Spis treści

Kazali mi to zdawać, choć algebrę miałem jakbym nie miał ciekawszych rzeczy do roboty i potrzebował tej powtórki. Fun times.

1 Operacje

Każdą funkcję która ma dwa argumenty i zwraca jeden wynik można nazwać operacją. Teoretycznie zatem można konwencjonalne operatory traktować jako funkcje. $+(1,1) = 2$

1.1 Działanie wewnętrzne i zewnętrzne

Działanie wewnętrzne w zbiorze A: $* : A \times A \to A$. Działanie zewnętrzne w zbiorze A: $* : F \times A \to A$

1.2 Własności operacji

Rozróżniamy kilka własności, które mogą mieć operacje.

- **Łączność** - $A * (B * C) = (A * B) * C$
- **Przemienność** - $A * B = B * A$
- **Rozdzielność** - $A * (B + C) = A * B + A * C$
- **Element neutralny** - $A * E = A$
- **Element odwrotny** - $A * A^{-1} = E$

2 Grupa

Grupa to zbiór G z działaniem wewnętrznym $*$ jeśli:

- $*$ jest łączne
- $*$ posiada element neutralny
- $*$ posiada element odwrotny

Dodatkowo jeśli $*$ jest przemienne to mamy grupę abelową.

2.1 Grupa $\mathbb{Z}_n$

Specyficzna grupa, która jest zbiorem liczb całkowitych od 0 do $n-1$ z działaniem $+$ modulo n. Elementem przeciwnym dla a jest $n-a$.

2.2 Grupa $\mathbb{Z}_n^\times$

$$\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n : NWD(a,n) = 1\}$$

A działanie tej grupy to mnożenie modulo n. Element przeciwny oblicza się algorytmem Euklidesa.

3 Podgrupa

Podgrupa to podzbiór grupy z odpowiednio dostosowanym działaniem. Na przykład podgrupą $\mathbb{Z}_{12}$ jest $(\{0,4,8\},+)$, ponieważ nie ma pary elementów z podzbioru, które po dodaniu dałyby coś spoza podzbioru.

3.1 Generowanie

Niech $(G,*)$ będzie grupą z elementem neutralnym E. Wtedy:

$$\langle g \rangle = \{\overbrace{g * g * \cdots * g}^{n} : n \in \mathbb{N}\} \cup \{E\} \cup \{\overbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}^{m} : m \in \mathbb{N}\}$$

Jeśli $G = \langle g \rangle$ dla pewnego g to G jest grupą cykliczną. Rzędem g jest $|\langle g \rangle|$

W $\mathbb{Z}_{12}$ podgrupą generowaną przez 4 jest $\{0,4,8\}$, a $rz(4) = |\langle 4 \rangle|$. Z kolei $\langle 1 \rangle = \mathbb{Z}_{12}$ zatem $\nVdash\nvDash$ jest grupą cykliczną. Jeżeli p jest liczbą pierwszą to $\mathbb{Z}_p^\times$ jest grupą cykliczną.

4 Funkcja Eulera

$$\varphi(n) = \begin{cases} 1 : n = 1 \\ |\mathbb{Z}_n^\times| : n > 1 \end{cases}$$

Jeśli p jest liczbą pierwszą to $\varphi(p^k) = p^k - p^{k-1}$ oraz $\varphi(p) = p-1$. Jeśli $NWD(m,n) = 1$ to $\varphi(mn) = \varphi(m)\varphi(n)$.

5 Permutacje

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$$

$$a_n = \pi(n)$$

5.1 Rozkład na cykle

$$\pi = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix} = (a_1, a_2, a_3, \ldots, a_n)$$

$$\pi' = \begin{pmatrix} a_1 & a_2 & b_1 & b_2 \\ a_2 & a_1 & b_2 & a_1 \end{pmatrix} = (a_1, a_2) \cdot (b_1, b_2)$$

5.2 Iloczyn transpozycji

$$(a_1, a_2, a_3, \ldots, a_k) = (a_1, a_k) \cdot (a_1, a_{k-1}) \cdot \cdots \cdot (a_1, a_3) \cdot (a_1, a_2)$$

5.3 Postać macierzowa

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

5.4 Znak permutacji

Ilość czynników w iloczynie transpozycji określa parzystość permutacji.

$$(-1)^n$$

gdzie n to ilość transpozycji

6 Pierścień

Pierścień to uporządkowana trójka $R(A, +, \cdot)$, gdzie A to zbiór, a + i $\cdot$ to działania spełniające następujące warunki:

- $(A, +)$ jest grupą abelową
- $+$ i $\cdot$ są są wewnętrzne dla A
- Dla każdego $a, b, c \in A$ zachodzi rozdzielność mnożenia względem dodawania: $a \cdot (b + c) = a \cdot b + a \cdot c$ oraz $(a + b) \cdot c = a \cdot c + b \cdot c$
- Istnieje element neutralny mnożenia $1 \in A : \forall a \in A : a \cdot 1 = 1 \cdot a = a$

6.1 Pierścień z jedynką

Pierścień z jedynką to pierścień, w którym istnieje element neutralny mnożenia oraz $A \neq \emptyset$

6.2 Pierścień przemienny

Pierścień przemienny to pierścień, w którym mnożenie jest przemienna

7 Ciało

Ciało $\mathbb{C}(K, +, \cdot)$ to pierścień przemienny z jedynką, oraz $(K \setminus \{0\}, \cdot)$ jest grupą. Innymi słowy: jest to niepusty zbiór K z działaniami $+$ i $\cdot$, które są przemienne, łączne, posiadają elementy neutralne i odwrotne, oraz istnieją takie pary (a, b) dla których:

$$a + b = 0 \text{ oraz } a \cdot b = 1$$

Przykładami ciał są: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

8 Wielomiany

Mówimy, że liczba z jest pierwiastkiem n-tego stopnia liczby w jeśli

$$z^n = w$$

Każdy wielomian $f \in \mathbb{C}[x]$ stopnia n ma n pierwiastków. Jeśli $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ to

$$f(x) = a_n (x - z_1)(x - z_2) \ldots (x - z_n)$$

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

Tabela 1: Dodawanie w wyżej zdefiniowanym ciele

8.1 Przykład ciała wielomianowego

Zbiór $\{0, 1, x, x+1\}$ z dodawaniem i mnożeniem modulo $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ jest ciałem.

8.2 Rozkładalność a ciała

Dlaczego zbiór $\{0, 1, x, x+1\}$ z dodawaniem i mnożeniem modulo $f(x) = x^2 + 1 \in \mathbb{Z}_2[x]$ nie jest ciałem? Ponieważ $x^2 + 1$ jest rozkładalny w $\mathbb{Z}_2[x]$.

Mówimy, że wielomian $f(x)$ jest rozkładalny w $\mathbb{Z}_p[x]$ jeśli gdy istnieją wielomiany $g_1, g_2 \in \mathbb{Z}_p[x]$ stopnia co najmniej 1 takie, że $f(x) = g_1(x)g_2(x)$.

Dla każdego $n \in \mathbb{N}$ i każdej liczby pierwszej p istnieje wielomian stopnia n w $\mathbb{Z}_p[x]$ który jest nierozkładalny.