Algebra Abstrakcyjna i Kodowanie - przykłady zadań

prof. dr hab. Jacek Cichoń

opracował: Mikołaj Pietrek

1 Struktury algebraiczne

Zadanie 1. Ile generatorów ma grupa C_{4000}?

Rozwiązanie. (J. Nigiel)
x jest generatorem.
istnieje A takie ze $A * x = 1 \bmod 4000$ (generowanie wszystkich elementów) oraz $4000 = 0 \bmod 4000$
$4000 * B = 0 \bmod 4000$
$Ax + 4000 * B = 1 \bmod 4000$
z Rozszerzonego Algorytmu Euklidesa mamy $\mathrm{NWD}(x, 4000) = 1$
odpowiedź: $\phi(4000) = 1600$

Rozwiązanie. (A.Lasecki, D.Nowak)
wszystkie generatory są względnie pierwsze
$\phi(4000) = 1600$

Rozwiązanie. (K.Kleczkowski)
Generator musi być względnie pierwszy z rzędem grupy, ponieważ w przeciwnym wypadku wyznaczałby podgrupę właściwą C_{4000}. Stąd liczbą generatorów nazywamy liczbę $\varphi(4000) = 1600$.

Zadanie 2. Wyznacz wszystkie podgrupy grupy Z_{11}^*

Rozwiązanie. (A.Lasecki, D.Nowak)
Grupa $\mathbb{Z}_{11}^*$ ma 10 elementów. Wiemy, że ranga każdego elementu musi dzielić 10, więc możliwe rangi to $10, 5, 2, 1$. Wiedząc to, wyznaczamy rangi poszczególnych elementów:

	$rank(2) = 10$	$rank(4) = 5$	$rank(6) = 10$	$rank(8) = 10$	$rank(10) = 2$
$rank(1) = 1$	$rank(3) = 5$	$rank(5) = 5$	$rank(7) = 10$	$rank(9) = 5$	

Zauważmy, że elementy 3,4,5 i 9 generują tą samą podgrupę: $\{1, 3, 4, 5, 9\}$, oraz element 10 generuje $\{1, 10\}$. Wobec tego podgrupy $\mathbb{Z}_{11}^*$ to: $\mathbb{Z}_{11}^*$, $\{1, 3, 4, 5, 9\}$, $\{1, 10\}$, $\{1\}$

Zadanie 3. Ile jest elementów rzędu 100 w grupie C_{4000}?

Rozwiązanie. Weźmy najmniejszy z takich elementów: 40 ($40 * 100 = 4000$) Zauważmy, że każdy element rangi 100 będzie należał do $\langle 40 \rangle$ ponieważ jeśli $a \in C_{4000}$ jest taki, że $rank(a) = 100$, to wtedy:

$$a * 100 \equiv 0 \bmod 4000 \rightarrow a' * 40 * 100 \equiv 0 \bmod 4000$$

Zauważmy również, że:

$$\langle 40 \rangle \cong C_{100}$$

Więc elementy rangi 100 w C_{4000} są generatorami C_{100}, czyli są to liczby < 100 także, że $\mathrm{NWD}\,(a, 100) = 1$, a takich liczb jest:

$$\varphi\,(100) = 40$$

Zadanie 4. Wyznacz podgrupę G grupy $\mathbb{Z}^2 = (\mathbb{Z}, +) \times (\mathbb{Z}, +)$ generowaną przez zbiór $\{(4,0), (10,0), (-18,0)\}$ oraz wyznacz rzędy elementów w grupie ilorazowej Z^2/G

Rozwiązanie. (A.Lasecki, D.Nowak)
dodając (i odejmując) liczby parzyste nie otrzymamy nieparzystej.
Da się za to otrzymać 2 oraz -2 z:

$$2 = 10 - 4 - 4$$

$$-2 = 2 - 4$$

Zatem:

$$G = \{(a, 0) : a \in 2\mathbb{Z}\} = 2\mathbb{Z} \times \{0\}$$

Warstwy G w są postaci $2\mathbb{Z} \times \{n\}$ i $(2\mathbb{Z} + 1) \times \{m\}$ gdzie $m, n \in \mathbb{Z}$ oraz dla $h \in \mathbb{Z}^2/G$:

$$rank(h) = \begin{cases} 1 : 2\mathbb{Z} \times \{0\} \\ 2 : (2\mathbb{Z} + 1) \times \{0\} \\ \infty : oth \end{cases}$$

Uwaga:

$$Z^2/G \cong C_2 \times \mathbb{Z}$$

Rozwiązanie. (K. Kleczkowski)
Wyznaczmy podgrupę generowaną przez dany zbiór:

$$G = \{(4,0)k + (10,0)l + (-18,0)m : k, l, m \in \mathbb{Z}\} = \{(2(2k + 5l - 9m), 0) : k, l, m \in \mathbb{Z}\} = \{(2k, 0) : k \in \mathbb{Z}\} = 2\mathbb{Z} \times \{0\}$$

Zauważmy, że $2\mathbb{Z}$ i $\{0\}$ są ideałami w $\mathbb{Z}$. Zatem

$$\mathbb{Z}\times\mathbb{Z}/_{2\mathbb{Z}\times\{0\}} \cong \left(\mathbb{Z}/_{2\mathbb{Z}}\right) \times \left(\mathbb{Z}/_{\{0\}}\right) \cong C_2 \times \mathbb{Z}$$

Weźmy podgrupę $C_2 \times \{0\}$. Mamy wtedy $\text{ord}(1,0) = 2$ i $\text{ord}(0,0) = 1$. Dla elementów ze zbioru $C_2 \times (\mathbb{Z} \setminus \{0\})$ mamy rzędy nieskończone.

