Kryptografia z elementami algebry, wykład 3

Maciej Grześkowiak

19 października 2021

Elementy algebry

Stwierdzenie Niech A będzie dowolnym podzbiorem grupy G. Istnieje wtedy najmniejsza w sensie inkluzji podgrupa H grupy G zawierająca A.

Dowód Niech $\mathcal{J}$ będzie rodziną wszystkich podgrup grupy G zawierających A. Jest to rodzina niepusta, gdyż zawiera grupę G. Rozważmy zbiór

$$\mathrm{H}_0 = \bigcap_{\mathrm{H} \in \mathcal{J}} \mathrm{H},$$

to znaczy część wspólna podgrup z rodziny $\mathcal{J}$. Jest to podgrupa grupy G. Jasne jest, że jest to najmniejsza w sensie inkluzji podgrupa zawierająca A.

Uwaga Podgrupę, o której mowa, nazywamy podgrupą generowaną przez zbiór A i oznaczamy $\langle A \rangle$. Zbiór A nazywamy zbiorem generatorów podgrupy H.

Definicja Grupę, w której istnieje skończony zbiór generatorów nazywamy skończenie generowaną.

Definicja Grupę, w która posiada jednoelementowy zbiór generatorów nazywamy cykliczną.

Przykłady

1. Grupa $\mathbb{Z}^+$ jest cykliczna, a jej generatorem jest 1 (lub -1),
2. Grupa $\mathbb{Z}_n^+$ jest cykliczna, a jej generatorem jest 1,
3. Grupy $\Phi(2)$, $\Phi(4)$ są cykliczne,
4. Grupa $\Phi(p^k)$ jest cykliczna, gdzie $k \in \mathbb{N}$ oraz $p > 2$ jest liczbą pierwszą.
5. Grupa $\Phi(8)$ nie jest cykliczna.

Rząd elementu w grupie

Definicja Niech G będzie dowolną grupą, a g jej dowolnym elementem. Rząd grupy $\langle g \rangle$ nazywamy rzędem elementu g w grupie G i oznaczamy symbolem $\mathrm{ord}(g)$.

Uwaga $\langle g \rangle$ jest podgrupą grupy G.

Przykłady

1. $\mathrm{ord}(1)$ w grupie $\mathbb{Z}^+$ jest nieskończony
2. $\mathrm{ord}(1)$ w grupie $\mathbb{Z}_n^+$ jest równy n
3. $\mathrm{ord}(1) = 1$ w grupie $\Phi(2)$,
4. $\mathrm{ord}(1) = 1$, $\mathrm{ord}(3) = 2$ w grupie $\Phi(4)$,
5. Jeśli $\langle g \rangle = \Phi(p^k)$, to $\mathrm{ord(g)} = \varphi(p^k)$

Potęga o wykładniku całkowitym

Niech G będzie dowolną grupą, a g jej dowolnym elementem.
Dla $n \in \mathbb{Z}$ definiujemy symbol:
(notacja multiplikatywna)

$$g^n = \begin{cases} g \ldots g, & \text{gdy} \quad n > 0 \\ e, & \text{gdy} \quad n = 0 \\ g^{-1} \ldots g^{-1}, & \text{gdy} \quad n < 0 \end{cases}$$

(notacja addytywna)

$$ng = \begin{cases} g + \ldots + g, & \text{gdy} \quad n > 0 \\ e, & \text{gdy} \quad n = 0 \\ (-g) + \ldots + (-g), & \text{gdy} \quad n < 0 \end{cases}$$

Kryptografia, złożoność obliczeniowa

Funkcja jednokierunkowa

Definicja: Mówimy, że $f : \mathbb{N} \mapsto \mathbb{R}$ jest jednokierunkowa jeżeli:

1. obliczenie wartości f jest czasu wielomianowego ze względu na liczbę bitów danych,
2. obliczenie f^{-1} jest czasu wykładniczego, ze względu na liczbę bitów danych.

