Nguyễn Hồ Đăng Duy - 22127085 - 22MMT

Bài 1. Cho tập số nguyên $\mathbb{Z}$ với phép toán $(*)$ được định nghĩa như sau:

- $m * n = m + n$ nếu m chẵn,
- $m * n = m - n$ nếu m lẻ.

Chứng minh rằng $(\mathbb{Z}, *)$ là một nhóm.

Để chứng minh $(\mathbb{Z}, *)$ là một nhóm, ta cần kiểm tra 4 tính chất

1) Tính đóng:

Nếu m chẵn: $m * n = m + n \in \mathbb{Z}$

Nếu m lẻ: $m * n = m - n \in \mathbb{Z}$

$(\forall m, n \in \mathbb{Z})$

Suy ra $(\mathbb{Z}, *)$ thoả tính đóng

2) Tính kết hợp

Xét $m, n, p \in \mathbb{Z}$, ta có:

(•) Nếu m, n, p đều chẵn

$(m * n) * p = (m * n) + p$

$= \underbrace{(m+n) + p = m + (n+p)}_{\text{Tính chất kết hợp của phép cộng}} = m * (n * p)$

(•) Nếu m lẻ, n và p chẵn $\rightarrow m * n = m - n$ lẻ

$(m * n) * p = (m - n) - p = m - n - p = m - (n + p) = m * (n * p)$

(•) Nếu n lẻ, m và p chẵn $\rightarrow \begin{cases} m * n = m + n & \text{lẻ} \\ n - p & \text{lẻ} \end{cases}$

$(m * n) * p = (m + n) * p = m + n - p = m + (n - p) = m * (n - p)$

(•) Nếu p lẻ, m và n chẵn

$(m * n) * p = (m + n) + p = m + n + p = m + (n + p) = m * (n * p)$

(•) Nếu m, n, p đều lẻ $\rightarrow m - n$ chẵn

$(m * n) * p = (m - n) * p = m - n + p = m - (n - p) = m * (n * p)$

Suy ra $(\mathbb{Z}, *)$ thoả tính kết hợp

3) Phần tử đơn vị

Ta có: (·) Nếu m chẵn: $m * 0 = m + 0 = m$

(·) Nếu m lẻ: $m * 0 = m - 0 = m$

Suy ra $(\mathbb{Z}, *)$ có phần tử đơn vị $e = 0$

4) Phần tử nghịch đảo

(·) Nếu m chẵn thì phần tử nghịch đảo của m là $-m$

Vì $m * (-m) = m + (-m) = 0 = e$

$(-m) * m = (-m) + m = 0 = e$

(·) Nếu m lẻ thì phần tử nghịch đảo của m là m

Vì $m * m = m - m = 0 = e$

Suy ra, với mọi trường hợp, ta đều tìm được phần tử nghịch đảo

Vậy qua 4 tính chất trên, ta kết luận $(\mathbb{Z}, *)$ là một nhóm

Bài 2. Ta định nghĩa tập $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ là tập các thặng dư không âm nhỏ nhất modulo n. Xét phép toán: với mọi $x, y \in \mathbb{Z}_n, x * y = (x + y) \pmod{n}$. Chứng minh rằng $(\mathbb{Z}_n, *)$ là một nhóm.

Để chứng minh $(\mathbb{Z}_n, *)$ là một nhóm, ta cần kiểm tra 4 tính chất

1) Tính đóng:

Xét $x, y \in \mathbb{Z}_n$, khi đó $0 \leq x, y \leq n-1$, từ đó

$0 \leq x + y \leq 2(n-1) < 2n$

nên $x * y = (x+y) \pmod{n}$ sẽ luôn nằm trong $\mathbb{Z}_n$

Vậy $x * y \in \mathbb{Z}_n \quad \forall x, y \in \mathbb{Z}_n$

2) Tính kết hợp

Xét $x, y, z \in \mathbb{Z}_n$, ta có

$$(x * y) * z = ((x+y)(\text{mod } n) + z) \bmod n$$
$$= (x+y+z) \bmod n$$
$$= (x + (y+z)) \bmod n$$
$$= (x + (y+z)(\text{mod } n)) \bmod n = x * (y * z)$$

Suy ra $(\mathbb{Z}_n, *)$ thoả tính kết hợp

3) phần tử đơn vị

Ta có, $\forall x \in \mathbb{Z}_n$ thì $x * 0 = (x+0) \bmod n = x \bmod n = x$
$0 * x = (0+x) \bmod n = x \bmod n = x$