Zadanie 5. Czy grupy Z_8^* oraz Z_{10}^* są izomorficzne?

Rozwiązanie. (A.Lasecki, D.Nowak)
$Z_8^* = \{1, 3, 5, 7\}$
$Z_{10}^* = \{1, 3, 7, 9\}$
$Z_8^* \quad rank(3) = 2 \quad rank(5) = 2 \quad rank(7) = 2$
$Z_8^* \quad rank(3) = 4 \quad rank(7) = 4 \quad rank(9) = 2$
Rangi elementów są różne.

Zadanie 6. Ile podgrup ma grupa S_3?

Rozwiązanie. (A.Lasecki, D.Nowak)
$|H| = 1 \rightarrow$ jedna
$|H| = 2 \rightarrow$ trzy
$|H| = 3 \rightarrow$ jedna
$|H| = 6 \rightarrow$ jedna
6 podgrup S_3

Zadanie 7. Rozważamy grupę $T = (\{z \in C : |z| = 1\}, \cdot)$. Niech $f(x) = x^2$. Pokaż, że f jest endomorfizmem T. Wyznacz jądro f oraz grupę ilorazową $T/ker(f)$.

Rozwiązanie. (A.Lasecki, D.Nowak)
$T = (\{z \in C : |z| = 1\}, \cdot)$
$A(x) = x^2$
Niech $x \in C$ oraz $|x| = 1$, wtedy $f(x) = x^2$
$|x^2| = |x| \cdot |x|$
ponieważ $|x| = 1$, to $|x^2| = 1$
zatem x^2 leży na kółku jednostkowym
Interpretacja geometryczna: dla dowolnego elementu z kółka, jedynie przesuwamy na kółku wartości

Rozwiązanie. (K. Kleczkowski)
Funkcja $f : T \to T$ jest endomorfizmem. Weźmy $x \in T$. Mamy $1 = |x| = |x| \cdot |x| = |x^2| \in T$. Wyznaczmy $\ker(f)$. Mamy $x^2 = 1$, stąd $x = \pm 1$, czyli $\ker(f) = \{-1, 1\}$. Stąd ${}^{T}/_{\ker(f)} = \{\{-t, t\} : t \in T\}$.

2 Elementy Teorii Liczb

Zadanie 1. Jakie wartości przyjmuje funkcja $f(n) = (n-1)! \mod n$?

Rozwiązanie. (A.Lasecki, D.Nowak)
$f(p) = (p-1)! \mod p = 1$
$(n \notin prime)$
Jeżeli $p \notin prime$ to albo:
1) istnieje n_1, n_2 t.że $n_1 > 1$, $n_2 > 1$, $n_1 \neq n_2$. Wtedy $n_1 \in (n-1)!$ oraz $n_2 \in (n-1)!$ oraz $n = n1 * n2$
(jest podzielne więc mod $n = 0$)
2) (COŚ) $n = p^2 = p > 2$, wtedy: $p \in (n-1)!$ oraz $2p \in (n-1)!$, zatem $(n-1)! \mod n = 0$
WYJĄTEK: $f(4) = 2$ LOL

Zadanie 2. Pokaż, ze dla dowolnej liczby naturalnej n mamy $n|\phi(n^2)$.

Rozwiązanie. (K. Kleczkowski)
Niech $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.

$$\varphi(n^2) = \prod_{i=1}^{k}(p_i^{2\alpha_i} - p_i^{2\alpha_i - 1}) = \prod_{i=1}^{k} p_i^{\alpha_i} \cdot \prod_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \cdot \varphi(n)$$

□

Zadanie 3. Wyznacz najmniejszą liczbę naturalną n taką, że $n \equiv 1 \mod 3$, $n \equiv 2 \mod 5$ i $n \equiv 3 \mod 8$.

Rozwiązanie. (A. Lasecki)

$$\begin{cases} n \equiv 1 \mod 3 \\ n \equiv 2 \mod 5 \\ n \equiv 3 \mod 8 \end{cases}$$

Użyjemy medoty sita. Zacznijmy od wyznaczenia najmniejszej liczby spełniającej pierwszą kongruencję. Jest to liczba 1. Mamy wtedy, że rozwiązanie pierwszych dwóch kongruencji będzie należało do ciągu:

$$1,\ 1+3,\ 1+3\cdot 2,\ \ldots,\ 1+3\cdot k,\ \ldots$$

Czyli:

$$1,\ 4,\ 7,\ \ldots$$

Liczba 7 spełnia drugą kongruencję więc teraz szukamy rozwiązania spełniającego wszystkie trzy. Znajduje się ono w ciągu:

$$7,\ 7+3\cdot 5,\ 7+3\cdot 5\cdot 2,\ \ldots,\ 7+3\cdot 5\cdot k,\ \ldots$$

Czyli:

$$7,\ 22,\ 37,\ 52,\ 67,\ \ldots$$

Rozwiązaniem układu kongruencji jest liczba 67

Zadanie 4. Rozwiąż układ równań: $2x \equiv 1 \mod 5$, $3x \equiv 9 \mod 6$, $4x \equiv 1 \mod 7$.