Funkcja jednokierunkowa, przykład

Przykład:
Niech G będzie dowolną grupą skończoną. Niech $g \in \mathrm{G}$ oraz $x < |\mathrm{G}|$
Definiujemy,

$$F(\mathrm{G}, g, x) = g^x \in \mathrm{G}$$

oraz

$$F^{-1}(\mathrm{G}, g, y) = x, \qquad \text{gdzie } y = g^x \qquad \text{dla} \quad y \in \mathrm{G}$$

o ile takie x istnieje.

Czy funkcja $F(\mathrm{G}, g, x)$ może być jednokierunkowa?

Funkcja jednokierunkowa, przykład

Przykład:
Niech $(\mathrm{G}, *)$ będzie grupą z działaniem $*$. Niech $g \in \mathrm{G}$ oraz $x < |\mathrm{G}|$
Definiujemy,

$$F(\mathrm{G}, g, x) = g * g * \ldots * g = g^x \in \mathrm{G}$$

oraz

$$F^{-1}(\mathrm{G}, g, y) = x, \qquad \text{gdzie } g^x = y, \quad y \in \mathrm{G}$$

Czy funkcja $F(\mathrm{G}, g, x)$ może być jednokierunkowa?

Funkcja jednokierunkowa, przykład

Przykład:
Niech p, q, $p > q$ będą różnymi liczbami pierwszymi. Czy funkcja $F(p, q) = pq$ może być jednokierunkowa? **Rozwiązanie:**

Wiemy, że

$$LB(p) = O(\log p), \quad LB(q) = O(\log q), \quad p > q$$

więc liczba bitów danych wynosi

$$O(\log p).$$

Ponadto, obliczenie $I(p, q)$ wymaga

$$O(\log^2 p).$$

Stąd, obliczenie $F(p, q)$ jest czasu wielomianowego.

Przykład:
Niech $p, q,\ p > q$ będą różnymi liczbami pierwszymi. Czy funkcja $F(p, q) = pq$ jest jednokierunkowa?

Rozwiązanie cd:
Niech $n = pq$,

$$I^{-1}(n) = d, \qquad d \mid n.$$

Ile operacji elementarnych na bitach wymaga obliczenie $F^{-1}(n)$? Naiwna metoda,

$$d = 2, 3, 4, 5, \ldots, [\sqrt{n}] + 1, \qquad \text{sprawdź } d \mid n?$$

Musimy wykonać $O(\sqrt{n})$ dzieleń, które wymagają

$$O(\log^2 n)$$

operacji elementarnych na bitach, stąd obliczenie $I^{-1}(n)$ wymaga

$$O(\sqrt{n})O(\log^2 n) = O(\sqrt{n}\log^2 n) = O((n\log^4 n)^{1/2}) = O(e^{\frac{1}{2}(\log(n\log^4 n))})$$

Przykład:
Niech $p, q,\ p > q$ będą różnymi liczbami pierwszymi. Czy funkcja $F(p, q) = pq$ jest jednokierunkowa?

Rozwiązanie cd:
Stąd obliczenie $I^{-1}(n)$ wymaga

$$\begin{aligned} O(\sqrt{n})O(\log^2 n) &= O(\sqrt{n}\log^2 n) = O((n\log^4 n)^{1/2}) \\ &= O(e^{\frac{1}{2}(\log(n\log^4 n))}) = O(e^{\frac{1}{2}(\log n + 4\log\log n))}) \\ &= O(e^{\frac{1}{2}\log n + 2\log\log n))}) = O(e^{\frac{1}{2}\log n}). \end{aligned}$$

Stąd, obliczenie $F^{-1}(n)$ jest czasu wykładniczego.
Funkcja $F(p, q)$ może być jednokierunkowa.

