# CHƯƠNG I. NHÓM

## A. CÁC DẠNG TOÁN VỀ NHÓM

**Dạng toán 1.** Kiểm tra $(G,.)$ có là một nhóm hay không.

**Cách giải 1:** $(G,.)$ là một nhóm nếu các tính chất sau được thỏa:

1) Qui tắc nhân (.) là một phép toán trên $G$, nghĩa là $\forall x,y\in G, xy$ được xác định duy nhất và $xy\in G$.
2) Tính kết hợp: $\forall x,y,z\in G,(xy)z=x(yz)$.
3) Tồn tại phần tử đơn vị phải $e\in G$, nghĩa là hệ phương trình $\forall x\in G, xy=x.$ (ẩn $y$) có nghiệm $y=e\in G$.
4) Mọi phần tử $x\in G$ đều khả nghịch phải trong G, nghĩa là phương trình $xy=e$ (ẩn $y$) có nghiệm $y\in G$ (phụ thuộc $x$).

**Nhận xét.** Có thể thay các tính chất 3 và 4 bằng các tính chất sau:

3′) Tồn tại phần tử đơn vị trái $e\in G$, nghĩa là hệ phương trình $\forall x\in G, yx=x.$ (ẩn $y$) có nghiệm $y=e\in G$.

4′) Mọi phần tử $x\in G$ đều khả nghịch trái trong G, nghĩa là phương trình $yx=e$ (ẩn $y$) có nghiệm $y\in G$ (phụ thuộc $x$).

**Cách giải 2:** $(G,.)$ là một nhóm nếu các tính chất sau được thỏa:

1) Qui tắc nhân (.) là một phép toán trên G, nghĩa là $\forall x,y\in G, xy$ được xác định duy nhất và $xy\in G$.
2) Tính kết hợp: $\forall x,y,z\in G,(xy)z=x(yz)$.
3) Với mỗi $a,b\in G$, các phương trình $ax = b$ (ẩn $x$) và $ya = b$ (ẩn $y$) có nghiệm trong $G$.

**Chú ý.** 1) Trong các cách giải trên, nếu một trong các tính chất không được thỏa thì $(G, .)$ không là nhóm.

2) Để chứng minh $(G,.)$ là một nhóm giao hoán, ngoài các tính chất trên ta cần kiểm tra thêm tính chất giao hoán: $\forall x,y\in G, xy=yx$.

3) $(G,.)$ là một nửa nhóm khi và chỉ khi phép toán nhân xác định trên $G$ và có tính kết hợp.

4) $(G,.)$ là một vị nhóm khi và chỉ khi phép toán nhân xác định trên $G$, có tính kết hợp và tồn tại phần tử đơn vị $e\in G$, nghĩa là hệ phương trình $\forall x\in G, xy=yx=x.$ (ẩn $y$) có nghiệm $y=e\in G$.

**Ví dụ 1.** Trong các trường hợp sau, hãy xét xem cấu trúc $(G,*)$ có là một nhóm hay không. Trong trường hợp $(G,*)$ là nhóm, hãy xét tính giao hoán của nhóm này.

a) $G=\mathbb{Q}\setminus\{-6\}, x*y=90xy+540x+540y+3234.$

b) $G=\mathbb{R}\times\mathbb{R}^*, (x,y)*(z,t)=(xz-yt,xt+yz).$

**Lời giải.**

a) Ta thấy $*$ là một phép toán trên G vì
$$\forall x, y \in G = \mathbb{Q} \setminus \{-6\},\ x * y = 90(x+6)(y+6) - 6 \in G.$$
- Tính giao hoán:
$$\forall x, y \in G,\ x * y = 90(x+6)(y+6) - 6 = 90(y+6)(x+6) - 6 = y * x.$$
- Tính kết hợp:
$$\forall x, y, z \in G, (x*y)*z = [90(x+6)(y+6)-6]*z = 8100(x+6)(y+6)(z+6) - 6$$
$$= x*[90(y+6)(z+6)-6] = x*(y*z).$$
- (G,$*$) có phần tử trung hòa là $-539/90$ vì với a $\in$ G ta có
$$\forall x \in G, x*a = x \Leftrightarrow \forall x \in G, 90(x+6)(a+6-6 = x \Leftrightarrow \forall x \in G, 90(x+6)(a+6) = x+6$$
$$\Leftrightarrow 90(a+6) = 1 \Leftrightarrow a = -\frac{539}{90} \in G.$$
- Mọi phần tử x $\in$ G có phần tử đối xứng là $\frac{1}{8100(x+6)} - 6 \in G$ vì với y $\in$ G ta có
$$x*y = -\frac{539}{90} \Leftrightarrow 90(x+6)(y+6) - 6 = -\frac{539}{90}$$
$$\Leftrightarrow 90(x+6)(y+6) = \frac{1}{90} \Leftrightarrow y = \frac{1}{8100(x+6)} - 6 \in G.$$
Suy ra $(G,*)$ là một nhóm giao hoán.

b) Ta thấy $*$ không phải là một phép toán trên G vì
$$\exists (x, y) = (1,1), (z, t) = (-1,1) \in G,\ (x, y) * (z, t) = (-2, 0) \notin G.$$
Do đó $(G,*)$ không phải là một nhóm.

**Ví dụ 2.** Chứng minh rằng một nửa nhóm khác rỗng, hữu hạn là một nhóm khi và chỉ khi phép toán tương ứng có tính giản ước. Chỉ ra rằng điều kiện hữu hạn không thể bỏ được.

**Lời giải.** ($\Rightarrow$) Hiển nhiên vì phép toán trong một nhóm có tính giản ước.

($\Leftarrow$) Theo Định lý 3.5, ta chỉ cần chứng minh rằng với mọi $a$, $b \in G$, các phương trình $ax = b$ và $ya = b$ đều có nghiệm trong $G$. Thật vậy, xét các ánh xạ:
$$\varphi : G \to G, \varphi(x) = ax \text{ và } \psi : G \to G, \psi(x) = yb.$$
Ta thấy $\varphi$, $\psi$ đều là đơn ánh. Thật vậy, do tính giản ước của phép nhân, ta có
$$\forall x, x' \in G, \varphi(x) = \varphi(x') \Rightarrow ax = ax' \Rightarrow x = x'.$$
Điều này chứng tỏ $\varphi$ là đơn ánh. Tương tự, $\psi$ cũng là đơn ánh. Từ đây, do tính hữu hạn của G, ta có $\varphi$, $\psi$ cũng là toàn ánh, và do đó các phương trình $ax = b$ và $ya = b$ đều có nghiệm trong $G$.

Giả thiết $G$ hữu hạn không thể bỏ được. Thật vậy, xét nửa nhóm vô hạn $(\mathbb{Z},+)$, ta thấy phép toán + có tính giản ước trong $\mathbb{Z}$ nhưng $(\mathbb{Z},+)$ không là nhóm.

**Dạng toán 2.** Chứng minh $H$ là một nhóm con của nhóm $(G,.)$.

**Cách giải**: Chứng minh các tính chất sau:
1) H $\subset$ G.
2) $e \in H$ (hay chỉ ra $H \neq \varnothing$).
3) $\forall x, y \in G, xy \in G.$.

4) $\forall x \in G, x^{-1} \in G.$

**Chú ý.** Có thể thay các tính chất 3 và 4 bằng tính chất 5 sau đây:

5) $\forall x, y \in G, x^{-1}y \in G.$

**Ví dụ.** Chứng minh $\mathrm{H} = \left\{ \begin{pmatrix} \mathrm{x} & \mathrm{y} \\ 2\mathrm{y} & \mathrm{x} \end{pmatrix} : \mathrm{x}, \mathrm{y} \in \mathbb{Q}, \mathrm{x}^2 + \mathrm{y}^2 > 0 \right\}$ là một nhóm con của nhóm $\mathrm{GL}(2, \mathbb{Q})$.

**Lời giải.** Trước hết ta nhận xét rằng

$$\forall \mathrm{x}, \mathrm{y} \in \mathbb{Q}, \begin{pmatrix} \mathrm{x} & \mathrm{y} \\ 2\mathrm{y} & \mathrm{x} \end{pmatrix} \in \mathrm{H} \Leftrightarrow \begin{pmatrix} \mathrm{x} & \mathrm{y} \\ 2\mathrm{y} & \mathrm{x} \end{pmatrix} \neq 0.$$

Ta chứng minh $\mathrm{H} \leq (\mathrm{GL}(2, \mathbb{Q}), .)$ Thật vậy,

- $\mathrm{H} \subset \mathrm{GL}(2, \mathbb{Q})$ do $\forall \mathrm{x}, \mathrm{y} \in \mathbb{Q}, \mathrm{x}^2 + \mathrm{y}^2 > 0 \Rightarrow \begin{vmatrix} \mathrm{x} & \mathrm{y} \\ 2\mathrm{y} & \mathrm{x} \end{vmatrix} = \mathrm{x}^2 - 2\mathrm{y}^2 \neq 0.$
- $\mathrm{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{H}.$
- $\forall \mathrm{A} = \begin{pmatrix} \mathrm{x} & \mathrm{y} \\ 2\mathrm{y} & \mathrm{x} \end{pmatrix}, \mathrm{B} = \begin{pmatrix} \mathrm{z} & \mathrm{t} \\ 2\mathrm{t} & \mathrm{z} \end{pmatrix} \in \mathrm{H}, \mathrm{AB} \neq 0 (\mathrm{do}\, \mathrm{AB} \in \mathrm{GL}(2, \mathbb{Q})), \mathrm{AB} = \begin{pmatrix} \mathrm{xz} + 2\mathrm{yt} & \mathrm{xt} + \mathrm{yz} \\ 2(\mathrm{xt} + \mathrm{yz}) & \mathrm{xz} + 2\mathrm{yt} \end{pmatrix}$

nên $\mathrm{AB} \in \mathrm{H}$.