Rozwiązanie. (A. Lasecki)

$$\begin{cases} 2x \equiv 1 \mod 5 \\ 3x \equiv 3 \mod 6 \\ 4x \equiv 1 \mod 7 \end{cases}$$

Użyjemy metody sita. Zacznijmy od wyznaczenia najmniejszej liczby spełniającej pierwszą kongruencję. Jest to liczba 6, czyli $x = 3$. Mamy wtedy, że rozwiązanie pierwszych dwóch kongruencji będzie należało do ciągu:

$$3\cdot 3,\ 3\cdot(3+5),\ \ldots$$

Liczba 9 spełnia drugą kongruencję ($x = 3$) więc teraz szukamy rozwiązania spełniającego wszystkie trzy. Znajduje się ono w ciągu:

$$4\cdot 3,\ 4\cdot(3+5\cdot 2),\ 4\cdot(3+5\cdot 2\cdot 2),\ 4\cdot(3+5\cdot 2\cdot 3),\ \ldots,\ 4\cdot(3+5\cdot 2\cdot k),\ \ldots$$

Uwaga: Zauważmy, że nie musimy przy każdym skoku dodawać $5 \cdot 6$, wystarczy $5 \cdot 2$, ponieważ gdy podstawimy wybraną liczbę pod $3x$ to nasze $5 \cdot 2$ zamieni się w $3 \cdot 5 \cdot 2 = 5 \cdot 6$

Uwaga w uwadze: Pamiętajmy, że aby znaleźć najmniejsze rozwiązanie spełniające kongruencję (wymagane do wyprowadzenia wzoru opisującego wszystkie wyniki), należy używać najmniejszych możliwych skoków, inaczej możemy przypadkiem pominąć jakąś liczbę.

Rozwiązaniem układu kongruencji jest liczba $4 \cdot (3 + 5 \cdot 2 \cdot 2) = 92$, czyli $x_{min} = 23$ i ogólnie $x = 23 + 5 \cdot 2 \cdot 7m$, gdzie $m \in \mathbb{N}$

Zadanie 5. Pokaż, że $(\forall a \in \mathbb{N})(\exists b, c \in \mathbb{N})(a^3 = b^2 - c^2)$

Rozwiązanie. (A. Lasecki)

Wiemy, że suma oraz różnica kwadratu każdej liczby naturalnej i jej samej jest zawsze liczbą parzystą. Stąd mamy:

$$b = \frac{a^2 + a}{2}, \quad c = \frac{a^2 - a}{2}$$

$$b,\ c \in \mathbb{N}$$

Oraz zauważmy, że:

$$b + c = a^2, \quad b - c = a$$

Podstawiając, otrzymujemy:

$$a^3 = (b + c)(b - c) = b^2 - c^2$$

□

Zadanie 6. Wyznacz zbiór $\{(a^2 - b^2) \mod 4 : a, b \in \mathbb{N}\}$

Rozwiązanie. (K. Kleczkowski)
Zbadajmy najpierw resztę $(2k+1)^2 \mod 4$.

$$(2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2+k) + 1$$

Stąd $(2k+1)^2 \equiv 1 \pmod 4$. Oczywiste jest, że $(2k)^2 \equiv 0 \pmod 4$. Stąd z działania na kongruencjach mamy, że $A = \{(a^2 - b^2) \mod 4 : a, b \in \mathbb{N}\} = \{0, 1, 3\}$.

Zadanie 7. Pokaż, ze jeśli liczby naturalne a i b są sumami dwóch kwadratów to również liczba $a \cdot b$ jest sumą dwóch kwadratów.

Rozwiązanie. (K. Kleczkowski)
Weźmy $x, y \in \mathbb{Z}[i]$. Oznaczmy $x = a + bi$ oraz $y = c + di$. Z własności modułu otrzymujemy:

$$|x|^2 \cdot |y|^2 = (a^2+b^2)(c^2+d^2) = |x \cdot y|^2 = (ac - bd)^2 + (ad + bc)^2$$

□

Zadanie 8. Niech $p > 2$ będzie liczba pierwszą. Niech a, b będą dwoma rożnymi generatorami grupy multiplikatywnej $\mathbb{Z}_p^*$. Pokaż, ze ab nie jest generatorem grupy $\mathbb{Z}_p^*$.

Rozwiązanie. (K. Kleczkowski, P. Witowski)
Wiemy, że wszystkie grupy cykliczne o tym samym rzędzie są izomorficzne, stąd $\mathbb{Z}_p^* \cong C_{p-1}$.

