

Matematyka dyskretna, zestaw 9.

9.1. Sprawdź czy zbiór \mathbb{R} wraz z działaniem

a) $a \circ b = a + b + 5$,

b) $a \circ b = ab - a - b + 2$,

tworzy grupę.

9.2. Wyznacz rząd grupy \mathbb{Z}_7^* i rzędy jej elementów oraz podaj generatory, o ile istnieją. Analogicznie dla grupy \mathbb{Z}_{15}^* .

9.3. Niech X będzie zbiorem niepustym i niech $\mathcal{P}(X)$ będzie rodziną wszystkich podzbiorów zbioru X . Pokaż, że struktura algebraiczna $(\mathcal{P}(X), \div, \cap)$, gdzie \div oznacza różnicę symetryczną, jest pierścieniem przemiennym z jedyneką.

9.4. Pokaż, że zbiór $\mathbb{Q}(\sqrt{5}) := a + b\sqrt{5} : a, b \in \mathbb{Q}$ wraz ze zwykłymi działaniami dodawania i mnożenia liczb tworzy ciało.

9.5. Weźmy dwa elementy ciała $\text{GF}(2^3)$: $A(x) = x^2 + x$ i $B(x) = x + 1$. Oblicz ich sumę oraz iloczyn, tj. $A(x) + B(x)$, $A(x) \cdot B(x)$, wybierając wielomian pierwotny $P(x) = x^3 + x + 1$.

9.6. Rozważmy ciało $\text{GF}(2^8)$ z wielomianem pierwotnym $P(x) = x^8 + x^4 + x^3 + x + 1$. Jest ono wykorzystywane w szyfrowaniu AES, a jego elementy można reprezentować przez ciągi 8-bitowe lub jedno/dwucyfrowe liczby szesnastkowe. Oblicz odwrotność elementu $5D$ i sprawdź swój wynik w tabeli z wykładu. Wskazówka: wymaga to zastosowania rozszerzonego algorytmu Euklidesa w stosunku do wielomianów.

9.7. Zbiór \mathbb{Z}_4 wraz z dodawaniem i mnożeniem modulo 4 tworzy pierścień, różny od $\text{GF}(4) = \text{GF}(2^2)$. Możemy również rozważyć pierścień oznaczany przez $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, którego elementy to pary liczb $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$, a ich dodawanie i mnożenie definiujemy jako:

$$(a, b) + (a', b') := (a + a' \bmod 2, b + b' \bmod 2),$$

$$(a, b) \cdot (a', b') := (a \cdot a' \bmod 2, b \cdot b' \bmod 2).$$

Tabelka mnożenia w $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ ma zatem postać:

	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$(0, 0)$	$(0, 0)$	$(0, 0)$	$(0, 0)$	$(0, 0)$
$(0, 1)$	$(0, 0)$	$(0, 1)$	$(0, 0)$	$(0, 1)$
$(1, 0)$	$(0, 0)$	$(0, 0)$	$(1, 0)$	$(1, 0)$
$(1, 1)$	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$

Zapisz tabelki dla dodawania i mnożenia w $\text{GF}(4)$ oraz \mathbb{Z}_4 , a także dla dodawania w $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Chociaż te trzy pierścienie wyglądają różnie, mogą być w pewnym sensie tożsame. Mówi o tym pojęcie izomorfizmu, czyli bijekcji, która zachowuje strukturę danego obiektu algebraicznego.

Nadobowiązkowo: sprawdź, czy dla którejś pary spośród omawianych trzech pierścieni istnieje bijekcja $h : R_1 \rightarrow R_2$ spełniająca warunki (tzn. izomorfizm):

$$\begin{aligned}\forall_{a,b \in R_1} h(a +_1 b) &= h(a) +_2 h(b), \\ \forall_{a,b \in R_1} h(a \cdot_1 b) &= h(a) \cdot_2 h(b),\end{aligned}$$

gdzie $(R_1, +_1, \cdot_1)$, $(R_2, +_2, \cdot_2)$ to dane dwa pierścienie. W tym celu można zauważyć, że izomorfizm odwzorowuje element neutralny dodawania w $(R_1, +_1, \cdot_1)$ na element neutralny dodawania w $(R_2, +_2, \cdot_2)$.

- 9.8. Wiadomość o treści KARAT można przesłać przy użyciu czterech elementarnych przekazów $K, A, R, T \in \mathbb{Z}_2 \times \mathbb{Z}_2$ (ściśle rzecz biorąc, są to wektory z przestrzeni wektorowej $\text{GF}(2) \times \text{GF}(2)$ nad ciałem $\text{GF}(2)$):

$$K = (0, 0), \quad A = (1, 0), \quad R = (0, 1), \quad T = (1, 1).$$

Jednakże, zakłócenia są w stanie spowodować, że niektóre 0 zmieniają się w 1 lub odwrotnie, w rezultacie czego odbiorca otrzyma np. wiadomość o treści KATAR. Aby zmniejszyć prawdopodobieństwo takiej sytuacji, należy zastosować kod korekcji błędów, oparty na dłuższych przekazach elementarnych. Rozważmy zatem $K, A, R, T \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ i niech na przykład:

$$K = (0, 0, 1, 1, 0), \quad A = (1, 0, 0, 1, 1).$$

Jak należy podobnie zakodować R i T , aby wszystkie przekazy elementarne pozostały odróżnialne nawet wtedy, gdy w każdym z nich na jednej z pozycji pojawi się błędna wartość (np. K zmieni się w $(1, 0, 1, 1, 0)$ i podobnie dla innych)? Przedstaw K , A , R i T oraz wszystkie możliwe ich zakłócone wersje w postaci tabelki.

Michał Bujak
Piotr Czarnik
Jakub Czartowski
Grzegorz Czelusta
Andrzej Kapanowski
Piotr Korcyl
Jakub Mielczarek
Andrzej Rostworowski