TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA KHOA HỌC MÁY TÍNH

————-oOo————-

BÀI TẬP VỀ NHÀ
MÔN ĐẠI SỐ MÁY TÍNH

BÀI TẬP BUỔI 4
NHÓM

Lớp: CS522.M11

Giảng viên giảng dạy: TS. Nguyễn Đình Hiển

Nhóm sinh viên thực hiện:

1. Phan Thanh Hải 18520705
2. Trần Ngọc Sương 18521353

TP. HỒ CHÍ MINH, 11/2021

Mục lục

Bài 1.

Cho $\big(G, \cdot\big)$ là một nửa nhóm khác rỗng. Chứng minh các mệnh đề sau tương đương:

(i) $\big(G, \cdot\big)$ là một nhóm.

(ii) $\forall\, a, b \in G$, các phương trình $ax = b$ và $ya = b$ đều có nghiệm trong G.

(iii) Trong G có phần tử đơn vị trái e và:

$$\forall\, x \in G, \exists\, x' \in G \text{ sao cho } x'x = e$$

(iv) Trong G có phần tử đơn vị phải e' và:

$$\forall\, x \in G, \exists\, x'' \in G \text{ sao cho } x.x'' = e'$$

Bài làm:

1.1. Chứng minh (i) $\Rightarrow$ (ii)

Dễ dàng, ta thấy $x = a^{-1}b$ là nghiệm của phương trình $ax = b$. Ta cũng có thể chứng minh đây là nghiệm duy nhất. Giả sử, $c \in G$ cũng là nghiệm của phương trình trên thì ta có: $a^{-1}(ac) = a^{-1}b$ hay $c = a^{-1}b = x$.

Chứng minh tương tự, ta cũng có $y = a^{-1}b$ là nghiệm của phương trình $ax = b$.

1.2. Chứng minh (ii) $\Rightarrow$ (iii)

Do $\big(G, \cdot\big)$ khác rỗng nên tồn tại $a \in G$. Theo (ii) thì $ax = a$ có nghiệm trong G. Gọi $e \in G$ là nghiệm của phương trình $ax = a$. Cho $b \in G$. Gọi c là nghiệm của phương trình $ax = b$. Ta có:

$$eb = e(ac) = (ea)c = ac = b.$$

Do đó, e là phần tử đơn vị trái của G. Với mỗi $a \in G$, nghiệm của phương trình $ya = e$ là nghịch đảo trái của a.

1.3. Chứng minh (iii) $\Rightarrow$ (iv)

Cho $a \in G$. Gọi a' là nghịch đảo trái trái của a và a'' là nghịch đảo trái của a'. Ta có:

$$aa' = e(aa') = (a''a')(aa') = a''(a'a)a' = a''ea' = a''a' = e.$$

Khi đó, a' là nghịch đảo phải của a.

Ta lại có: $ae = a(a'a) = (aa')a = ea = a, \forall\, a \in G$.

Vì thế, e là phần tử đơn vị phải của G

1.4. Chứng minh (iv) $\Rightarrow$ (i)

Từ (iv), ta có: e' là phần tử đơn vị phải và $xx'' = e$, $\forall\, x \in G$, $\exists\, x'' \in G$

Ta cần chứng minh e' cũng là phần tử đơn vị trái.

Đặt $x' \in G$ sao cho $x''x' = e'$:

$$x''x = (x''x)e' = (x''x)(x''x') = x''(xx'')x' = x''ex' = x''x' = e'$$

Ta lại có:

$e'x = (xx'')x = x(x''x) = xe' = x \Rightarrow e'$ là phần tử đơn vị trái của G.

Khi đó, ta có: $\forall\, x \in G, \exists\, x' \in G$ sao cho $x'x = xx' = e$.

Do đó, $\big(G, \cdot\big)$ là một nhóm.

Từ **1.1, 1.2, 1.3** và **1.4**, ta đã chứng mình được 4 mệnh đề trên tương đương.

Bài 2.

(Định lý Lagrange) Cho G là một nhóm con hữu hạn và H là một nhóm con của G. Chứng minh rằng khi đó:

$$\big|G\big| = \big|H\big|.\big|G/H\big|$$

Với G/H là tập thương của G trên H theo quan hệ $\sim$ trong bài học.

Kí hiệu: $\big|A\big|$ nghĩa là số phần tử của tập hợp A, card(A).

Bài làm:

Nếu $G = H$ thì điều cần chứng minh là hiển nhiên đúng.