Weźmy więc generatory $a', b' \in C_{p-1}$ takie, że $a' \neq b'$. Zauważmy, że rząd grupy jest parzysty, ponieważ liczba pierwsza $p > 2$ jest nieparzysta, a stąd $p-1$ jest parzyste. Ponieważ generatory C_{p-1} są względnie pierwsze z $p-1$, stąd generatory są nieparzyste w tej grupie. Suma $a' + b'$ jest parzysta, ponieważ suma dwóch liczb nieparzystych jest parzysta, a stąd $a' + b'$ nie może być generatorem w C_{p-1}. Ponieważ $\mathbb{Z}_p^* \cong C_{p-1}$, to ab, choćby się zesrało, nie może być generatorem $\mathbb{Z}_p^*$. □

3 Pierścienie i ciała

Zadanie 1. Niech $n \geqslant 1$ będzie liczbą naturalną. Wyznacz $\text{NWD}(x^{6n} + x + 1, x^2 + 1)$ w pierścieniu $\mathbb{Z}_3[x]$.

Rozwiązanie. (K. Kleczkowski)
Zauważmy, że wielomian $x^2 + 1$ jest pierwszy w $\mathbb{Z}_3[x]$. Wobec tego ${}^{\mathbb{Z}_3[x]}/_{(x^2+1)} \cong \mathbb{Z}_3[i]$, gdzie $i^2 + 1 = 0$. Niech $w(x) = x^{6n} + x + 1$. Obliczmy $w(i)$.

$$w(i) = i^{6n} + i + 1 = (i^2)^{3n} + i + 1 = (-1)^{3n} + i + 1 = (-1)^n + 1 + i$$

Można zauważyć, że $w(i) \neq 0$. Stąd z twierdzenia Bézouta stwierdzamy, iż wielomian w nie jest podzielny przez $x^2 + 1$ zatem jest względnie pierwszy z $x^2 + 1$. Stąd $\gcd(x^{6n} + x + 1, x^2 + 1) = 1$.

Zadanie 2. Korzystając z tego, że wielomian $x^3 + x + 1$ jest nierozkładalny w ciele $\mathbb{Z}_5$, rozszerzamy ciało $\mathbb{Z}_5$ o taki element j, że $j^3 = 4j + 4$. Ile elementów ma to ciało? Znajdź element odwrotny i przeciwny do elementu $1 + j + j^2$ w tym ciele.

Rozwiązanie. (K. Kleczkowski)
Zauważmy, że ${}^{\mathbb{Z}_5[x]}/_{(x^3+x+1)} \cong \mathbb{Z}_5[j]$. Przyjrzyjmy się warstwie $r + (x^3+x+1) = \{(x^3+x+1)q + r : q \in \mathbb{Z}_5[x]\}$. Możemy powiedzieć, że $\deg(r) \leqslant 2$, zatem wielomian r jest postaci $r_0 + r_1 x + r_2 x^2$. Stąd $\left|{}^{\mathbb{Z}_5[x]}/_{(x^3+x+1)}\right| = |\mathbb{Z}_5[j]| = 5^3$.

Znajdźmy element odwrotny do $1+j+j^2$. Weźmy $x = a+bj+cj^2 \in \mathbb{Z}_5[j]$ taki, że $(1+j+j^2)\cdot x = 1$. Mamy więc równanie:

$$\begin{aligned}(1+j+j^2)\cdot x &= (1+j+j^2)(a+bj+cj^2)\\ &= a+aj+aj^2+bj+bj^2+bj^3+cj^2+cj^3+cj^4\\ &= a+aj+aj^2+bj+bj^2+b(4j+4)+cj^2+c(4j+4)+c(4j+4)j\\ &= a+aj+aj^2+bj+bj^2+4bj+4b+cj^2+4cj+4c+4cj^2+4cj\\ &= a+4b+4c+(a+b+4b+4c+4c)j+(a+b+c+4c)j^2\\ &= a+4b+4c+(a+3c)j+(a+b)j^2\end{aligned}$$

Należy rozwiązać układ równań:

$$\begin{cases} a+4b+4c=1\\ a+3c=0\\ a+b=0\end{cases}$$

Rozwiązaniem tego układu jest trójka $(a,b,c)=(4,1,2)$, czyli elementem odwrotnym do $1+j+j^2$ jest element $4+1j+2j^2$. Element przeciwny jest równy:

$$-(1+j+j^2) = -1-j-j^2 = 4+4j+4j^2$$

Zadanie 3. Niech $f : \mathbb{Q}[x] \to \mathbb{Q}(i)$ będzie określone wzorem $f(w) = w(2i)$. Korzystając z tego, że $\mathbb{Q}[x]$ jest pierścieniem ideałów głównych wyznacz jądro $\ker(f)$.

