^7 є полем тоді й лише тоді, коли $n=3,5,6$.

Тест для самоконтролю

1. У множині $A=\{a+b\sqrt{2}:\ a,b\in Z\}$ відносно додавання нейтральним елементом є:

А. $0+0\sqrt{2}$ **Б.** $1+1\sqrt{2}$ **В.** $0+1\sqrt{2}$ **Г.** $1+0\sqrt{2}$

2. У множині $B=\{a+b\sqrt{3}:\ a,b\in Q\}$ відносно множення нейтральним елементом є:

А. $0+0\sqrt{3}$ **Б.** $1+1\sqrt{3}$ **В.** $0+1\sqrt{3}$ **Г.** $1+0\sqrt{3}$

3. У множині2 $A=\{a+b\sqrt{2}:\ a,b\in Z\}$ відносно додавання протилежним до елементу $c+d\sqrt{2}$ буде:

А. $c-d\sqrt{2}$ **Б.** $-c-d\sqrt{2}$ **В.** немає протилежного **Г.** $\dfrac{c-d\sqrt{2}}{c^2-2d^2}$

4. У множині $B=\{a+b\sqrt{3}:\ a,b\in Q\}$ відносно множення протилежним до елементу $c+d\sqrt{2}$ буде:

А. $-c-d\sqrt{3}$ **Б.** немає протилежного **В.** $\dfrac{c-d\sqrt{3}}{c^2-3d^2}$ **Г.** $c-d\sqrt{3}$

5. Адитивна група G називається абелевою, якщо $\forall\ a,b,c\in G$:

А. $(a+b)+c=a+(b+c)$ **Б.** $a+b=b+a$ **В.** $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ **Г.** $a\cdot b=b\cdot a$

6. Мультиплікативна група G називається абелевою, якщо $\forall\ a,b,c\in G$:

А. $(a+b)+c=a+(b+c)$ **Б.** $a+b=b+a$ **В.** $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ **Г.** $a\cdot b=b\cdot a$

7. Операція додавання у множині $M=\left\{\begin{pmatrix} a & b \\ 1 & -a \end{pmatrix},\ a,b\in R\right\}$

А. замкнена **Б.** незамкнена

8. Операція множення у множині $M=\left\{\begin{pmatrix} a & b \\ 1 & -a \end{pmatrix},\ a,b\in R\right\}$

А. замкнена **Б.** незамкнена

9. Яке з твердження правильне:

А. Якщо G – адитивна група, то G – кільце.

Б. Якщо G – кільце з одиницею, то G – поле.

В. Якщо G – кільце, то G – адитивна група.

Г. Якщо G – кільце, то в G кожний ненульовий елемент обернений?

10. Яке з твердження неправильне:

А. Кільце з 1, в якому кожний елемент оборотний, називається полем.

Б. Група називається мультиплікативною, якщо в ній задано операцію множення.

В. Кільце з 1, в якому кожний ненульовий елемент оборотний, називається полем.

Г. Група називається адитивною, якщо в ній задано операцію додавання?

Відповіді: 1. А. 2. Г. 3. Б. 4. В. 5. Б. 6. Г. 7. Б. 8. Б. 9. В. 10. А.