Giả sử $H = \{h_1, h_2, ...h_n\}$ nhỏ hơn nhóm G và $x \in G \setminus H$. Lúc này tất cả các phần tử của tập $Hx = \{h_1x, h_2x, ...h_nx\}$ khác nhau và không trùng với các phần tử của H. Vì từ $h_ix = h_jx$ dẫn đến $h_i = h_j$, nhưng $h_ix = h_j$ dẫn đến $x = h_i^{-1}h_j \in H$ là không thể. Nếu như $H \cup Hx = G$ thì định lý được chứng minh.

Nếu như $H \cup Hx$ nhỏ hơn G, thì có thể chọn $x' \in G \setminus (H \cup Hx)$ và thành lập nên tập $Hx' = \{h_1x', h_2x', ...h_nx'\}$. Tương tự các phần tử của tập này cũng khác nhau và không trùng với các phần tử của tập $H \cup Hx$. Cứ tiếp tục như thế, nhận kết quả như sau $G = H \cup Hx \cup Hx' \cup ...$

Từ đây có G chia hết cho n hay $\big|G\big| = \big|H\big|.\big|G/H\big|$.

Bài 3.

Chứng minh $\big(G, \cdot\big)$ là nhóm với:

a. $G = \mathbb{Z}$: tập các số nguyên.

$\cdot$ là phép toán cộng thông thường trên tập số nguyên.

b. Cho p là một số nguyên tố.

$G = \big\{1, 2, \dots, p-1\big\}$.

$\cdot$ là phép toán nhân trên số nguyên theo modulo p.

c. $G = \big\{A \mid A \in M^3\big(\mathbb{R}\big), \det\big(A\big) \neq 0\big\}$ với $M^3\big(\mathbb{R}\big)$ là tập hợp các ma trận vuông số thực bậc 3.

$\cdot$ là phép nhân trên ma trận.

Bài làm:

a. Hiển nhiên, ta có $G \neq \varnothing$.

Phép toán cộng trên G có tính chất kết hợp (vì phép cộng trên tập số nguyên cũng có tính chất kết hợp).

Tồn tại một phần tử đơn vị là phần tử $0 \in G$ sao cho $\forall\, x \in G$ thì $x + 0 = 0 + x = x$.

Tồn tại một phần tử khả nghịch $-x \in G$ của phần tử $x \in G$ sao cho $x + (-x) = -x + x = 0$.

Như vậy, $\big(G, \cdot\big)$ là nhóm. (đpcm)

b. Hiển nhiên, ta có $G \neq \varnothing$.

Phép nhân trên số nghuyên theo modulo p có tính chất kết hợp. Thật vậy, $\forall\, a_1, a_2, a_3 \in G, a_1 \equiv b_1 \pmod p, a_2 \equiv b_2 \pmod p, a_3 \equiv b_3 \pmod p$ thì ta có:

$$(a_1 \cdot a_2) \cdot a_3 \equiv (b_1 \cdot b_2) \cdot b_3 \pmod p \equiv b_1 \cdot (b_2 \cdot b_3) \pmod p \equiv a_1 \cdot (a_2 \cdot a_3).$$

Tồn tại một phần tử đơn vị là phần tử $1 \in G, 1 \equiv 1 \pmod p$ sao cho $\forall\, a \in G, a \equiv b \pmod p, a \cdot 1 = 1 \cdot a = a$. Thật vậy:

$$a \cdot 1 \equiv (b \cdot 1) \pmod p \equiv b \pmod p \equiv a.$$

$$1 \cdot a \equiv (1 \cdot b) \pmod{p} \equiv b \pmod{p} \equiv a.$$

Tồn tại một phần tử khả nghịch $r \in G$ của phần tử $a \in G$. Thật vậy:

Khi đó: $\gcd(a, p) = 1$. Suy ra, tồn tại một cặp (r, s) sao cho $ar + ps = 1$. Vì p là số nguyên tố nên $ar \pmod{p} \equiv 1$.

Như vậy, $(G, \cdot)$ là nhóm. (đpcm)

c. Hiển nhiên, ta có $G \neq \varnothing$.

Phép nhân giữa 2 ma trận vuông có tính kết hợp.

$\forall A \in G$, tồn tại một phần tử đơn vị là phần tử $I_{3,3} \in G$ sao cho $A \cdot I_{3,3} = I_{3,3} \cdot A = A$.

$\forall A \in G \setminus \{0\}$, $\det(A) \neq 0$ nên A là ma trận khả nghịch. Khi đó, ta luôn tìm được ma trận A^{-1} sao cho $A \cdot A^{-1} = A^{-1} \cdot A = I_{3,3}$.

Như vậy, $(G, \cdot)$ là nhóm. (đpcm)