Rozwiązanie. (K. Kleczkowski)
Pokażmy, że $f : \mathbb{Q}[x] \to \mathbb{Q}(i)$ jest homomorfizmem. Weźmy dwa dowolne $a, b \in \mathbb{Q}[x]$. Policzmy:

$$f(a+b) = (a+b)(2i) = a(2i)+b(2i) = f(a)+f(b)$$

Podobnie:

$$f(a\cdot b) = (a\cdot b)(2i) = a(2i)\cdot b(2i) = f(a)\cdot f(b)$$

Również zauważamy, że $f(\mathbf{0}) = 0$ oraz $f(\mathbf{1}) = 1$.

Czyli f jest homomorfizmem.

Skoro mamy homomorfizm, to $\ker(f)$ jest ideałem w $\mathbb{Q}[x]$. Z twierdzenia Bézouta mamy, że $w(a) = 0$ wtedy i tylko wtedy, gdy $(x-a)|w$.

Zauważmy, iż ${}^{\mathbb{Q}[x]}/_{(x^2+1)} \cong \mathbb{Q}(i)$. Stąd z twierdzenia Bézouta mamy, że $w(2i) = 0$ wtedy i tylko wtedy, gdy $(x^2+4)|w$, bo w $\mathbb{Q}(i)$ mamy $(2i)^2+4 = 0$. Zatem $\ker(f) = (x^2+4)$.

Zadanie 4. Znajdź w pierścieniu $\mathbb{Z}_8[x]$ element odwrotny do wielomianu $w(x) = 1+2x^2$.

Rozwiązanie. (K. Kleczkowski)
Wielomian $w = w_0 + w_1x + \ldots + w_nx^n \in \mathbb{Z}_8[x]$ jest odwracalny wtedy i tylko wtedy, gdy w_0 jest odwracalny oraz w_i jest nilpotentem dla $i \geqslant 1$.[1]

Istotnie, wielomian $1+2x^2$ jest odwracalny, ponieważ 1 jest odwracalna i $2^3 = 0$. Weźmy więc $p \in \mathcal{U}(\mathbb{Z}_8[x])$ takie, że $p\cdot(1+2x^2) = 1$. Obliczmy więc:

$$\left(\sum_{n=0}^{\infty} p_nx^n\right)\left(1+2x^2\right) = \sum_{n=0}^{\infty} p_nx^n + \sum_{n=0}^{\infty} 2p_nx^{n+2} = p_0+p_1x+(p_2+2p_0)x^2+(p_3+2p_1)x^3+\ldots = 1$$

Niewątpliwie $p_0 = 1$ oraz $p_1 = 0$. Po rozwiązaniu układu równań (współczynniki odpowiednie przyrównujemy do zera), to otrzymujemy wielomian $p = 1+6x^2+4x^4$.

[1] Dowód tej obserwacji jest tutaj.

Zadanie 5. Niech K będzie ciałem charakterystyki p. Pokaż, że funkcja $f(x) = x^p$ jest różnowartościowym homomorfizmem z K do K.

Rozwiązanie. (K. Kleczkowski)
Sprawdźmy, czy $f : K \to K$ jest homomorfizmem. Weźmy $a, b \in K$.

$$f(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$$

Ponieważ ciało jest charakterystyki p i $p|\binom{p}{k}$ dla każdego $1 \leqslant k \leqslant p-1$, stąd mamy, że

$$\binom{p}{k} = pn = \underbrace{(1_K + 1_K + \ldots + 1_K)}_{p} \cdot n = 0 \cdot n = 0$$

Wobec tego $f(a+b) = a^p + b^p = f(a) + f(b)$. Dowodzenie zachowywania mnożenia jest trywialne. Czyli f jest homomorfizmem.

Pokażmy, że f jest iniekcją. Niech $f(a) = f(b)$ dla pewnych $a, b \in K$. Mamy, że $f(a) - f(b) = f(a-b) = 0_K$. Ponieważ jest to homomorfizm ciał, mamy, że $a - b = 0_K$ i $a = b$. □

Zadanie 6. Niech K będzie ciałem charakterystyki p. Wyznacz zbiór $\{x \in K : x^p = x\}$.

Rozwiązanie. (A. Lasecki i troszeczkę K. Kleczkowski)
Poszukujemy rozwiązań równania $x^p - x = 0$. Ponieważ jest to równanie stopnia p to wiemy, że będzie ono miało co najwyżej p rozwiązań.

Lemat. Każde ciało charakterystyki p zawiera podciało izomorficzne z $\mathbb{Z}_p$.
Rozważmy kanoniczny homomorfizm:

$$\varphi : \mathbb{Z} \to K$$

$$\varphi(n) = n1_k = \underbrace{1_k + \ldots + 1_k}_{n \text{ razy}}$$

Mamy wtedy, że:

$$\varphi(n+m) = (n+m)1_k = n1_k + m1_k = \varphi(n) + \varphi(m)$$

$$\varphi(nm) = (nm)1_k = (n1_k) \cdot (m1_k) = \varphi(n)\varphi(m)$$

$$\ker(\varphi) = p\mathbb{Z}$$

Wiemy, że $\ker(\varphi)$ jest ideałem w $\mathbb{Z}$, stąd ${}^{\mathbb{Z}}/_{\ker(\varphi)}$ jest pierścieniem ilorazowym, które jest ciałem, ponieważ $\ker(\varphi)$ jest ideałem maksymalnym. Z pierwszego twierdzenia o izomorfizmie otrzymujemy ${}^{\mathbb{Z}}/_{\ker(\varphi)} \cong \varphi[\mathbb{Z}]$, a z kolei $\varphi[\mathbb{Z}] \subseteq K$. Stąd mamy, że ${}^{\mathbb{Z}}/_{\ker(\varphi)}$ jest podciałem ciała K z dokładnością do izomorfizmu. Zauważmy, że ${}^{\mathbb{Z}}/_{\ker(\varphi)} = {}^{\mathbb{Z}}/_{p\mathbb{Z}} \cong \mathbb{Z}_p$. □