Suy ra $(\mathbb{Z}_n, *)$ có phần tử đơn vị $e = 0$

4) Phần tử nghịch đảo

$\forall x \in \mathbb{Z}_n$, luôn tồn tại phần tử $(n-x) \in \mathbb{Z}_n$ sao cho
$x * (n-x) = (x + (n-x)) \bmod n = n \bmod n = 0 = e$
$(n-x) * x = ((n-x) + x) \bmod n = n \bmod n = 0 = e$

Suy ra, $\forall x \in \mathbb{Z}_n$, phần tử nghịch đảo của x là $(n-x)$

Vậy qua 4 tính chất trên, ta kết luận $(\mathbb{Z}_n, *)$ là một nhóm

Bài 3. Gọi $\mathbb{Z}_n^* = \{x | \gcd(x,n) = 1\}$ là tập các thặng dư không âm nguyên tố cùng nhau với n. Ta định nghĩa phép toán $\circ$ trên $\mathbb{Z}_n^*$ như sau: với mọi $x, y \in \mathbb{Z}_n, x \circ y = xy \pmod n$ (x nhân y theo nghĩa phép nhân thông thường trên tập số nguyên).

a) Chứng minh rằng $(\mathbb{Z}_n, \circ)$ là một nhóm.

b) Chỉ ra cấp của nhóm $(\mathbb{Z}_n, \circ)$ là $\phi(n)$-là phi hàm Euler.

c) Dựa vào câu b, chỉ ra rằng với mọi số nguyên tố p thì tập $\mathbb{Z}_p^*$ cùng với phép toán $\circ$ luôn luôn là một nhóm có $p-1$ phần tử.

a) Chứng minh rằng $(\mathbb{Z}_n^*, \circ)$ là một nhóm

Để chứng minh $(\mathbb{Z}_n^*, \circ)$ là một nhóm, ta cần kiểm tra 4 tính chất

1) Tính đóng:

$\forall x, y \in \mathbb{Z}_n^*$ thì $x \circ y = xy \pmod n$

Vì $x, y \in \mathbb{Z}_n^*$ nên $\gcd(x,n) = 1$ và $\gcd(y,n) = 1$ $\Big\} \Rightarrow \gcd(xy, n) = 1$

Suy ra, $x \circ y \in \mathbb{Z}_n^*$ hay $(\mathbb{Z}_n^*, \circ)$ thoả tính đóng

2) Tính kết hợp

$\forall x, y, z \in \mathbb{Z}_n^*$, ta có

$$(x \circ y) \circ z = \left(xy \pmod n\right) z \pmod n = xyz \pmod n$$
$$= x \pmod n \left((yz) \bmod n\right)$$
$$= x \circ (y \circ z)$$

Suy ra, $(\mathbb{Z}_n^*, \circ)$ thoả tính kết hợp

3) Phần tử đơn vị

$\forall x \in \mathbb{Z}_n^*$, ta có:

$x \circ 1 = x.1 \pmod n = x \pmod n = x$

$1 \circ x = 1.x \pmod n = x \pmod n = x$

Suy ra, $\forall x \in \mathbb{Z}_n^*$ có phần tử đơn vị $e = 1$

4) Phần tử nghịch đảo

$\forall x \in \mathbb{Z}_n^*$, vì $\gcd(x, n) = 1$ nên theo định lý Euler,

ta có: $x^{\phi(n)} \equiv 1 \pmod n$

Đặt $y = x^{\phi(n)-1}$, suy ra

$$x \circ y = xy \pmod n = x . x^{\phi(n)-1} \pmod n$$
$$= x^{\phi(n)} \pmod n = 1 = e$$

Suy ra, $\forall x \in \mathbb{Z}_n^*$ thì có phần tử nghịch đảo $y = x^{\phi(n)-1}$

Vậy qua 4 tính chất trên, ta kết luận $(\mathbb{Z}_n^*, \circ)$ là một nhóm

b) Chỉ ra cấp của nhóm $(\mathbb{Z}_n^*, \circ)$ là $\phi(n)$

- Cấp của một nhóm hữu hạn là số phần tử của nhóm đó

- Phi hàm Euler $\phi(n)$ dùng để đếm các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n

$\Rightarrow$ cấp của nhóm $(\mathbb{Z}_n^*, \circ)$ là $\phi(n)$ (dựa trên định nghĩa $\mathbb{Z}_n^*$)

c) Chỉ ra rằng $\forall$ số nguyên tố p thì $(\mathbb{Z}_p^*, \circ)$ luôn là nhóm có $p-1$ phần tử

Dựa trên kết quả câu b, ta có cấp của $\mathbb{Z}_p^*$ là $\phi(p)$

Mà p là số nguyên tố nên $\phi(p) = p - 1$

Bài 4. Chứng minh rằng $(\mathbb{Z}_6^*, \circ)$ và $(\mathbb{Z}_{17}^*, \circ)$ là các nhóm cyclic. Tìm các phần tử sinh của chúng.