- $\forall \mathrm{A} = \begin{pmatrix} \mathrm{x} & \mathrm{y} \\ 2\mathrm{y} & \mathrm{x} \end{pmatrix} \in \mathrm{H}, 0 \neq \mathrm{A}^{-1} = \frac{1}{\mathrm{x}^2 - 2\mathrm{y}^2} \begin{pmatrix} \mathrm{x} & -\mathrm{y} \\ -2\mathrm{y} & \mathrm{x} \end{pmatrix} = \begin{pmatrix} \frac{\mathrm{x}}{\mathrm{x}^2 - 2\mathrm{y}^2} & -\frac{\mathrm{y}}{\mathrm{x}^2 - 2\mathrm{y}^2} \\ -2\frac{\mathrm{y}}{\mathrm{x}^2 - 2\mathrm{y}^2} & \frac{\mathrm{x}}{\mathrm{x}^2 - 2\mathrm{y}^2} \end{pmatrix}$

nên $\mathrm{A}^{-1} \in \mathrm{H}$.

**Dạng toán 3.** Chứng minh $H$ là nhóm con sinh bởi tập hợp $S$.

**Cách giải**: Để chứng minh $\mathrm{H} = < \mathrm{S} >$ ta tiến hành các bước sau:

1) Chứng minh $H \leq G$ (xem Dạng toán 2).
2) Chứng minh $S \subset H$.
3) Với mọi $x \in H$, chỉ ra $x \in < S >$ bằng cách biểu diễn $x$ dưới dạng $x = s_1 s_2 \ldots s_n$, trong đó $s_i \in S$ hay $s_i \in S^{-1}$ với mọi $1 \leq \mathrm{i} \leq \mathrm{n}$.

**Ví dụ.** Chứng minh nhóm thay phiên $A_n$ được sinh bởi các 3-chu trình.

**Lời giải.** Gọi $H$ là nhóm con của $S_n$ sinh bởi các 3-chu trình. Vì mọi 3-chu trình đều là hoán vị chẵn nên $H \subset A_n$. Đảo lại, xét $\sigma = (i\ j)(k\ l)$ là tích của hai chu trình. Ta có

- Nếu $|\{i, j\} \cap \{k, l\}| = 2$ thì $\{i, j\} = \{k, l\}$ và $\sigma = \mathrm{Id} \in H$.
- Nếu $|\{i, j\} \cap \{k, l\}| = 1$ thì ta có thể giả sử $i \neq j = k \neq l \neq i$ nên $\sigma = (i\ j)(j\ l) = (i\ j\ l) \in H$.

- Nếu $|\{i,j\}\cap\{k,l\}|=0$ thì $i,j,k,l$ đôi một khác nhau và ta có

$$\sigma=(i\ j)(k\ l)=(i\ j)(j\ k).(j\ k)(k\ l)\in H \text{ (theo lý luận trên).}$$

Kết quả trên chứng tỏ $H$ chứa tất cả các phép hoán vị có dạng tích của hai chu trình. Từ đây, do mọi hoán vị chẵn là tích của một số chẵn chu trình nên chúng cũng thuộc $H$, điều này chứng tỏ $A_n\subset H$. Vậy $A_n=H$ là là nhóm con sinh bởi các 3-chu trình.

**Dạng toán 4.** Xác định cấp $n$ (nguyên dương) của một phần tử $x$ có cấp hữu hạn trong một nhóm.

**Cách giải 1:** Chứng minh $n$ là số nguyên dương nhỏ nhất thỏa $x^n=e$, nghĩa là

1) $\forall 1\le k<n, x^k\ne e$;

2) $x^n=e$.

**Cách giải 2:** Chứng minh các tính chất sau:

1) $x^n=e$;

2) $\forall k\in\mathbb{Z}, x^k=e\Rightarrow k\vdots n$.

**Ví dụ.** Chứng minh rằng trong nhóm hoán vị $S_n$, mọi k-chu trình đều có cấp k và cấp của tích các chu trình rời nhau bằng bội số chung nhỏ nhất của các cấp của các chu trình này.

**Lời giải.** a) Cho $\sigma=(i_1\dots i_k)$ là một k-chu trình. Khi đó, với mọi số nguyên dương $m<k$, ta có

$$\begin{cases}\sigma^m(i_1)=i_{m+1}\ne i_1,\\ \sigma^k(i_r)=i_r,\forall 1\le r\le k,\\ \sigma^k(i)=i,\forall i\in\{1,\dots,n\}\setminus\{i_1,\dots,i_k\}\end{cases}$$

nên $\sigma^k=\mathrm{Id}$ và $\forall 1\le m<k, \sigma^m\ne \mathrm{Id}$. Do đó $\sigma$ có cấp $k$.

b) Cho $\sigma_1,\dots,\sigma_r$ là các chu trình rời nhau từng đôi một, có cấp lần lượt là $k_1,\dots,k_r$. Gọi $k$ là bội số chung nhỏ nhất của $k_1,\dots,k_r$. Vì các chu trình rời nhau thì giao hoán lẫn nhau nên

$$(\sigma_1\dots\sigma_r)^k=\sigma_1^{\,k}\dots\sigma_r^{\,k}=\mathrm{Id}\dots\mathrm{Id}=\mathrm{Id}.$$

Mặt khác,

$$\forall m\in\mathbb{Z},(\sigma_1\dots\sigma_r)^m=Id\Rightarrow\sigma_1^{\,m}\dots\sigma_r^{\,m}=Id$$

$$\Rightarrow\begin{cases}\sigma_1^{\,m}=Id\\ \dots\qquad (do\ \sigma_1,\dots,\sigma_r \text{ roi nhau})\\ \sigma_r^{\,m}=Id\end{cases}$$

$$\Rightarrow\begin{cases}m\vdots k_1\\ \dots\qquad\Rightarrow m\vdots k.\\ m\vdots k_r\end{cases}$$

Suy ra $\sigma_1\dots\sigma_r$ có cấp $k$.

**Dạng toán 5.** Tìm các phần tử có cấp hữu hạn trong một nhóm.
**Cách giải:** Xét nhóm $(G,*)$, ta tiến hành các bước sau:

1) Với $x \in G, n \in \mathbb{N}^*$, tìm biểu thức của $x^n = \underbrace{x*...*x}_{n}$.
2) Xác định $x \in G$ sao cho phương trình $x^n = e$ (ẩn $n$) có nghiệm $n \in \mathbb{N}^*$.

**Ví dụ.** Trong nhóm $(G,*)$ ở Câu a, Ví dụ 1, Dạng toán 1, hãy tìm tất cả các phần tử có cấp hữu hạn.
**Lời giải**. Với x ∈ G và n ≥ 1, bằng qui nạp ta chứng minh được rằng

$$\underbrace{x*...*x}_{n} = 90^{n-1}(x+6)^n - 6.$$

Do đó với $x \in G$ ta có

$$o(x) < \infty \Leftrightarrow \exists n \geq 1, \underbrace{x*...*x}_{n} = -\frac{539}{90} \Leftrightarrow \exists n \geq 1,\ 90^{n-1}(x+6)^n - 6 = -\frac{539}{90}$$

$$\Leftrightarrow \exists n \geq 1,\ (x+6)^n = \frac{1}{90^n} \Leftrightarrow \left[\begin{array}{l} x+6 = \frac{1}{90} \\ x+6 = -\frac{1}{90} \end{array}\right. \Leftrightarrow \left[\begin{array}{l} x = -\frac{539}{90} \in G \\ x = -\frac{541}{90} \in G. \end{array}\right.$$

Vậy trong G chỉ có hai phần tử có cấp hữu hạn là $x_1 = -\frac{539}{90}, x_2 = -\frac{541}{90}$.

**Dạng toán 6.** Chứng minh $H$ là một nhóm con chuẩn tắc của nhóm $(G,*)$.
**Cách giải:** Chứng minh các tính chất sau:

1) $H$ là một nhóm con của $G$ (xem Dạng toán 2);
2) $\forall x \in G, x^{-1}Hx \subset H$, nghĩa là $\forall x \in G, \forall h \in H, x^{-1}hx \in H$.

**Nhận xét:** Có thể thay tính chất 2 bằng tính chất 2′ sau:

2′) $\forall x \in G, xHx^{-1} \subset G$, nghĩa là $\forall x \in G, \forall h \in H, xhx^{-1} \in G$.

**Ví dụ.** Cho $H$, $K$ là hai nhóm con của nhóm $(G,.)$. Chứng nminh rằng

a) Nếu $H$ chuẩn tắc trong $G$ thì $HK$ là nhóm con của $G$.
b) Nếu $H$, $K$ đều chuẩn tắc trong $G$ thì $HK$ là nhóm con chuẩn tắc của $G$.