Z lematu wiemy, że w ciele K jest podciało izomorficzne z $\mathbb{Z}_p$, oznaczmy je jako P, a izomorfizm jako $\psi : P \to \mathbb{Z}_p$. Wiemy, że $|P| = p$ oraz, że $(\forall x \in P)\,(p \mid \psi\,(x^p - x))$. Tę własność dostajemy z izomorfizmu z $\mathbb{Z}_p$ oraz z faktu, że $x^{p-1} \equiv 1 \bmod p$. Wobec tego poszukiwanym przez nas zbiorem jest właśnie P.

4 Kody korekcyjne

Zadanie 1. Z przestrzeni liniowej $\mathbb{Z}_7 \times \mathbb{Z}_7$ konstruujemy płaszczyznę rzutową. Ile jest punktów w tej przestrzeni? Ile jest linii w tej przestrzeni?

Rozwiązanie. W zbiorze $\mathbb{Z}_7^3 \setminus \{(0,0,0\}$ definiujemy relację $\sim$

$$\bar{v} \sim \bar{u} \exists a \in \mathbb{Z}_7 \setminus \{0\} : \quad \bar{u} = a \cdot \bar{v}.$$

Jest to relacja równoważności, więc tworzy podział zbioru $\mathbb{Z}_7^3 \setminus \{(0,0,0\}$ na klasy abstrakcji.
Zbiór $(\mathbb{Z}_7^3 \setminus \{(0,0,0\})/_\sim$ wszystkich klas abstrakcji względem relacji $\sim$ nazywa się płaszczyzną rzutową i oznacza zwykle przez $\mathbb{P}^2_{\mathbb{Z}_7}$. Elementy płaszczyzny $\mathbb{P}^2_{\mathbb{Z}_7}$ (tj. klasy abstrakcji) nazywa się punktami. Klasą abstrakcji elementu $\bar{v} = (v_1, v_2, v_3) \in \mathbb{Z}_7^3 \setminus \{(0,0,0\}$ oznacza się przez $[v_1 : v_2 : v_3]$

$$[v_1 : v_2 : v_3] = [\bar{v}]_\sim = \{\bar{u} \in \mathbb{Z}_7^3 \setminus \{(0,0,0\} : \quad \bar{v} \sim \bar{u}\} = \{\bar{u} \in \mathbb{Z}_7^3 \setminus \{(0,0,0\} : \quad \exists a \in \mathbb{Z}_7 \setminus \{0\} : \quad \bar{u} = a\bar{v}\} =$$
$$= \{1 \cdot \bar{v}, 2 \cdot \bar{v}, 3 \cdot \bar{v}, 4 \cdot \bar{v}, 5 \cdot \bar{v}, 6 \cdot \bar{v}\} = \langle \bar{v} \rangle \setminus \{(0,0,0)\}.$$

Każda klasa abstrakcji ma 6 elementów (bo dla $a, b \in \mathbb{Z}_7 \setminus \{0\}$ je?li $a \neq b$, to $a \cdot \bar{v} \neq b \cdot \bar{v}$). Zatem wszystkich klas abstrakcji (punktów) jest $\frac{7^3-1}{6} = 57$.

Jeżli mamy dwa różne punkty $V = [v_1 : v_2 : v_3], U = [u_1 : u_2 : u_3] \in \mathbb{P}^2_{\mathbb{Z}_7}$, to odpowiadają im wektory $v = (v_1, v_2, v_3), u = (u_1, u_2, u_3) \in \mathbb{Z}_7^3 \setminus \{(0,0,0\}$. Wektory te rozpinają w $\mathbb{Z}_7^3$ płaszczyznę (podprzestrzeń dwuwymiarową), której elementy są postaci $a\bar{v} + b\bar{u}$ $(a, b \in \mathbb{Z}_7)$. Punkty odpowiadającej im prostej $UV \subset \mathbb{P}^2_{\mathbb{Z}_7}$ mają postać $[av_1 + bu_1 : av_2 + bu_2 : av_3 + bu_3]$. Prosta (linia) UV to zbiór

$$UV = \{[av_1 + bu_1 : av_2 + bu_2 : av_3 + bu_3] : \quad (a, b) \in \mathbb{Z}_7^2 \setminus \{(0,0)\}\}.$$

