Kryptografia z elementami algebry, wykład 1

Maciej Grześkowiak

10 grudnia 2021

Elementy algebry

Działania

Algebra zajmuje się badaniem działań określonych w pewnych zbiorach.

Definicja: Działaniem wewnętrzym (dwuargumentowym) w zbiorze A nazywamy dowolne odwzorowanie

$$* : A \times A \to A, \qquad (a, b) \to *(a, b).$$

Będziemy zapisywać $*(a, b) = a * b$.

Działania

Przykłady

- $\mathbb{N}^+ = (\mathbb{N}, +)$, $\mathbb{Z}^* = (\mathbb{Z}, *)$, $\mathbb{Q}^* = (\mathbb{Q}, *)$, $\ldots$,
- Niech $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$
- $\mathbb{Z}_n^+ = (\mathbb{Z}_n, +_n)$, $\mathbb{Z}_n^* = (\mathbb{Z}_n, *_n)$, gdzie $+_n = +\pmod{n}$,
- $\Phi(n) = \{a \in \mathbb{Z}_n^* : (a, n) = 1\}$, $(\Phi(n), *_n)$,
- $\ldots$

Działania

Algebra zajmuje się badaniem działań określonych w pewnych zbiorach.

Definicja: Działaniem wewnętrzym (dwuargumentowym) w zbiorze A nazywamy dowolne odwzorowanie

$$* : A \times A \to A, \qquad (a, b) \to *(a, b).$$

Będziemy zapisywać $*(a, b) = a * b$.

Działania

Niech $*$ będzie działaniem wewnętrzym w niepustym zbiorze A.

Definicja Mówimy, że działanie $*$ jest łączne, gdy

$$a * (b * c) = (a * b) * c, \qquad a, b, c \in A.$$

Przykład:
Dodawanie i mnożenie w $\mathbb{N}$ jest łączne.
Potęgowanie liczb naturalnych nie jest łączne tzn, działanie

$$\diamond : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \qquad \diamond(a, b) \to a^b.$$

Mamy,

$$2 \diamond (3 \diamond 5) = 2 \diamond 3^5 = 2^{243},$$
$$(2 \diamond 3) \diamond 5 = 8 \diamond 5 = 8^5 = 2^{15}.,$$

Działania

Definicja Mówimy, że działanie $*$ jest przemienne, gdy

$$a * b = b * a, \qquad a, b \in A.$$

Przykład:
Dodawanie i mnożenie w $\mathbb{N}$ jest przemienne.
Potęgowanie liczb naturalnych nie jest przemienne. Mamy,

$$a \diamond b = a^b,$$
$$b \diamond a = b^a.$$

Definicja Mówimy, że e jest elementem neutralnym działania $*$ jeśli

$$a * e = e * a = a, \qquad a \in A.$$

Przykład:
Elementy neutralne dodawania i mnożenia w $\mathbb{N}$ to 0 i 1.
Potęgowanie liczb naturalnych nie posiada elementu neutralnego. Mamy,

$$a \diamond e = a^e,$$
$$e \diamond a = e^a?$$

Działania

Definicja Niech działanie $*$ ma element neutralny. Mówimy, że $b \in A$ jest elementem przeciwnym do $a \in A$, gdy

$$a * b = b * a = e.$$

Stwierdzenie 1 Element neutralny, o ile istnieje, jest wyznaczony jednoznacznie. Jeżeli działanie jest łączne, to każdy element posiada co najwyżej jeden element przeciwny.

Dowód Niech e i e' będą dwoma elementami neutralnymi działania $*$. Wtedy,

$$e' = e * e',$$

ponieważ e jest elementem neutralnym. Podobnie,

$$e = e * e'.$$

Stąd, $e = e'$, co dowodzi pierwszej tezy. Niech b i c będą dwoma elementami przeciwnymi do a. Wtedy,

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$

Stąd, $b = c$.

Zasadnicze pojęcia teorii grup

Definicja Grupą nazywamy spełniające następujące warunki:

1. (łączność działania) $\forall a, b, c \in G \qquad a(bc) = (ab)c$,
2. (istnienie elementu neutralnego) $\exists e \in G \quad \forall a \in G \qquad ae = ea = a$,
3. (istnienie elementu odwrotnego) $\forall a \in G \quad \exists b \in G \qquad ab = ba = e$.

Definicja Grupę, w której działanie jest przemienne nazywany przemienną lub abelową.

Przykłady

1. Zbióry $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+, \mathbb{C}^+$ są grupami abelowymi,
2. Zbióry $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ (bez zera) są grupami abelowymi,
3. Zbiór reszt modulo n, $\mathbb{Z}_n^+ = \{0, 1, \ldots, n-1\}$ z działaniem dodawania (mod n),
4. Zbiór zredukowanych reszt modulo n, $\Phi(n) = \{a \in \mathbb{Z}_n : (a, n) = 1\}$ z działaniem mnożenia (mod n), jest grupą abelową,

Zasadnicze pojęcia teorii grup

Oznaczenia Przy zapisie addytywnym:. Element neutralny, to 0, a przeciwny do a, to $-a$. Przy zapisie multiplikatywnym:. Element neutralny, to 1, a odwrotny do a, to a^{-1}.