**Lời giải.** a) Cho $H \lhd G, K \leq G$. Khi đó $HK \leq G$ vì

- $e = ee \in HK$.
- $\forall h_1, h_2 \in H, \forall k_1, k_2 \in K, (h_1k_1)^{-1}(h_2k_2) = (k_1^{-1}h_1^{-1}k_1)(k_1^{-1}h_2k_1)(k_1^{-1}k_2) \in HK$.

b) Cho $H \lhd G, K \lhd G$. Theo Câu a, $HK \leq G$, hơn nữa,

$\forall x \in G, x^{-1}(HK)x = (x^{-1}Hx)(x^{-1}Kx) = HK$.

Do đó $HK \lhd G$.

**Dạng toán 7.** Chứng minh qui tắc $f: G \to G'$ là một đồng cấu từ nhóm $(G,.)$ vào nhóm $(G',.)$.
**Cách giải:** Chứng minh các tính chất sau:

1) $f$ là một ánh xạ từ $G$ đến $G'$, nghĩa là
   - $\forall x \in G, f(x) \in G'$;
   - $\forall x, y \in G, x = y \Rightarrow f(x) = f(y)$.
2) $\forall x, y \in G, f(xy) = f(x)f(y)$.

**Ví dụ.** Cho $G$, $G'$ lần lượt là các nhóm cyclic hữu hạn cấp $m$, $n$ với các phần tử sinh là $x$ và $y$. Xét tương ứng $f$: $G \to G'$ định bởi $f(x^k) = y^{kl}$ với mọi $k \in \mathbf{N}$, trong đó $l \in \mathbf{N}^*$ cho trước. Chứng minh rằng $f$ là một đồng cấu nhóm khi và chỉ khi $ml$ chia hết cho n.
**Lời giải**.

a) ($\Rightarrow$) Nếu $f$ là một đồng cấu nhóm thì $e' = f(e) = f(x^m) = y^{ml}$ nên $ml$ chia hết cho $o(y) = n$.

($\Leftarrow$) Giả sử $ml$ chia hết cho $o(y) = n$. Khi đó

- $f$ là một ánh xạ từ $G$ đến $G'$. Thật vậy,

$$\forall r, s \in \mathbf{Z}, x^r = x^s \Rightarrow m|(r-s) \Rightarrow ml|\ (r-s)l$$

$$\Rightarrow n|(r-s)l \Rightarrow n|(rl-sl)$$

$$\Rightarrow y^{rl} = y^{sl}, \text{ nghĩa là } f(x^r) = f(x^s).$$

- $\forall r, s \in \mathbf{Z}, f(x^r x^s) = f(x^{r+s}) = y^{(r+s)l} = y^{rl+sl} = y^{rl}y^{sl} = f(x^r)f(x^s)$.

Do đó $f$ là một đồng cấu nhóm.

**Dạng toán 8.** Chứng minh qui tắc $f$: $G \to G'$ với $(G,.)$, $(G',.)$ là các nhóm, là một đơn cấu (toàn cấu, đẳng cấu).
**Cách giải:** Tiến hành các bước sau:
1) Chứng minh $f$ là một đồng cấu (Xem Dạng toán 7).
2) Đơn cấu: Chứng minh $f$ là đơn ánh bằng cách chỉ ra $\ker(f) = \{e'\}$, nghĩa là $\forall x \in G, f(x) = e \Rightarrow x = e'$.
3) Toàn cấu: Chứng minh $f$ là toàn ánh bằng cách chỉ ra $\text{Im}(f) = G'$, nghĩa là $\forall y \in G'$, phương trình $f(x) = y$ (ẩn x) luôn luôn có nghiệm trong $G$.
4) Đẳng cấu: Chứng minh $f$ là song ánh bằng cách chỉ ra $f$ có ánh xạ ngược, nghĩa là $\forall y \in G'$, phương trình $f(x) = y$ (ẩn x) luôn luôn có duy nhất một nghiệm trong $G$.

**Ví dụ.** Cho nhóm $(G,.)$. Chứng minh rằng với mỗi $g \in G$, ánh xạ $\varphi_g$: $G \to G$ định bởi $\varphi_g(x) = gxg^{-1}$ là một tự đẳng cấu của $G$.
**Lời giải.** $\varphi_g$ là một tự đẳng cấu của $G$ vì
- $\varphi_g$ là một đồng cấu do $\forall x, y \in G, \varphi_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \varphi_g(x)\varphi_g(y)$.
- $\varphi_g$ là một song ánh do $\forall x, y \in G, \varphi_g(x) = y \Leftrightarrow gxg^{-1} = y \Leftrightarrow y = g^{-1}xg \in G$.

**Dạng toán 9.** Xác định Im($f$) và ker($f$) của đồng cấu nhóm $f: G \to G'$.
**Cách giải:** Dùng định nghĩa:

1) $\text{Im}(f) = \{f(x) | x \in G\}$ hay $\text{Im}(f) = \{y \in G' | \exists x \in G, f(x) = y\}$.
2) $\ker(f) = \{x \in G | f(x) = e'\}$.

**Ví dụ.** Cho ánh xạ $f: \mathbf{Z} \to \mathbf{Z}$ định bởi $f(x) = nx$ với mọi $x \in \mathbf{Z}$, trong đó $n \in \mathbf{N}^*$ cho trước. Chứng minh rằng $f$ là một đồng cấu nhóm cộng. Tìm Im($f$) và ker($f$).
**Lời giải.** $f$ là một đồng cấu nhóm cộng vì

$$\forall x, y \in \mathbf{Z}, f(x+y) = n(x+y) = nx + ny = f(x) + f(y).$$

Ta có

$$\text{Im}(f) = \{f(x) | x \in \mathbf{Z}\} = \{nx | x \in \mathbf{Z}\} = n\mathbf{Z},$$
$$\ker(f) = \{x \in \mathbf{Z} | f(x) = 0\} = \{x \in \mathbf{Z} | nx = 0\} = \{x \in \mathbf{Z} | x = 0\} = \{0\}.$$

**Dạng toán 10.** Chứng minh sự đẳng cấu giữa các nhóm
**Cách giải 1**: Để chứng minh $G \simeq G'$ ta xây dựng một đẳng cấu $f$ từ $G$ vào $G'$ (xem Bài toán 8).
**Cách giải 2**: Để chứng minh $G/H \simeq G'$ ta sử dụng Định lý đẳng cấu 1 bằng cách xây dựng một toàn cấu $f$ từ $G$ vào $G'$ (xem Dạng toán 8) sao cho $\ker(f) = H$.

**Ví dụ.** Chứng minh rằng

a) $GL(n, \mathbb{R}) / SL(n, \mathbb{R}) \simeq \mathbb{R}^*$.
b) Nhóm thương $\mathbb{R} / \mathbb{Z}$ đẳng cấu với nhóm nhân $T$ các số phức có môđun bằng 1.

**Lời giải**. a) Xét qui tắc $f: GL(n, \mathbb{R}) \to \mathbb{R}^*$ định bởi $f(A) = \det(A)$. Ta có

- $f$ là một ánh xạ vì $\forall A \in GL(n, \mathbb{R}), f(A) = \det(A) \in \mathbb{R}^*$ ($\det(A) \neq 0$ do A khả nghịch).
- $f$ là một đồng cấu vì
  $\forall A, B \in GL(n, \mathbb{R}), f(AB) = \det(AB) = \det(A)\det(B) = f(A)f(B)$.
- $f$ là một toàn ánh vì
  $$\forall \alpha \in \mathbb{R}^*, \exists D_1(\alpha) \in GL(n, \mathbb{R}), f(D_1(\alpha)) = \det D_1(\alpha) = \alpha,$$

trong đó $D_1(\alpha)$ là ma trận chéo cấp $n$ có các hệ số trên đường chéo lần lượt là α, 1,…, 1.

- $\ker(f) = \{A \in GL(n, \mathbb{R}) \mid \det(A) = 1\} = SL(n, \mathbb{R})$.

Từ đây, theo Định lý đẳng cấu 1 ta có $GL(n, \mathbb{R}) / SL(n, \mathbb{R}) \simeq \mathbb{R}^*$.

b) Xét qui tắc $f: \mathbb{R} \to \mathbb{C}^*$ định bởi $f(x) = \cos 2\pi x + i \sin 2\pi x$. Ta có

- $f$ là một ánh xạ vì
  $\forall x \in \mathbb{Z}, f(x) = \cos 2\pi x + i \sin 2\pi x \in \mathbb{C}^*$ ($f(x) \neq 0$ do $|f(x)| = 1$).
- $f$ là một đồng cấu vì
  $$\forall x, y \in \mathbb{Z}, f(x+y) = \cos 2\pi(x+y) + i \sin 2\pi(x+y)$$
  $$= (\cos 2\pi x + i \sin 2\pi x)(\cos 2\pi y + i \sin 2\pi y).$$
  $$= f(x)f(y).$$

- $\mathrm{Im}(f) = \{f(x) \mid x \in \mathbb{R}\} = \{\cos 2\pi x + i \sin 2\pi x \mid x \in \mathbb{R}\}$
  $= \{\cos y + i \sin y \mid y \in \mathbb{R}\} = \{z \in \mathbb{C} \mid |z| = 1\} = T.$

- $\ker(f) = \{x \in \mathbb{R} \mid f(x) = 1\} = \{x \in \mathbb{R} \mid \cos 2\pi x + i \sin 2\pi x = 1\}$
  $= \{x \in \mathbb{R} \mid \cos 2\pi x = 1, \sin 2\pi x = 0\} = \{x \in \mathbb{R} \mid \exists k \in \mathbb{Z}, 2\pi x = 2k\pi\} = \mathbb{Z}.$

Từ đây, theo Định lý đẳng cấu 1 ta có $\mathbb{R}) / \mathbb{Z} \simeq T$.