1) $(\mathbb{Z}_6^*, \circ)$

Theo câu 3, $\mathbb{Z}_6^* = \{1, 5\}$ và phép toán $\circ$ được định nghĩa:

$\forall x, y \in \mathbb{Z}_6^*: x \circ y = xy \pmod 6$

Ta có: $5^2 = 5.5 \pmod 6 = 1$

$5^1 = 5 \pmod 6 = 5$

Vậy $(\mathbb{Z}_6^*, \circ)$ là một nhóm cyclic và có phần tử sinh là 5

2) $(\mathbb{Z}_{17}^*, \circ)$

Theo câu 3, $\mathbb{Z}_{17}^* = \{1, 2, 3, \dots, 16\}$ và phép toán $\circ$ được định nghĩa:

$\forall x, y \in \mathbb{Z}_{17}^*;\ x \circ y = xy \pmod{17}$

Ta có:

$3^1 = 3 \pmod{17} = 3$; $3^2 = 9 \pmod{17} = 9$

$3^3 = 27 \pmod{17} = 10$; $3^4 = 3^3.3 \pmod{17} = 13$

$3^5 = 3^4.3 \pmod{17} = 5$; $3^6 = 3^5.3 \pmod{17} = 15$

$3^7 = 3^6.3 \pmod{17} = 11$; $3^8 = 3^7.3 \pmod{17} = 16$

$3^9 = 3^8.3 \pmod{17} = 14$; $3^{10} = 3^9.3 \pmod{17} = 8$

$3^{11} = 3^{10}.3 \pmod{17} = 7$; $3^{12} = 3^{11}.3 \pmod{17} = 4$

$3^{13} = 3^{12}.3 \pmod{17} = 12$; $3^{14} = 3^{13}.3 \pmod{17} = 2$

$3^{15} = 3^{14}.3 \pmod{17} = 6$; $3^{16} = 3^{15}.3 \pmod{17} = 1$

Vậy $(\mathbb{Z}_{17}^*, \circ)$ là một nhóm cyclic và có phần tử sinh là 3 chứng.

Bài 5. Giả sử X là một nhóm cyclic cấp n sinh bởi phần tử a. Xét phần tử $b = a^k \in X$. Chứng minh rằng:

a) Cấp của b là $\dfrac{n}{d}$ với d là ước chung lớn nhất của n và k.

b) b là phần tử sinh của X khi và chỉ khi $(n, k) = 1$.

a) Để chứng minh cấp của b là $\frac{n}{d}$ với $d = \gcd(n, k)$ thì ta cần chứng minh 2 điều:

(i) $(a^k)^{\frac{n}{d}} = e$

(ii) $\forall m \in X, \ (a^k)^m = e \Rightarrow \frac{n}{d} \mid m$

Thật vậy, ta có:

(i) $(a^k)^{\frac{n}{d}} = a^{k.\frac{n}{d}} = (a^n)^{\frac{k}{d}} = e^{\frac{k}{d}} = e$ $\left(\frac{k}{d} \in \mathbb{N} \text{ vì } d \mid k\right)$

(ii) $\forall m \in X, \ (a^k)^m = e \Rightarrow a^{km} = e$
$\Rightarrow n \mid km$

$\Rightarrow \exists r \in \mathbb{Z} : km = n.r \quad (*)$

Vì $d = \gcd(n, k)$ nên ta có thể viết $k = d.k'$, khi đó $(k', \frac{n}{d}) = 1$

$(*) \Rightarrow dk'm = nr \Rightarrow k'm = \frac{n}{d} r \Rightarrow \frac{n}{d} \mid k'm \Rightarrow \frac{n}{d} \mid m$

Từ (i) và (ii), suy ra cấp của b là $\frac{n}{d}$

b) b là phần tử sinh của X $\Leftrightarrow a = b = a^k \Leftrightarrow k = 1$

$\Leftrightarrow (n, k) = (n, 1) = 1$

Vậy b là phần tử sinh của X khi và chỉ khi $(n, k) = 1$

Bài 6. Giả sử a, b là hai phần tử của một nhóm có cấp là r và s, $(r,s) = 1$ và $ab = ba$. Chứng minh rằng cấp của phần tử ab là rs.