Elementy algebry

Homomorfizm grup

Definicja Odwzorowanie

$$f : G \to G'$$

nazywamy homomorfizmem grup jeśli

$$f(ab) = f(a)f(b), \qquad a, b \in G.$$

Mówimy, że

1. f jest monomorfizmem, gdy f jest injekcją,
2. f jest epimorfizmem, gdy f jest surjekcją,
3. f jest izomorfizmem, gdy f jest jednocześnie surjekcją i injekcją,

Przykłady

Rozważmy odwzorowanie

$$f : \mathbb{Z}^+ \to \Phi(7), \qquad f(n) = 3^n \pmod 7$$

Jest to homomorfizm. Istotnie

$$f(n+m) = 3^{n+m} \pmod 7 = 3^n 3^m \pmod 7 = f(n)f(m).$$

Przykłady

Rozważmy odwzorowanie

$$f : \mathbb{Z}^+ \to \mathbb{Z}_8^+, \qquad f(n) = n2 \pmod 8)$$

Jest to homomorfizm. Istotnie

$$f(n+m) = (n+m)2 \pmod 8 = n2 + m2 \pmod 8 = f(n)f(m).$$

Przykłady

Rozważmy odwzorowanie

$$f : \mathbb{Z}^+ \to \Phi(8), \qquad f(n) = 3^n \pmod 8$$

Jest to homomorfizm. Istotnie

$$f(n+m) = 3^{n+m} \pmod 8 = 3^n 3^m \pmod 8 = f(n)f(m).$$

Homomorfizm grup

Homomorfizm przenosi jedynkę G na jedynkę G′.
Istotnie,

$$f(e) = f(ee) = f(e)f(e).$$

Monożąc obustronnie przez $f(e)^{-1}$ dostajemy

$$e' = f(e).$$

Ponadto,

$$f(a^{-1}) = f(a)^{-1}.$$

Istotnie,

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e).$$

Stąd teza.

Definicja Zbiór

$$\mathrm{Ker}(f) = \{g \in \mathsf{G} : f(g) = e'\}$$

nazywamy jądrem homomorfizmu f.

Definicja Zbiór

$$\mathrm{Im}(f) = \{g' \in \mathsf{G}' : \exists g \in \mathsf{G} \;\; f(g) = g'\}$$

nazywamy obrazem homomorfizmu f.

Przykłady

Mamy homomorfizm,

$$f : \mathbb{Z}^+ \to \Phi(7), \qquad f(n) = 3^n \pmod 7$$

Wtedy,

$$\mathrm{Ker}(f) = \{n \in \mathbb{Z}^+ : f(n) = 1 \pmod 7)\} = 6\mathbb{Z}^+,$$

oraz

$$\mathrm{Im}(f) = \{a \in \Phi(7) : \exists n \in \mathbb{Z}^+ \;\; f(n) = a \pmod 7)\} = \Phi(7).$$

Przykłady

Mamy homomorfizm,

$$f : \mathbb{Z}^+ \to \mathbb{Z}_8^+, \qquad f(n) = n2 \pmod 8$$

Wtedy,

$$\mathrm{Ker}(f) = \{n \in \mathbb{Z}^+ : f(n) = 0 \pmod 8\} = 4\mathbb{Z}^+,$$

oraz

$$\mathrm{Im}(f) = \{a \in \mathbb{Z}_8^+ : \exists n \in \mathbb{Z}^+ \;\; f(n) = a \pmod 8\} = \{0, 2, 4, 6\}.$$

Przykłady

Mamy homomorfizm,

$$f : \mathbb{Z}^+ \to \Phi(8), \qquad f(n) = 3^n \pmod 8$$

Wtedy,

$$\mathrm{Ker}(f) = \{n \in \mathbb{Z}^+ : f(n) = 1 \pmod 8\} = 2\mathbb{Z}^+,$$

oraz

$$\mathrm{Im}(f) = \{a \in \Phi(8) : \exists n \in \mathbb{Z}^+ \ \ f(n) = a \pmod 0\} = \{1, 3\}.$$

Homomorfizm grup

Stwierdzenie 5 Niech $f : \mathsf{G} \to \mathsf{G}'$ będzie homomorfizmem grup. Wtedy $\mathrm{Im}(f)$ jest podgrupą grupy G', $\mathrm{Ker}(f)$ podgrupą grupy G.