## B. LỜI GIẢI BÀI TẬP VỀ NHÓM

**Bài 1.1.** a) Xem Ví dụ 1trong Dạng toán 1 và Ví dụ trong Dạng toán 5.

**b)** $G = \mathbb{R}^+ \setminus \{1\}, x * y = x^{\ln y}$.

Ta thấy $*$ là một phép toán trên G vì

$$\forall x, y \in G = \mathbb{R}^+ \setminus \{1\},\ x * y = x^{\ln y} = e^{\ln(x^{\ln y})} = e^{\ln x \ln y} \in G.$$

- Tính giao hoán:
$$\forall x, y \in G,\ x * y = x^{\ln y} = y^{\ln x} = y * x.$$
- Tính kết hợp:
$$\forall x, y, z \in G, (x * y) * z = (e^{\ln x \ln y}) * z = e^{\ln(e^{\ln x \ln y}) \ln z} = e^{\ln x \ln y \ln z}$$
$$= x^{\ln x \ln(e^{\ln y \ln z})} = e^{\ln x \ln(y * z)} = x * (y * z).$$
- (G,∗) có phần tử trung hòa là e (cơ số của logarit Nêpe) vì với a ∈ G ta có
$$\forall x \in G, x * a = x \Leftrightarrow \forall x \in G, x^{\ln a} = x \Leftrightarrow \ln a = 1 \Leftrightarrow a = e \in G.$$
- Mọi phần tử x ∈ G có phần tử đối xứng là $e^{1/\ln x}$ vì với y ∈ G ta có

$$x * y = e \Leftrightarrow e^{\ln x \ln y} = e \Leftrightarrow \ln x \ln y = 1$$
$$\Leftrightarrow \ln y = \frac{1}{\ln x} \Leftrightarrow y = e^{1/\ln x} \in G.$$

Suy ra $(G,*)$ là một nhóm giao hoán.

- Với x ∈ G và n ≥ 1, bằng qui nạp ta chứng minh được rằng
$$\underbrace{x * \ldots * x}_{n} = e^{(\ln x)^n}.$$

Do đó với x ∈ G ta có

$$o(x) < \infty \Leftrightarrow \exists n \geq 1, \underbrace{x * \ldots * x}_{n} = e \Leftrightarrow \exists n \geq 1,\ e^{(\ln x)^n} = e$$
$$\Leftrightarrow \exists n \geq 1,\ (\ln x)^n = 1 \Leftrightarrow \left[\begin{array}{l} \ln x = 1 \\ \ln x = -1 \end{array}\right. \Leftrightarrow \left[\begin{array}{l} x = e \in G \\ x = \frac{1}{e} \in G. \end{array}\right.$$

Vậy trong G chỉ có hai phần tử có cấp hữu hạn là $x_1 = e, x_2 = \frac{1}{e}$.

**c)** $G=\mathbb{R}, x*y=\sqrt[n]{x^n+y^n}$, n là số nguyên dương lẻ.

Ta thấy $*$ là một phép toán trên G vì

$$\forall x,y\in G=\mathbb{R}, x*y=\sqrt[n]{x^n+y^n}\in G.$$

- Tính giao hoán:

$$\forall x,y\in G=\mathbb{R}, x*y=\sqrt[n]{x^n+y^n}=\sqrt[n]{y^n+x^n}=y*x.$$

- Tính kết hợp:

$$\forall x,y,z\in G,(x*y)*z=\sqrt[n]{x^n+y^n}*z=\sqrt[n]{\left(\sqrt[n]{x^n+y^n}\right)^n+z^n}=\sqrt[n]{x^n+y^n+z^n}$$

$$=\sqrt[n]{x^n+\left(\sqrt[n]{y^n+z^n}\right)^n}=x*\sqrt[n]{y^n+z^n}=x*(y*z).$$

- (G,$*$) có phần tử trung hòa là 0 vì với a $\in$ G ta có

$$\forall x\in G, x*a=x\Leftrightarrow\forall x\in G,\sqrt[n]{x^n+a^n}=x\Leftrightarrow\forall x\in G, x^n+a^n=x^n\Leftrightarrow a=0\in G.$$

- Mọi phần tử x $\in$ G có phần tử đối xứng là $-$x $\in$ G vì với y $\in$ G ta có

$$x*y=0\Leftrightarrow\sqrt[n]{x^n+y^n}=0\Leftrightarrow x^n+y^n=0\Leftrightarrow x^n=y^n\Leftrightarrow y=-x\in G.$$

Suy ra $(G,*)$ là một nhóm giao hoán.

- Với x $\in$ G và m $\geq$ 1, bằng qui nạp ta chứng minh được rằng

$$\underbrace{x*\ldots*x}_{m}=\sqrt[n]{mx^n}$$

Do đó với x $\in$ G ta có

$$o(x)<\infty\Leftrightarrow\exists m\geq 1,\underbrace{x*\ldots*x}_{m}=0\Leftrightarrow\exists m\geq 1,\sqrt[n]{mx^n}=0\Leftrightarrow x=0\in G.$$

Vậy trong G chỉ có một phần tử có cấp hữu hạn là 0.

**d)** $G=\mathbb{R}, x*y=\left(\sqrt[n]{x}+\sqrt[n]{y}\right)^n$, n là số nguyên dương lẻ.

Tương tự câu c) ta có $(G,*)$ là một nhóm giao hoán, trong đó

- phần tử trung hòa là 0;
- Mọi phần tử x $\in$ G có phần tử đối xứng là $-$ x $\in$ G.

Với x $\in$ G và m $\geq$ 1, bằng qui nạp ta có

$$\underbrace{x*\ldots*x}_{m}=\left(m\sqrt[n]{x}\right)^n$$

và trong G chỉ có một phần tử có cấp hữu hạn là 0.

**e)** $G=\mathbb{R}^+, x*y=\ln(e^x+e^y-1)$.

Ta thấy $*$ là một phép toán trên G vì

$\forall x,y\in G=\mathbb{R}^+, x*y=\ln(e^x+e^y-1)\in G$ do $\ln(e^x+e^y-1)>\ln(e^x)=x>0$.

- Tính giao hoán:

$$\forall x, y \in G, x * y = \ln(e^x + e^y - 1) = \ln(e^y + e^x - 1) = y * x.$$

- Tính kết hợp:

$\forall x, y, z \in G,$

$$(x * y) * z = \ln(e^x + e^y - 1) * z = \ln\left(e^{\ln(e^x + e^y - 1)} + e^z - 1\right) = \ln(e^x + e^y + e^z - 2)$$

$$= \ln\left(e^x + e^{\ln(e^y + e^z - 1)} - 1\right) = \ln\left(e^x + e^{y*z} - 1\right) = x * (y * z).$$

- (G,∗) không có phần tử trung hòa vì với mọi số thực a ta có

$$\forall x \in G, x * a = x \Leftrightarrow \forall x \in G, \ln(e^x + e^a - 1) = x \Leftrightarrow \forall x \in G, e^x + e^a - 1 = e^x \Leftrightarrow a = 0 \notin G.$$

Vậy $(G,*)$ là một nửa nhóm giao hoán nhưng không là vị nhóm.

f) $G = \mathbb{R} \times \mathbb{R}^*, (x, y) * (z, t) = (x + yz, yt).$

Ta thấy $*$ là một phép toán trên G vì

$$\forall (x, y), (z, t) \in G = \mathbb{R} \times \mathbb{R}^*, (x, y) * (z, t) = (x + yz, yt) \in G \text{ do } yt \neq 0.$$

- Không có tính giao hoán:

$$\exists \alpha = (0,2), \beta = (1,1) \in G, \alpha * \beta = (0,2) * (1,1) = (0 + 2.1, 2.1) = (2,2)$$

$$\neq (1,2) = (1 + 1.0, 1.2) = (1,1) * (0,2) = \beta * \alpha.$$

- Tính kết hợp:

$$\forall (x, y), (z, t), (u, v) \in G, ((x, y) * (z, t)) * (u, v) = (x + yz, yt) * (u, v) = (x + yz + ytu, ytv)$$

$$= (x, y) * (z + tu, tv) = (x, y) * ((z, t) * (u, v))$$

- (G,∗) có phần tử trung hòa phải là (0,1) vì với (a,b) ∈ G ta có

$$\forall (x, y) \in G, (x, y) * (a, b) = (x, y) \Leftrightarrow \forall (x, y) \in G, (x + ya, yb) = (x, y)$$

$$\Leftrightarrow \begin{cases} \forall x \in \mathbb{R}, x + ya = x \\ \forall y \in \mathbb{R}^*, yb = y \end{cases} \Leftrightarrow (a, b) = (0,1),$$

- Mọi phần tử (x, y) ∈ G có phần tử đối xứng phải là $(-\frac{x}{y}, \frac{1}{y}) \in G$ vì với (z, t) ∈ G ta có

$$(x, y) * (z, t) = (0,1) \Leftrightarrow (x + yz, yt) = (0,1) \Leftrightarrow \begin{cases} x + yz = 0 \\ yt = 1 \end{cases}$$

$$\Leftrightarrow \begin{cases} z = -\frac{x}{y} \\ t = \frac{1}{y} \end{cases} \Leftrightarrow (z, t) = (-\frac{x}{y}, \frac{1}{y}) \in G.$$

Suy ra $(G,*)$ là một nhóm không giao hoán.