Definicja Rzędem grupy G nazywamy ilość jej elementów i oznaczamy $|G|$ lub $\sharp G$.

Przykład

1. $|\mathbb{Z}^+| = \infty$,
2. $|\mathbb{Z}_n^+| = n$,
3. $|\Phi(n)| = \varphi(n)$, gdzie

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Zasadnicze pojęcia teorii grup

Definicja Niepusty podzbiór H grupy G nazywamy podgrupą, gdy dla dowolnych $a, b \in H$ element $ab^{-1} \in$ H. Piszemy wtedy H $<$ G

Przykłady

1. $\mathbb{Z}^+$ jest podgrupą $\mathbb{Q}^+$,
2. $\mathbb{Q}^+$ jest podgrupą $\mathbb{R}^+$,
3. $\mathbb{Q}^*$ jest podgrupą $\mathbb{R}^*$,
4. $\mathbb{R}^*$ jest podgrupą $\mathbb{C}^*$,
5. $\{0, 6\}$ jest podgrupą $\mathbb{Z}_{12}^+$,
6. $\{1, 5\}$ jest podgrupą $\Phi(8)$,
7. $\Phi(n) < \Phi(n)$, $\mathbb{Z}^+ < \mathbb{Z}^+$.

Stwierdzenie 2 Niech G będzie grupą, $H \subset G$ niepustym podzbiorem. Wtedy następujące warunki są równoważne:

1. H jest podgrupą grupy G.
2. $e \in H$ oraz podzbiór H jest zamknięty ze względu na mnożenie i operacje brania odwrotności tzn. $ab, b^{-1} \in H$ dla dowolnych $a, b \in H$.
3. H wraz ze mnożeniem, które jest działaniem grupowym grupy G, jest grupą.

Dowód (1. $\Rightarrow$ 2) Niech a będzie dowolnym elementem H. Ponieważ $\mathrm{H} \neq \emptyset$ takie a istnieje. Zgodnie z definicją podgrupy $e = aa^{-1} \in \mathrm{H}$.

Podobnie korzystając z definicji podgrupy dla $e = a$ dostajemy $b^{-1} = eb^{-1} \in \mathrm{H}$. Ponieważ $b^{-1} \in \mathrm{H}$ mamy $ab = a(b^{-1})^{-1} \in \mathrm{H}$.

Implikacje (2. $\Rightarrow$ 3) i (3. $\Rightarrow$ 1) są oczywiste.

Zasadnicze pojęcia teorii grup

Zobaczymy w jaki sposób H wyznacza rozbicie G na rozłączne podzbiory.

Definicja Niech H będzie podgrupą grupy G. Warstwą lewostronną podgrupy H wyznaczoną przez element $a \in G$ nazywamy zbiór

$$aH = \{ah : h \in H\}.$$

Każdy element warstwy lewostronnej nazywamy jej reprezentantem.

Przykład Niech $H = \{0, 6\}$. Wiemy, że $H < \mathbb{Z}_{12}^{+}$. Weźmy $9 \in \mathbb{Z}_{12}^{+}$. Mamy,

$$9 + H = \{9 + h : h \in H\} = \{9 + 0, 9 + 6\} = \{9, 3\}$$

Stwierdzenie 3 Warstwy lewostronne są albo identyczne albo rozłączne. Suma mnogościowa wszystkich warstw lewostronnych jest równa całej grupie. Dwie warstwy lewostronne aH i bH są sobie równe wtedy i tylko wtedy, gdy $b^{-1}a \in$ H.

Dowód Niech $aH \cap bH \neq \emptyset$ i niech $ah = bh'$, gdzie $h, h' \in H$ są dowolnymi elementami. Wtedy $a = bh'h^{-1}$, a więc

$$ah'' = (bh'h^{-1})h'' = b(h'h^{-1}h'') \in bH.$$

Stąd $aH \subset bH$. Z symetrii założenia wynika, że $bH \subset aH$. Mamy więc $aH = bH$ i pierwsza teza jest udowodniona.

Ponieważ $a \in aH$ więc teza o sumie warstw lewostronnych jest oczywista.

Niech teraz $aH = bH$. Wtedy $a = bh$ dla pewnego $h \in H$. Mnożąc obustronnie przez b^{-1} otrzymujemy $b^{-1}a = h \in H$. Załóżmy, że $b^{-1}a \in H$. Wtedy,

$$b^{-1}a = h \in H \Rightarrow a = bh \Rightarrow a \in bH \Rightarrow aH \cap bH \neq \emptyset \Rightarrow aH = bH.$$

Zasadnicze pojęcia teorii grup

Analogicznie definiujemy warstwy prawostronne, są to podzbiory postaci

$$Ha = \{ha : h \in H\}.$$

Definicja Indeksem podgrupy H w grupie G nazywamy ilość (moc zbioru) różnych warstw lewostronnych H w G. Indeks oznaczamy symbolem (G : H).