Để chứng minh cấp của ab là rs thì ta phải chứng minh 2 điều:

(i) $(ab)^{rs} = e$

(ii) $\forall k$, $(ab)^k = e \Rightarrow rs \mid k$

Thật vậy:

(i) $(ab)^{rs} = \underbrace{ab.ab.ab\ldots}_{rs \text{ lần}} = a^{rs}.b^{rs}$ (vì $ab = ba$)

$= (a^r)^s.(b^s)^r$

$= e^s.e^r = e$

(ii) Tương tự, ta có: $(ab)^k = e \Leftrightarrow a^k.b^k = e$

$\Leftrightarrow a^k = b^{-k} \in \langle a \rangle \cap \langle b \rangle$ (*)

Đặt $H = \langle a \rangle \cap \langle b \rangle$. Ta có $\begin{cases} H \leq \langle a \rangle \\ H \leq \langle b \rangle \end{cases}$

nên $\begin{cases} |H| \mid |\langle a \rangle| = r \\ |H| \mid |\langle b \rangle| = s \end{cases} \Rightarrow |H| \mid (r,s) = 1$

Từ (*), suy ra $\begin{cases} a^k = e \\ b^{-k} = e \end{cases} \Rightarrow \begin{cases} r \mid k \\ s \mid k \end{cases} \Rightarrow rs \mid k$ (do $(r,s) = 1$)

Vậy cấp của ab là rs

Bài 7. Cho G là một nhóm cấp n và $(n, m) = 1$. Chứng minh rằng mọi phần tử h của G có một căn bậc m, nghĩa là $h = g^m$ với một g nào đó của G.

Theo định lý Lagrange, $\forall g \in G$ ta có: $g^n = e$

Vì $\gcd(n, m) = 1 \Rightarrow \exists a, b \in \mathbb{Z}: an + bm = 1$

$\forall h \in G$, xét $g = h^b$. Ta sẽ chứng minh rằng g là căn bậc m của h

Ta có:

$$g^m = (h^b)^m = h^{b.m} = h^{1-a.n} = h.(h^n)^{-a} = h.e = h$$

Do đó: $g = h^b$ là phần tử thỏa $g^m = h$

Vậy mọi $h \in G$ đều có phần tử thỏa mãn $g^m = h$ với $(n, m) = 1$

Bài 8. (**Khuyến khích sinh viên làm lấy điểm cộng**) Dựa vào định lý Lagrange và khái niệm cấp của một phần tử trong nhóm hữu hạn, hãy chứng minh định lý Fermat nhỏ và định lý Euler bằng ngôn ngữ của lý thuyết nhóm.

1) Định lý Fermat nhỏ: $a^{p-1} \equiv 1 \pmod p$ với $(a, p) = 1$ và p là số nguyên tố

Xét $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$ gồm các số nguyên nhỏ hơn p và không chia hết cho p (p là số nguyên tố)

Từ kết quả câu 3, ta có $\mathbb{Z}_p^*$ là một nhóm Abel có $e = 1$ và có cấp là $(p-1)$

Theo định lý Lagrange, cấp của phần tử $a \in \mathbb{Z}_p^*$ phải chia hết cho cấp của $\mathbb{Z}_p^*$, tức là chia hết cho $p-1$. Hay, nếu cấp của a là d thì $d \mid p-1$

$\Rightarrow a^{p-1} = e = 1 \Rightarrow a^{p-1} \equiv 1 \pmod p$ (đpcm)

2) Định lý Euler: $\forall a, n$: $\gcd(a, n) = 1$ thì $a^{\phi(n)} \equiv 1 \pmod{n}$

Xét $\mathbb{Z}_n^* = \{x \mid \gcd(x, n) = 1\}$. Từ kết quả câu 3 ta có $\mathbb{Z}_n^*$ là nhóm Abel có cấp là $\phi(n)$ và $e = 1$

Theo định lý Lagrange, cấp của $a \in \mathbb{Z}_n^*$ phải là ước của $\phi(n)$. Nghĩa là:

$$a^{\phi(n)} = e = 1 \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n} \quad (\text{đpcm})$$