- Với (x, y) ∈ G và n ≥ 1, bằng qui nạp ta chứng minh được rằng

$$\underbrace{(x, y) * \ldots * (x, y)}_{n} = (x + xy + \ldots + xy^{n-1}, y^n)$$

Do đó với (x, y) ∈ G ta có

$$o(x,y)<\infty \Leftrightarrow \exists n\geq 1, \underbrace{(x,y)*\ldots*(x,y)}_{n}=(0,1) \Leftrightarrow \exists n\geq 1,(x+xy+\ldots+xy^{n-1},y^n)=(0,1)$$

$$\Leftrightarrow \exists n\geq 1,\begin{cases} x+xy+\ldots+xy^{n-1}=0 \\ y^n=1 \end{cases} \Leftrightarrow \left[\begin{array}{l} y=1, x=0, \\ y=-1, x\in\mathbb{R}. \end{array}\right.$$

Vậy trong G các phần tử có cấp hữu hạn là: (0,1) và (x,–1) với $x\in\mathbb{R}$.

g) Xem Dạng toán 1, Ví dụ 1.

h) $G=\mathbb{R}^2\setminus\{(0,0)\}, (x,y)*(z,t)=(xz-yt,xt+yz).$

Ta thấy $*$ là một phép toán trên G vì

$\forall (x,y),(z,t)\in G=\mathbb{R}\times\mathbb{R}^*, (x,y)*(z,t)=(xz-yt,xt+yz)\in G.$

Thật vậy, nếu $(xz-yt,xt+yz)\notin G$ thì $(xz-yt,xt+yz)=(0,0)$, dẫn đến

$$\begin{cases} xz-yt=0 \\ xt+yz=0 \end{cases} \Rightarrow \begin{cases} x(z^2+t^2)=0 \\ y(z^2+t^2)=0 \end{cases} \Rightarrow (x,y)=(0,0)\notin G,$$

và ta có mâu thuẫn.

- Tính giao hoán:

$\forall (x,y),(z,t)\in G,\ (x,y)*(z,t)=(xz-yt,xt+yz)=(zx-ty,zy+tx)=(z,t)*(x,y).$

- Tính kết hợp:

$\forall (x,y),(z,t),(u,v)\in G,$

$$\begin{aligned}((x,y)*(z,t))*(u,v)=(xz-yt,xt+yz)*(u,v)&=((xz-yt)u-(xt+yz)v,(xz-yt)v+(xt+yz)u)\\ &=(x(zu-tv)-y(zv+tu),x(zv+tu)+y(zu-tv))\\ &=(x,y)*(zu-tv,zv+tu)=(x,y)*((z,t)*(u,v)).\end{aligned}$$

- (G,∗) có phần tử trung hòa là (1, 0) vì

$$\forall (x,y)\in G,(x,y)*(a,b)=(x,y)\Leftrightarrow \forall (x,y)\in G,(xa-yb,xb+ya)=(x,y)$$

$$\Leftrightarrow \forall (x,y)\in G,\begin{cases} xa-yb=x \\ xb+ya=y \end{cases} \Leftrightarrow (a,b)=(1,0)\in G.$$

- Mọi phần tử (x, y) ∈ G có phần tử đối xứng là $\left(\frac{x}{x^2+y^2},-\frac{y}{x^2+y^2}\right)\in G$ vì với (z, t) ∈ G ta có

$$(x,y)*(z,t)=(1,0)\Leftrightarrow (xz-yt,xt+yz)=(1,0)\Leftrightarrow \begin{cases} xz-yt=1 \\ xt+yz=0 \end{cases}$$

$$\Leftrightarrow \begin{cases} z=\dfrac{x}{x^2+y^2} \\ t=-\dfrac{y}{x^2+y^2} \end{cases} \Leftrightarrow (z,t)=\left(\frac{x}{x^2+y^2},-\frac{y}{x^2+y^2}\right)\in G.$$

Suy ra $(G,*)$ là một nhóm giao hoán.

- Với (x, y) ∈ G và n ≥ 1, bằng qui nạp ta chứng minh được rằng

$$\underbrace{(x,y)*\ldots*(x,y)}_{n}=(x_n,y_n),$$

trong đó $x_n$ và $y_n$ lần lượt là các phần thực và phần ảo của số phức $(x + iy)^n$. Do đó với (x, y) ∈ G ta có

$$o(x,y)<\infty \Leftrightarrow \exists n\geq 1, \underbrace{(x,y)*\ldots*(x,y)}_{n}=(1,0)\Leftrightarrow \exists n\geq 1,(x+iy)^n=1.$$

Vậy trong G các phần tử có cấp hữu hạn là:

$$\{(x, y) \in G| \exists n \in \mathbf{N}^*,\ (x + iy)^n = 1\},$$

đó chính là tập hợp tất cả các phần tử (x, y) ∈ G sao cho số phức x + iy là một căn bậc n nào đó của 1.

**Bài 1.2.** a) Xem Ví dụ 2 trong Dạng toán 1,.

b) Cho (G,.) là một nhóm và H là một tập con khác rỗng, hữu hạn, kín đối với phép toán nhân. Ta chứng minh H là một nhóm con của G. Thật vậy, hiển nhiên (H,.) là một nửa nhóm hữu hạn, khác rỗng của G, hơn nữa, phép toán nhân có tính giản ước trong H (vì phép toán nhân có tính giản ước trong nhóm G). Do đó theo Câu a, H là một nhóm con của G.

**Bài 1.3.** Với (X,.) là một nửa nhóm khác rỗng và a ∈ X,

$$aX = \{ax| x \in X\};\ Xa = \{xa| x \in X\}.$$

Ta chứng minh

$$(X,.) \text{ là nhóm} \Leftrightarrow \forall a \in X,\ aX = Xa = X.$$

(⇒) Xét ánh xạ $\varphi : G \to G, \varphi(x) = ax$. Ta chứng minh φ là song ánh. Thật vậy, hiển nhiên, φ được xác định, hơn nữa,

$$\forall y \in X, \varphi(x) = y \Leftrightarrow ax = y \Leftrightarrow x = a^{-1}y \in X.$$

Vậy φ là song ánh, và do đó $\varphi(X) = X$, nghĩa là $aX = X$. Tương tự, $Xa = X$.

(⇐) Với mọi a, b ∈ X, từ đẳng thức aX = X, ta suy ra phương trình ax = b có nghiệm trong X. Tương tự, từ đẳng thức Xa = X, ta suy ra phương trình ya = b có nghiệm trong X. Theo Định lý 3.5, (X,.) là nhóm.

**Bài 1.4.** Xét (G,∗) với $\forall x, y \in G, x * y = xay$, ta có,

- Tính kết hợp:
  $\forall x, y, z \in G, (x * y) * z = (xay) * z = (xay)az = xa(yaz) = xa(y * z) = x * (y * z).$
- (G,∗) có phần tử trung hòa phải là $a^{-1}$ vì
  $$\forall x \in G, x * a^{-1} = xaa^{-1} = x.$$
- Mọi phần tử x ∈ G có phần tử đối xứng phải là $x' = (axa)^{-1} \in G$ vì
  $$\forall x \in G, x * x' = xa(axa)^{-1} = a^{-1}(axa)(axa)^{-1} = a^{-1}.$$
  Theo Định lý 3.5, (G,∗) là một nhóm.

**Bài 1.5.** Xét phần tử $y = xax^{-1} \in G$ . Ta có

1) $y^2 = (xax^{-1})(xax^{-1}) = xa^2x^{-1} = xex^{-1} = e.$
2) $y \neq e$ vì nếu $y = e$ thì $xax^{-1} = e$, dẫn đến $a = x^{-1}x = e$, mâu thuẫn.

Vậy y có cấp 2. Do tính duy nhất của a, ta có y = a. Từ đó ax = xa.

**Bài 1.6.** Từ giả thiết ta suy ra với mọi z ∈ G, $z^2$ = e nên z = $z^{-1}$. Xét x, y∈ G bất kỳ, ta có

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

Suy ra G giao hoán.

**Bài 1.7.** a) Quan hệ ~ định bởi:

$$\forall x, y \in G, x \sim y \Leftrightarrow \exists a \in G, x = a^{-1}ya$$

là một quan hệ tương đương trên G vì:

1) Tính phản xạ: $\forall x \in G, x \sim x$ vì $\exists a = e \in G,\ e^{-1}xe = exe = x.$
2) Tính đối xứng:

$$\forall x, y \in G, x \sim y \Rightarrow \exists a \in G, x = a^{-1}ya$$
$$\Rightarrow \exists b = a^{-1} \in G, y = b^{-1}xb \Rightarrow\ y \sim x.$$

3) Tính bắc cầu:

$$\forall x, y, z \in G, \begin{cases} x \sim y \\ y \sim z \end{cases} \Rightarrow \begin{cases} \exists a \in G, x = a^{-1}ya \\ \exists b \in G, y = b^{-1}zb \end{cases}$$
$$\Rightarrow \exists c = ba \in G, x = a^{-1}(b^{-1}zb)a = c^{-1}zc \Rightarrow\ x \sim z.$$

b) (⇐): Nếu G giao hoán thì quan hệ ~ chính là quan hệ = nên hiển nhiên đây là một quan hệ thứ tự trên G.