Każda prosta ma 8 punktów. Istotnie, parą (a, b) możemy wybrać na $7^2 - 1 = 48$ sposobów, ale jeśli $(a_1, b_1) = k(a_2, b_2)$ dla $k \neq 0$, to

$$[a_1v_1 + b_1u_1 : a_1v_2 + b_1u_2 : a_1v_3 + b_1u_3] = [ka_2v_1 + kb_2u_1 : ka_2v_2 + kb_2u_2 : ka_2v_3 + kb_2u_3] =$$
$$= [k(a_2v_1 + b_2u_1) : k(a_2v_2 + b_2u_2) : k(a_2v_3 + b_2u_3)] = [a_2v_1 + b_2u_1 : a_2v_2 + b_2u_2 : a_2v_3 + b_2u_3],$$

więc dla par $(a, b), (2a, 2b), (3a, 3b), (4a, 4b), (5a, 5b), (6a, 6b)$ dostajemy ten sam punkt. Stąd możemy parę (a, b) wybrać tak, by punkty się nie duplikowały na $\frac{48}{6} = 8$ sposobów.

Oczywiście, każda z $\binom{57}{2} = 1596$ możliwości wyboru dwóch punktów, daje nam prostą, ale nie jest to liczba wszystkich prostych, ponieważ przy różnych wyborach dwóch punktów, możemy otrzymać tą samą prostą. Trzeba policzyć ile razy zduplikowaliśmy tą samą prostą.
Mamy $\binom{8}{2} = 28$ możliwości wyboru dwóch różnych punktów z jednej prostej. Zatem wszystkich prostych mamy:

$$\frac{\binom{57}{2}}{\binom{8}{2}} = \frac{1596}{28} = 57.$$

W ogólnym przypadku: jeśli rozpatrujemy płaszczyznę rzutową $\mathbb{P}^2_{\mathbb{F}_q}$, to

- wszystkich punktów w tej przestrzeni jest
$$\frac{q^3 - 1}{q - 1} = q^2 + q + 1$$
- każda prosta ma punktów
$$\frac{q^2 - 1}{q - 1} = q + 1$$
- wszystkich prostych w tej przestrzeni jest
$$\frac{\binom{q^3-1}{2}}{\binom{q+1}{2}} = \frac{\binom{q^2+q+1}{2}}{\binom{q+1}{2}} = \frac{(q^2+q+1)!}{2! \cdot (q^2+q-1)!} \cdot \frac{2!(q-1)!}{(q+1)!} = \frac{(q^2+q+1)!}{(q^2+q-1)!} \cdot \frac{(q-1)!}{(q+1)!} =$$
$$= \frac{(q^2+q)(q^2+q+1)}{q(q+1)} = q^2 + q + 1$$

Rozwiązanie (Re-edit). Weźmy dowolne ciało K. Zdefiniujmy relację $\sim$ określoną na $K^{n+1} \setminus \{\mathbf{0}\}$ w następujący sposób:

$$\mathbf{u} \sim \mathbf{v} \iff (\exists \lambda \neq 0)(\mathbf{u} = \lambda \cdot \mathbf{v})$$

Jest to relacja równoważności. Definiujemy przez to płaszczyznę rzutową — $\mathbb{P}^n(K) := \left(K^{n+1} \setminus \{\mathbf{0}\}\right) /_\sim$. Punktami w przestrzeni rzutowej nazywamy klasy abstrakcji relacji $\sim$. Klasa abstrakcji wygląda następująco:

$$[\mathbf{v}]_\sim = \{\mathbf{u} \in K^n \setminus \{\mathbf{0}\} : (\exists \lambda \in K \setminus \{0\})(\mathbf{u} = \lambda \cdot \mathbf{v})\} = \{\lambda \cdot \mathbf{v} \in K^n \setminus \{\mathbf{0}\} : \lambda \in K \setminus \{0\}\} = \operatorname{span}\{\mathbf{v}\} \setminus \{\mathbf{0}\}$$

Prostą w takiej przestrzeni opisuje się przez:

$$[\mathbf{uv}] = \{[\mathbf{w}]_\sim : \mathbf{w} \in \operatorname{span}\{\mathbf{u}, \mathbf{v}\} \setminus \{\mathbf{0}\}\}$$

Analogicznie definiuje się wyższe podprzestrzenie.

Weźmy $\mathbb{P}^2(\mathbb{Z}_7)$. Zauważmy, że moc dowolnej klasy abstrakcji wynosi $7 - 1$, ponieważ $\mathbb{Z}_7^*$ jest cykliczna, a stąd parami różne punkty w otoczce będą wymnożone przez wszystkie elementy tej grupy. Po usunięciu wektora zerowego dostajemy, że klasa abstrakcji liczy $7 - 1$ elementów.

Dowolna linia ma $\frac{7^2-1}{7-1}$ elementów, ponieważ możemy na tyle sposobów wybrać skalary aby obliczyć otoczkę $\{\mathbf{u}, \mathbf{v}\}$.