Twierdzenie 1 (Lagrange) Niech G będzie grupą skończoną, a H jej podgrupą. Wtedy

$$|G| = (G : H)|H|.$$

Dowód Udowodnimy najpierw, że każda warstwa lewostronna aH jest równoliczna z H. W tym celu rozważmy odwzorowanie

$$f : \mathrm{H} \to a\mathrm{H}, \qquad f(h) = ah.$$

Jeśli $f(h) = f(h')$, to $ah = ah'$. Mnożąc obustronnie przez a^{-1} dostajemy $h = h'$. Zatem f jest injekcją (różnowartościowa). Z definicji warstwy lewostronnej wynika, że jest to też suriekcja. Więc zbiory aH i H są równoliczne. Teza jest teraz łatwa do uzyskanie. Zbiór G jest sumą (G : H) rozłącznych zbiorów, których każdy ma |H| elementów. Zatem $|\mathrm{G}| = (\mathrm{G} : \mathrm{H})|\mathrm{H}|$.

Kryptografia, złożoność obliczeniowa

Notacja wielkie-O

Definicja Niech $f, g : \mathbb{N} \mapsto \mathbb{R}$. Mówimy, że

$$f(n) = O(g(n))$$

jeśli istnieje stała $c > 0$ taka, że dla każdego $n \geq n_0$ mamy

$$|f(n)| \leq cg(n).$$

Własności:
Niech $f(n) = O(g(n))$, $u(n) = O(w(n))$, to

1. $f(n) \pm u(n) = O(g(n) + w(n))$,
2. $f(n)u(n) = O(g(n)w(n))$.

Notacja wielkie-O, przykłady

Zadanie: Zabadaj czy $f(n) = O(g(n))$ lub $g(n) = O(f(n))$, gdzie

$$f(n) = n^2 + n + 1, \quad g(n) = 50n + 30.$$

Rozwiązanie:
Istnieje $n_0 = 10$ oraz $c = 6$ takie, że dla każdego $n \geq n_0$ zachodzi

$$|50n_0 + 30| \leq c(n_0^2 + n_0 + 1)$$

Stąd, $50n + 30 = O(n^2 + n + 1)$.
Ustalmy $c > 0$. Istnieje n_0 takie, że dla każdego $n \geq n_0$ zachodzi

$$|n_0^2 + n_0 + 1| \geq c(50n_0 + 30)$$

Notacja wielkie-O, przykłady

Zadanie: Niech $LB(n)$ oznacza liczbę bitów n, dla $n \in \mathbb{N}$. Za pomocą notacji wielkie-O oszacuj funkcję $LB(n)$.

Rozwiązanie:
Niech

$$n = (b_{k-1} b_{k-2} \dots b_0)_2, \quad b_{k-1} = 1.$$

Stąd,

$$2^{k-1} \leq n < 2^k,$$

oraz

$$LB(n) = [\log_2 n] + 1 = [\frac{\log n}{\log 2}] + 1 = O(\log n).$$

Operacje elementarne na bitach

p	0	0	0	0	1	1	1	1
r_1	0	0	1	1	0	0	1	1
r_2	0	1	0	1	0	1	0	1
w	0	1	1	0	1	0	0	1
np	0	0	0	1	0	1	1	1

Operacje elementarne na bitach, przykład

Zadanie: Niech $a, b \in \mathbb{N}$, gdzie $a \geq b$. Ile elementarnych operacji na bitach potrzeba do obliczenia $S(a, b) = a + b$?

Zadanie: Niech $a, b \in \mathbb{N}$, gdzie $a \geq b$. Ile elementarnych operacji na bitach potrzeba do obliczenia $I(a, b) = ab$?

Operacje elementarne na bitach, przykład

Przykład: Niech $a = (1011)_2, b = (1001)_2$, to

$$\begin{array}{cccccc} & 1 & 0 & 1 & 1 \\ + & 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 & 0 \end{array}$$

Stąd, wykonujemy $O(\log a)$ operacji elementarnych na bitach.

Operacje elementarne na bitach, przykład

Przykład: Niech $a = (1011)_2, b = (1001)_2$, to

$$
\begin{array}{cccccccc}
 & & & & 1 & 0 & 1 & 1 \\
 & & & * & 1 & 0 & 0 & 1 \\
\hline
 & & & & 1 & 0 & 1 & 1 \\
 & & & 0 & 0 & 0 & 0 & \\
 & & 0 & 0 & 0 & 0 & & \\
+ & 1 & 0 & 1 & 1 & & & \\
\hline
\end{array}
$$

Stąd, wykonujemy $O(\log a)O(\log b) = O(\log^2 a)$ operacji elementarnych na bitach.

Notacja wielkie-O, przykłady

Zadanie 1: Zabadaj czy $f(n) = O(g(n))$ lub $g(n) = O(f(n))$, gdzie

1. $f(n) = n^3 + 1$, $g(n) = 1000n^2 + 60n$,
2. $f(n) = n + 1$, $g(n) = 5\log(n)$,
3. $f(n) = n^2 + n + 1$, $g(n) = 5n^2 + 7$.