(⇒) Giả sử ~ là một quan hệ thứ tự trên G. Khi đó theo Câu a, ~ vừa là một quan hệ thứ tự, vừa là một quan hệ tương trên G. Do đó, nếu x ~ y thì x = y. Với mọi x, y ∈G, xét phần tử z = $x^{-1}$yx, ta thấy ngay z ~ y, do đó theo lý luận trên z = y, từ đó xy = yx. Vậy G giao hoán.

**Bài 1.8.** Gọi n là số nguyên sao cho với mọi x, y ∈ G, ta có

$$\begin{cases} (xy)^n = x^n y^n & (1) \\ (xy)^{n+1} = x^{n+1} y^{n+1} & (2) \\ (xy)^{n+2} = x^{n+2} y^{n+2} & (3) \end{cases}$$

Khi đó

- Từ (1) và (2) ta suy ra $(x^n y^n)(xy) = x^{n+1}y^{n+1}$ nên $y^n x = xy^n$. (4)
- Tương tự, từ (2) và (3) ta suy ra $y^{n+1}x = xy^{n+1}$. (5)

Từ (4) và (5) ta có

$$(xy)y^n = xy^{n+1} = y^{n+1}x = y(y^n x) = y(xy^n) = (yx)y^n,$$

do đó xy = yx. Suy ra G giao hoán.

**Bài 1.9.** Xét ánh xạ $\varphi : G \to G, \varphi(x) = x^{-1}$. Ta thấy φ là song ánh vì

$$\forall y \in X, \varphi(x) = y \Leftrightarrow x^{-1} = y \Leftrightarrow x = y^{-1} \in X.$$

Do đó $\varphi(G) = G$, nghĩa là $\{x_1, ..., x_n\} = \{x_1^{-1}, ..., x_n^{-1}\}$. Từ đây, do tính giao hoán ta có

$$x_1...x_n = x_1^{-1}...x_n^{-1} = (x_1...x_n)^{-1}.$$

Suy ra $(x_1...x_n)^2 = e$.

**Bài 1.10.** Cho σ là một hoán vị có cấp 2k + 1. Khi đó $\sigma^{2k+1} = Id$ nên $sgn(\sigma^{2k+1}) = 1$. Suy ra $(sgn(\sigma))^{2k+1} = 1$. Từ đó $sgn(\sigma) = 1$, nghĩa là σ là một hoán vị chẵn.
**Chiều đảo không đúng**: Trong nhóm hoán vị $S_7$, xét $\sigma = (1\ \ 2)(3\ \ 4)(5\ \ 6\ \ 7)$. Dễ thấy σ là một hoán vị chẵn và σ có cấp 6 cũng là một số chẵn.

**Bài 1.11.** a)

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 5 & 7 & 6 & 1 & 8 & 4 & 10 & 9 \end{pmatrix}$$
$$= (1\ \ 2\ \ 3\ \ 5\ \ 6)(4\ \ 7\ \ 8)(9\ \ 10)$$
$$= (1\ \ 6)(1\ \ 5)(1\ \ 3)(1\ \ 2)(4\ \ 8)(4\ \ 7)(9\ \ 10),$$
$$\sigma_2 = (1\ \ 3\ \ 4\ \ 7)(2\ \ 5)(1\ \ 2\ \ 4\ \ 3)$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 7 & 3 & 4 & 2 & 6 & 1 & 8 & 9 & 10 \end{pmatrix} = (1\ \ 5\ \ 2\ \ 7)$$
$$= (1\ \ 7)(1\ \ 2)(1\ \ 5).$$

Suy ra $\sigma_1, \sigma_2$ đều là các hoán vì lẻ, $o(\sigma_1) = BCNN(5, 3, 2) = 30$, $o(\sigma_2) = 4$.
b)

$$\sigma_1\sigma_2 = (1\ \ 2\ \ 3\ \ 5\ \ 6)(4\ \ 7\ \ 8)(9\ \ 10)(1\ \ 5\ \ 2\ \ 7)$$
$$= (1\ \ 6)(2\ \ 8\ \ 4\ \ 7)(3\ \ 5)(9\ \ 10)$$
$$= (1\ \ 6)(2\ \ 7)(2\ \ 4)(2\ \ 8)(3\ \ 5)(9\ \ 10),$$
$$\sigma_2^2 = (1\ \ 5\ \ 2\ \ 7)^2 = (1\ \ 2)(5\ \ 7),$$
$$\sigma_2^{-1} = (7\ \ 2\ \ 5\ \ 1) = (1\ \ 5)(1\ \ 2)(1\ \ 7),$$
$$\sigma_2^{-2} = (1\ \ 2)(5\ \ 7),$$
$$\sigma_1^2\sigma_2 = (1\ \ 2\ \ 3\ \ 5\ \ 6)^2(4\ \ 7\ \ 8)^2(9\ \ 10)^2(1\ \ 5\ \ 2\ \ 7)$$
$$= (1\ \ 3\ \ 6\ \ 2\ \ 5)(4\ \ 8\ \ 7)(1\ \ 5\ \ 2\ \ 7) = (2\ \ 4\ \ 8\ \ 7\ \ 3\ \ 6)$$
$$= (2\ \ 6)(2\ \ 3)(2\ \ 7)(2\ \ 8)(2\ \ 4),$$
$$\sigma_1\sigma_2^2 = (1\ \ 2\ \ 3\ \ 5\ \ 6)(4\ \ 7\ \ 8)(9\ \ 10)(1\ \ 2)(5\ \ 7)$$
$$= (1\ \ 3\ \ 5\ \ 8\ \ 4\ \ 7\ \ 6)(9\ \ 10)$$
$$= (1\ \ 6)(1\ \ 7)(1\ \ 4)(1\ \ 8)(1\ \ 5)(1\ \ 3)(9\ \ 10).$$

Suy ra
- $\sigma_1\sigma_2$, $\sigma_2^2$, $\sigma_2^{-2}$ là các hoán vị chẵn, $o(\sigma_1\sigma_2) = 4$, $o(\sigma_2^2) = 2$, $o(\sigma_2^{-2}) = 2$;
- $\sigma_2^{-1}$, $\sigma_1^2\sigma_2$, $\sigma_1\sigma_2^2$ là các hoán vị lẻ và $o(\sigma_2^{-1}) = 4$, $o(\sigma_1^2\sigma_2) = 6$, $o(\sigma_1\sigma_2^2) = 14$.

c) Tìm $\sigma \in S_n$ thoả $\sigma_1\sigma\sigma_2^{-2} = \sigma_1^{\,3}$.

$$\sigma_1\sigma\sigma_2^{-2} = \sigma_1^3 \Leftrightarrow \sigma = \sigma_1^2\sigma_2^2 = (\sigma_1^2\sigma_2)\sigma_2 = (2\ \ 4\ \ 8\ \ 7\ \ 3\ \ 6)(1\ \ 5\ \ 2\ \ 7)$$
$$= (1\ \ 5\ \ 4\ \ 8\ \ 7)(2\ \ 3\ \ 6).$$

**Bài 1.12**. Suy từ tính chất: Trong nhóm hoán vị $S_n$, các chu trình rời nhau thì giao hoán lẫn nhau.

**Bài 1.13**. Trong nhóm hoán vị $S_4$, xét chu trình $\sigma = (1\ \ 2\ \ 3\ \ 4)$, ta có $\sigma^2 = (1\ \ 3)(2\ \ 4)$ không là chu trình.

**Bài 1.14**. ($\Leftarrow$) Giả sử (m, k) = 1. Khi đó tồn tại các số nguyên a, b sao cho ma + kb = 1. Suy ra

$$\sigma = \sigma^{ma + kb} = \sigma^{ma}\sigma^{kb} = (\sigma^m)^a. \qquad (1)$$

Vì $\sigma$ là một k-chu trình nên nếu $\sigma^m$ không là k-chu trình thì phải có dạng tích của các chu trình rời nhau có chiều dài nhỏ hơn k, từ đó $(\sigma^m)^a$ cũng có dạng đó, mẫu thuẫn với (1).

($\Rightarrow$) Giả sử $\sigma^m$ là một k-chu trình. Khi đó $\sigma^m$ có cấp k. Đặt (m, k) = d . Ta có

$$(\sigma^m)^{k/d} = (\sigma^k)^{m/d} = Id.$$

Do đó k/d là bội số của k. Suy ra d = 1, nghĩa là m và k nguyên tố cùng nhau.

**Bài 1.15**. a) $H = \left\{ \begin{pmatrix} x & y \\ 2y & x \end{pmatrix} : x, y \in \mathbb{Q} \right\} \leq (M(2,\mathbb{Q}), +)$ vì:

- $H \subset M(2,\mathbb{Q})$.
- $0 = \begin{pmatrix} x & y \\ 2y & x \end{pmatrix} \in H$.
- 
- $\forall A = \begin{pmatrix} x & y \\ 2y & x \end{pmatrix}, B = \begin{pmatrix} z & t \\ 2t & z \end{pmatrix} \in H, A - B = \begin{pmatrix} x - z & y - t \\ 2(y - t) & x - z \end{pmatrix} \in H$

b) Xem Ví dụ trong dạng toán 2.

c) Ta có $U = \left\{ z \in \mathbb{C} \mid \exists k \in \mathbb{N}^*, z^k = 1 \right\} \leq (\mathbb{C}^*, .)$ vì

- $U \subset \mathbb{C}^*$ do $\forall z \in U, z \neq 0$.
- $1 \in H$ do $1 \in \mathbb{C}, 1^2 = 1$.
- $\forall z \in H, \exists k \in \mathbb{N}^*, z^k = 1$. Khi đó $(z^{-1})^k = 1$ nên $z^{-1} \in H$.
- $\forall z, t \in H, \exists k, l \in \mathbb{N}^*, z^k = 1 = t^l$. Khi đó $(zt)^{kl} = (z^k)^l(t^l)^k = 1$ nên $zt \in H$.