Ilość wszystkich punktów jest równa $\frac{7^3-1}{7-1}$. Wszystkie pary punktów tworzące proste można wybrać na $\binom{\frac{7^3-1}{7-1}}{2}$ sposobów. Wszystkich punktów w prostej jest $\frac{7^2-1}{7-1}$, wobec tego należy usunąć wszystkie punkty, które generują tą samą prostą. Stąd wszystkich prostych jest

$$\frac{\binom{\frac{7^3-1}{7-1}}{2}}{\binom{\frac{7^2-1}{7-1}}{2}}$$

Zadanie 2. Czy istnieje kod liniowy o parametrach $[10, 5, 5]$?

Rozwiązanie. (K. Kleczkowski)
Przypuśćmy, że $\mathcal{C}$ jest $[10, 5, 5]$-kodem. Weźmy macierz generującą G i macierz parzystości H. Zauważmy, że $\Delta(\mathcal{C}) = 5$, czyli macierz H ma co najmniej 5 kolumn liniowo zależnych. Macierz H generuje kod dualny, który jest $[10, 10-5]$-kodem. Jednakże $\dim(\operatorname{span}(H)) < 5$, stąd mamy sprzeczność, kod nie istnieje. □

Zadanie 3. Pokaż, że zbiór $\mathcal{C} = \{(0, 0), (1, 2), (2, 4), (3, 1), (4, 3)\} \subseteq \mathbb{Z}_5^2$ jest kodem liniowym nad ciałem $\mathbb{Z}_5$. Wyznacz kod dualny do kodu $\mathcal{C}$.

Rozwiązanie. (K. Kleczkowski)
Niewątpliwie $\operatorname{span}\{(1, 2)\} = \mathcal{C}$, stąd $\mathcal{C}$ jest jednowymiarową podprzestrzenią liniową $(\mathbb{Z}_5)^2$, czyli $\mathcal{C}$ jest $[2, 1]_5$-kodem. Wobec tego kod dualny jest $[2, 1]_5$-kodem. Otrzymujemy, że $G = [1, 2]$ a stąd $H = [-2, 1] = [3, 1]$. Czyli $\operatorname{span}\{(3, 1)\} = \mathcal{C}^\perp$.

Zadanie 4. Niech

$$G = \begin{bmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 3 & 5 \end{bmatrix}$$

będzie macierzą generującą kod $\mathcal{C}$ długości 4 nad ciałem $\mathbb{Z}_7$. Pokaż, że $\mathcal{C}^\perp = \mathcal{C}$

Zadanie 5. Przekształć macierz kodu o macierzy generującej

$$G = \begin{bmatrix} 3 & 2 & 1 & 2 & 3 & 1 \\ 1 & 0 & 1 & 3 & 4 & 1 \end{bmatrix}$$

będzie macierzą generującą kod $\mathcal{C}$ nad ciałem $\mathbb{Z}_5$. Przekształć macierz G do postaci standardowej. Wyznacz parametry tego kodu.

Rozwiązanie. (J. Nigiel)
Zauważmy, że kolumny nr 1 i 5 są liniowo niezależne. Możemy zamieniać kolumny, zatem zamieńmy kolumnę 2 z 5. Otrzymujemy macierz $\begin{bmatrix} 3 & 3 & 1 & 2 & 2 & 1 \\ 1 & 4 & 1 & 3 & 0 & 1 \end{bmatrix}$. Teraz przekształcamy macierz, aby w pierwszych kolumnach otrzymać identyczność:

$$\begin{bmatrix} 3 & 3 & 1 & 2 & 2 & 1 \\ 1 & 4 & 1 & 3 & 0 & 1 \end{bmatrix} \underset{w_1 \leftarrow w_1 + 2 \cdot w_2}{\sim} \begin{bmatrix} 0 & 1 & 3 & 3 & 2 & 3 \\ 1 & 4 & 1 & 3 & 0 & 1 \end{bmatrix} \underset{w_2 \leftarrow w_2 + w_1}{\sim} \begin{bmatrix} 0 & 1 & 3 & 3 & 2 & 3 \\ 1 & 0 & 4 & 1 & 2 & 4 \end{bmatrix} \underset{k_1 \leftrightarrow k_2}{\sim} \begin{bmatrix} 1 & 0 & 3 & 3 & 2 & 3 \\ 0 & 1 & 4 & 1 & 2 & 4 \end{bmatrix}$$

Otrzymaliśmy postać standardową. Oczywiście $n = 6$, a $M = 2$. Zauważmy, że wszystkie kolumny (oprócz 3. i 6.) są liniowo niezależne, zatem jeśli w kodzie jedna z pozycji będzie równa 0, to albo $x = y = 0$ (wtedy cały kod jest 000000), albo tylko to miejsce będzie miało w kodzie 0. Ponieważ kolumna nr 3 powtarza się, jeśli w kodzie na 3 miejscu będzie 0, to na 6 też. Zatem $\Delta(\mathcal{C}) = \{min\{d_h(\bar{0}, \bar{c}) : c \in \mathcal{C} \setminus \{\bar{0}\}\}\} = 4$ (Ponieważ 0 może być w kodzie maksymalnie 2 razy). Stąd kod $\mathcal{C}$ jest $[6, 2, 4]_5$.

Zadanie 6. Korzystając ze wzoru Stirlinga wyznacz asymptotykę liczb $\binom{3n}{n}$.