Dowód Niech $a', b' \in \mathrm{Im}(f)$. Wtedy istnieją $a, b \in \mathsf{G}$ takie, że $a' = f(a)$ oraz $b' = f(b)$. Zatem,

$$a'(b')^{-1} = f(a)f(b)^{-1} = f(ab^{-1}),$$

to oznacza, że $a'(b')^{-1} \in \mathrm{Im}(f)$. Stąd $\mathrm{Im}(f)$ jest podgrupą G'. Weźmy $a, b \in \mathrm{Ker}\, f$. Wtedy $f(a) = f(b) = e'$. Stąd,

$$f(ab^{-1}) = f(a)f(b)^{-1} = e'.$$

Stąd $ab^{-1} \in \mathrm{Ker}(f)$. Zatem $\mathrm{Ker}(f)$ jest podgrupą G.

Stwierdzenie 6 Homomorfizm, którego jądro jest trywialne jest injekcją.
Dowód Niech $f(a) = f(b)$. Wtedy,

$$f(ab^{-1}) = f(a)f(b)^{-1} = e',$$

a więc $ab^{-1} \in \mathrm{Ker}(f)$. Ponieważ jądro jest trywialne, to $ab^{-1} = e'$, więć $a = b$.

Kryptografia, złożoność obliczeniowa

Problem Logarytmu Dyskretnego

Niech G będzie grupą cykliczną rzędu q, gdzie q jest liczbą pierwszą, a g jej generatorem. Rozważmy odwzorowanie

$$f : \mathbb{Z}^+ \to \mathrm{G}, \qquad f(n) = g^n.$$

Jest to homomorfizm. Istotnie

$$f(n+m) = g^{n+m} = g^n g^m = f(n)f(m).$$

Jądro tego homomorfizmu

$$\mathrm{Ker}(f) = \{n \in \mathbb{Z}^+ : f(g) = e\} = \{n : g^n = e\} = q\mathbb{Z}^+$$

jest podgrupą $\mathbb{Z}^+$.

Obraz tego homomorfizmu

$$\mathrm{Im}(f) = \{g' \in \mathrm{G} : \exists n \in \mathrm{Z}^+ \;\; f(n) = g'\} = \{g^n : n \in \mathbb{Z}^+\}$$

jest podgrupą G.

Ponadto, $g \in \mathrm{Im}(f)$. Wiemy, że g jest generatorem, a więc G jest najmniejszą w sensie inkluzji podgrupą zawierajacą g.

Stąd $\mathrm{Im}(f) = \mathrm{G}$, a zatem f jest epimorfizmem.

Problem Logarytmu Dyskretnego, (DLP)

Niech G będzie grupą cykliczną rzędu q, gdzie q jest liczbą pierwszą, a g jej generatorem. Rozważmy odwzorowanie

$$f : \mathbb{Z}^+ \to \mathsf{G}, \qquad f(n) = g^n.$$

Definicja Problem obliczenia odwrotności odwzorowania f nazywamy Problemem Logarytmu Dyskretnego przy podstawie g w grupie G.

To znaczy:
Dane: $g, y \in \mathsf{G}$
Oblicz: $n \in \mathbb{N}$ takie, że $g^n = y$.

Co więcej,

$$\mathsf{G} \cong \mathbb{Z}_q^+.$$

Istotnie, odwzorowanie

$$f : \mathsf{G} \to \mathbb{Z}_q^+, \qquad f(g^n) = n \pmod q.$$

jest homomorfizmem oraz

$$\mathrm{Ker}(f) = \{e\}, \qquad \mathrm{Im}(f) = \mathbb{Z}_q^+.$$