Chứng minh tương tự, ta có

$$U_n = \left\{ z \in \mathbb{C} \mid z^n = 1 \right\} \leq (\mathbb{C}^*, .);$$
$$T = \left\{ z \in \mathbb{C} \mid |z| = 1 \right\} \leq (\mathbb{C}^*, .).$$

**Bài 1.16**. Trước hết ta nhận xét rằng với các số nguyên k, l ta có

$$k\mathbb{Z} \subset l\mathbb{Z} \Leftrightarrow k \vdots l.$$

1) $m\mathbb{Z} \cap n\mathbb{Z} = [m,n]\mathbb{Z}$. Thật vậy,

$$k \in m\mathbb{Z} \cap n\mathbb{Z} \Leftrightarrow \begin{cases} k \in m\mathbb{Z} \\ k \in n\mathbb{Z} \end{cases} \Leftrightarrow \begin{cases} k \vdots m \\ k \vdots n \end{cases} \Leftrightarrow k \vdots [m,n] \Leftrightarrow k \in [m,n]\mathbb{Z}.$$

2) $m\mathbb{Z} + n\mathbb{Z} = (m,n)\mathbb{Z}$.

Theo nhận xét trên $m\mathbb{Z} \subseteq (m,n)\mathbb{Z}$ và $n\mathbb{Z} \subseteq (m,n)\mathbb{Z}$ nên $m\mathbb{Z} + n\mathbb{Z} \subseteq (m,n)\mathbb{Z}$.

Đảo lại, đặt (m,n) = d, khi đó tồn tại các số nguyên a, b sao cho ma + kb = d nên

$$(m,n)\mathbb{Z} = d\mathbb{Z} = (ma+nb)\mathbb{Z} \subset ma\mathbb{Z} + nb\mathbb{Z} \subset m\mathbb{Z} + n\mathbb{Z}.$$

Do đó $m\mathbb{Z} + n\mathbb{Z} = (m,n)\mathbb{Z}$.

**Bài 1.17.** Ta chứng minh các khẳng định sau tương đương:

a) xH là nhóm con của G $\Leftrightarrow$ c) $x \in H$.

a) $\Rightarrow$ c) Vì xH là nhóm con của G nên $e \in xH$, nghĩa là $\exists y \in H$, $e = xy$. Suy ra $x^{-1} = y \in H$. Từ đó $x = y^{-1} \in H$.

c) $\Rightarrow$ a) Vì H kín đối với phép nhân nên với $x \in H$, ta có $xH \subseteq H$, hơn nữa, do $x^{-1} \in H$ nên ta cũng có $x^{-1}H \subseteq H$ hay $H \subseteq xH$. Vậy xH = H, và do đó $xH \le G$.

Chứng minh tương tự ta được: b) Hx là nhóm con của G $\Leftrightarrow$ c) $x \in H$.

**Bài 1.18.** Với mỗi $x \in G$, đặt $H^x = x^{-1}Hx$. Ta chứng minh $H^x \le G$. Thật vậy,

- $e = x^{-1}ex \in H^x$.
- $\forall a, b \in H^x$, $\exists y, z \in H$, $a = x^{-1}yx$, $b = x^{-1}zx$,

$$a^{-1}b = (x^{-1}y^{-1}x)(x^{-1}zx) = x^{-1}(y^{-1}z)x \in H^x.$$

**Bài 1.19. a)** $C(G) \le C(a) \le G$: Hiển nhiên $C(G) \subseteq C(a)$. Do đó ta chỉ cần chứng minh $C(a) \le G$. Thật vậy,

- $e \in C(a)$ vì ae = ea = a.
- $\forall x, y \in C(a)$, $xy \in C(a)$ vì (xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy).
- $\forall x \in C(a)$, $x^{-1} \in C(a)$ vì từ ax = xa ta suy ra $x^{-1}a = ax^{-1}$.

**b)** $C(G) = \bigcap_{b \in G} C(b)$: Do Câu a, ta chỉ cần chứng minh $\bigcap_{b \in G} C(b) \subseteq C(G)$. Thật vậy, nếu $x \in \bigcap_{b \in G} C(b)$ thì $bx = xb, \forall b \in G$, nên $x \in C(G)$.

**c)** Cho H là một nhóm con của C(G). Khi đó H cũng là một nhóm con của G. Hơn nữa, do mọi phần tử của H giao hoán với mọi phần tử của G nên $\forall x \in G$, xH = Hx. Điều này chứng tỏ H là nhóm con chuẩn tắc của G.

d) Xét nhóm tuyến tính tổng quát $GL(n,\mathbb{R})$, ta có

$$C(GL(n,\mathbb{R})) = \left\{ \lambda I_n \mid \lambda \in \mathbb{R}^* \right\}.$$

Thật vậy, hiển nhiên các ma trận dạng $\lambda I_n$ với $\lambda \in \mathbb{R}^*$ đều thuộc $C(GL(n,\mathbb{R}))$. Đảo lại, cho $X = (x_{ij}) \in GL(n,\mathbb{R})$ tùy ý. Với mỗi $1 \le i \ne j \le n$, đặt $T_{ij} = I_n + E_{ij}$, trong đó

$E_{ij}$ là ma trận vuông cấp n có tất cả các hệ số là 0, trừ hệ số ở dòng i, cột j là 1. Hiển nhiên, $T_{ij} \in GL(n,\mathbb{R})$, do đó

$$XT_{ij} = XT_{ij} \Leftrightarrow X + XE_{ij} = X + E_{ij}X \Leftrightarrow XE_{ij} = E_{ij}X.$$

Từ đẳng thức sau cùng ta suy ra $x_{ii} = x_{jj}$ và $x_{ki} = 0$, $\forall 1 \le k \ne i \le n$. Từ đó X có dạng $\lambda I_n$ với $\lambda \in \mathbb{R}^*$.

**Bài 1.20.** Chứng minh

$$H \cup K \le G \Leftrightarrow H \subset K \text{ hay } K \subset H.$$

Chiều đảo là hiển nhiên. Ta chứng minh chiều thuận. Thật vậy, giả sử $H \cup K \le G$ và $H \not\subset K$. Khi đó $\exists h \in H \setminus K$. Với mọi $k \in K$, vì h, k đều thuộc $H \cup K$ nên theo tính chất của nhóm con ta có $hk \in H \cup K$, nghĩa là $hk \in H$ hay $hk \in K$. Đặt x = hk. Nếu $x \in K$ thì $h = xk^{-1} \in K$, mâu thuẫn. Vậy $x \in H$, do đó $k = h^{-1}x \in H$. Điều này chứng tỏ $K \subset H$.

**Bài 1.21**. a) Sử dụng tính kết hợp của phép nhân.
b) Sử dụng tính chất $(x^{-1})^{-1} = x$.
c) Sử dụng tính chất $(xy)^{-1} = y^{-1}x^{-1}$.
d) i) $\Rightarrow$ ii) Nếu $A \le G$ thì

$$AA = \{ab \mid a, b \in A\} \subset A = \{ae \mid a \in A\} \subset AA;$$

$$A^{-1} = \{a^{-1} \mid a \in A\} \subset A = \{(a^{-1})^{-1} \mid a \in A\} \subset A^{-1}$$

nên $AA = A$ và $A^{-1} = A$.
ii) $\Rightarrow$ iii): Hiển nhiên.
iii) $\Rightarrow$ i): Từ đẳng thức $A^{-1}A = A$ ta suy ra $\forall x, y \in A$, $x^{-1}y \in A$ do đó $A \le G$.
e) ($\Rightarrow$) Nếu $AB \le G$ thì theo Câu d và Câu c ta có $AB = (AB)^{-1} = B^{-1}A^{-1} = BA$.
($\Leftarrow$) Giả sử $AB = BA$. Theo Câu d ta có
$(AB)^{-1}AB = (B^{-1}A^{-1})AB = (BA)AB = [B(AA)]B = (BA)B = (AB)B = A(BB) = AB$.
và do đó $AB \le G$.

Khi đó, vì $A = \{ae \mid a \in A\} \subset AB; B = \{eb \mid b \in B\} \subset AB$ nên $A \vee B \subset AB$. Mặt khác, vì $A \subset A \vee B$ và $B \subset A \vee B$ nên $AB \subset A \vee B$. Do đó $AB = A \vee B$.

**Bài 1.22**. a) $H_n = \{x \in G \mid x^n \in H\} \le G$ vì

- $e \in H_n$ do $e^n = e \in H$.
- $\forall x, y \in H_n$, $x^{-1}y \in H_n$ do $(x^{-1}y)^n = (x^n)^{-1}y^n \in H$.

Hơn nữa, $H \subset H_n$ vì $\forall x \in H$, $x^n \in H$.
b) Nếu p|q thì $\forall x \in H_p$, $x^q = (x^p)^{q/p} \in H$ nên $H_p \subset H_q$. Từ kết quả này ta suy ra $H_d \subset H_m \cap H_n$. Đảo lại, vì d = rm + sn với $r, s \in \mathbb{Z}$ nên $\forall x \in H_m \cap H_n$,

$$x^d = x^{rm+sn} = (x^m)^r (x^n)^s \in H,$$

do đó $x \in H_d$. Điều này chứng tỏ $H_m \cap H_n \subset H_d$. Vậy $H_m \cap H_n = H_d$. Từ đó $H_m \cap H_n = H$ khi và chỉ khi $H_d = H$, nghĩa là trong nhóm thương G/H không có phần tử nào có cấp lớn hơn 1 và là ước số của d.

**Bài 1.23**. a) Vì G giao hoán nên mọi nhóm con của G đều chuẩn tắc. Do đó để chứng minh $K = \left\{x \in G \mid \exists n \in \mathbb{N}^*, x^n \in H\right\}$ là nhóm con chuẩn tắc của G ta chỉ cần chứng minh $K \le G$. Thật vậy,

- $e \in K$ do $e^1 = e \in H$.
- $\forall x, y \in K, x^{-1}y \in K$ do $\exists m, n \in \mathbb{N}^*, x^m, y^n \in H \Rightarrow (x^{-1}y)^{mn} = (x^m)^{-n}(y^n)^m \in H$

.

b) Giả sử $\bar{x} \in G/K$ có cấp m. Khi đó $\overline{x^m} = (\bar{x})^m = K$ nên $x^m \in K$. Suy ra $\exists n \in \mathbb{N}^*, (x^m)^n \in H$, nghĩa là $x^{mn} \in H$. Điều này chứng tỏ $x \in K$ hay $\bar{x} = K$, và do đó $\bar{x}$ có cấp 1.

**Bài 1.24**. Xét ánh xạ

$$\varphi : G/H \cap K \to G/H \times G/K,\ \varphi(x(H \cap K)) = (xH, xK) = (xH, xK)$$

Ta thấy φ là đơn ánh vì

$$\forall x, y \in G, \varphi(x(H \cap K)) = \varphi(y(H \cap K)) \Rightarrow (xH, xK) = (yH, yK) \Rightarrow \begin{cases} xH = yH \\ xK = yK \end{cases}$$

$$\Rightarrow x^{-1}y \in H \cap K \Rightarrow x(H \cap K) = y(H \cap K).$$

Do đó

$$|G/H \cap K| \le |G/H \times G/K| = |G/H| \times |G/K|.$$

Mà $|G/H| = [G:H] < \infty, |G/K| = [G:K] < \infty$ nên $|G/H \cap K| < \infty$. Do đó $H \cap K$ có chỉ số hữu hạn trong G.

**Bài 1.25**. Xét ánh xạ $\varphi : H \times K \to HK$ định bởi

$$\forall x \in H, y \in K,\ \varphi(x, y) = xy.$$

Ta có

$$\forall x_1, x_2 \in H, y_1, y_2 \in K, \varphi(x_1, y_1) = \varphi(x_2, y_2) \Leftrightarrow x_1y_1 = x_2y_2$$

$$\Leftrightarrow x_1^{-1}x_2 = y_1y_2^{-1} \in H \cap K$$

$$\Leftrightarrow \exists z \in H \cap K, (x_2, y_2) = (x_1z, z^{-1}y_1).$$

Cho $x \in H, y \in K$. Kết quả trên cho ta

$$\varphi^{-1}(xy) = \{(xz, z^{-1}y) \mid z \in H \cap K\}$$

nên ánh xạ $\psi : H \cap K \to \varphi^{-1}(xy)$ định bởi $\psi(z) = (xz, z^{-1}y)$, được xác định và là toàn ánh. Hơn nữa, ψ cũng là đơn ánh vì

$$\forall z, t \in H \cap K, \psi(z) = \psi(t) \Rightarrow (xz, z^{-1}y) = (xt, t^{-1}y)$$

$$\Rightarrow xz = xt$$

$$\Rightarrow z = t.$$

Vậy $\psi$ là song ánh và do đó $|\varphi^{-1}(xy)| = |H \cap K|$. Ta đã chứng minh

$$\forall t \in HK, |\varphi^{-1}(t)| = |H \cap K|.$$

Từ đây, do

$$H \times K = \bigcup_{t \in HK} \varphi^{-1}(t)$$

ta suy ra

$$|H||K| = |H \times K| = \sum_{t \in HK} |\varphi^{-1}(t)| = |HK||H \cap K|.$$

Do đó $|HK| = \dfrac{|H||K|}{|H \cap K|}$.

**Bài 1.26**. Xem Ví dụ trong Dạng toán 4.

**Bài 1.27**. a) Xét $\sigma \in S_9$ có cấp 20. Viết $\sigma$ dưới dạng tích các chu trình rời nhau từng đôi một $\sigma = \sigma_1 \ldots \sigma_r$, trong đó $\sigma_j$ có cấp $k_j$. Khi đó, theo Bài tập 1.26, bội số chung nhỏ nhất của $k_1, \ldots, k_r$ bằng 20. Vì $k_1 + \ldots + k_r \le 9$ nên ta phải có $r = 2$ và $\{k_1, k_2\} = \{4, 5\}$. Do đó $\sigma$ là tích của hai chu trình rời nhau gồm một chu trình chiều dài 4 và một chu trình chiều dài 5. Đảo lại, cũng theo Bài tập 1.26, các phép hoán vị có dạng như trên đều có cấp 20.

b) Giả sử trong $S_9$ tồn tại phần tử $\sigma$ có cấp 18. Viết $\sigma$ dưới dạng tích các chu trình rời nhau từng đôi một $\sigma = \sigma_1 \ldots \sigma_r$, trong đó $\sigma_j$ có cấp $k_j$. Lý luận tương tự Câu a, ta có bội số chung nhỏ nhất của $k_1, \ldots, k_r$ bằng $18 = 2.3^2$. Vì mỗi $k_j \le 9$ nên ta phải có $r = 1$ và $k_1 = 9$ và do đó $\sigma$ có cấp 9, mâu thuẫn..

**Bài 1.28**. Trước hết ta có nhận xét sau: "*Nếu G là một nhóm giao hoán hữu hạn thỏa tính chất mọi phần tử khác e trong G đều có cấp là số nguyên tố p cho trước thì G có cấp là một lũy thừa của p*". Thật vậy, hiển nhiên khẳng định trên đúng nếu $|G| = 1$. Xét $|G| > 1$. Chọn $a \in G \setminus \{e\}$ và đặt $H = \langle a \rangle$. Ta có H là một nhóm con chuẩn tắc của G và $|H| = p$. Xét nhóm thương G/H. Ta có $|G/H| = |G|/|H| < |G|$ và mọi phần tử khác H trong G/H đều có cấp p vì $\forall \bar{x} \in G/H, (\bar{x})^p = \overline{x^p} = \bar{e} = H$. Do đó theo giả thiết qui nạp $|G/H|$ là một lũy thừa của p. Từ đó $|G| = |G/H||H|$ cũng là một lũy thừa của p và khẳng định trên được chứng minh.

Ta có $1111 = 11.101$. Ta chứng minh mọi nhóm G giao hoán cấp 1111 đều cyclic. Thật vậy, giả sử G không cyclic. Khi đó một phần tử $x \in G \setminus \{e\}$ bất kỳ có cấp là 11 hoặc 101. Vì 1111 không là lũy thừa của 11, cũng không là lũy thừa của 101 nên từ nhận xét trên ta suy ra tồn tại các phần tử $a, b \in G$ sao cho a có cấp 11, b có cấp 101. Do 11 và 101 nguyên tố cùng nhau, phần tử ab có cấp là $11.101 = 1111$ (xem Bài 1.30), do đó $G = \langle ab \rangle$ và G cyclic, mâu thuẫn. Vậy G cyclic.

Trở lại bài toán đã cho, ta có $G = \langle \sigma \rangle$ với $\sigma$ có cấp 1111. Ta giải bài toán bằng phản chứng. Giả sử khẳng định trong bài toán là sai. Khi đó với mỗi $i \in \{1, \ldots, 999\}$, tồn tại $\varphi \in G$ sao cho $\varphi(i) \ne i$. Từ đây, vì $\varphi$ là một lũy thừa của $\sigma$, ta có $\sigma(i) \ne i$. Điều này chứng tỏ trong phân tích $\sigma$ dưới dạng tích các chu trình rời nhau từng đôi

một $\sigma = \sigma_1 \ldots \sigma_r$ với $\sigma_j$ có chiều dài $k_j$, ta có $k_1 + \ldots + k_r = 999$. Vì mỗi $k_j$ chỉ có thể là 11 hoặc 101 nên ta suy ra tồn tại các số nguyên dương s, t sao cho $11s + 101t = 999$, điều này mâu thuẫn vì dễ thấy phương trình trên không thể có nghiệm nguyên dương (s, t).

**Nhận xét.** Thật ra, nếu dùng Bổ đề Cauchy "*Cho G là một nhóm hữu hạn. Nếu p là một ước số nguyên tố của |G| thì trong G luôn luôn tồn tại một phần tử có cấp p*" (xem Giáo trình Đại số hiện đại) thì ta có thể chứng minh được các kết quả sau:

1) *Nếu G là một nhóm hữu hạn (không nhất thiết giao hoán) thỏa tính chất mọi phần tử khác e trong G đều có cấp là lũy thừa của một số nguyên tố p cho trước thì G có cấp là một lũy thừa của p.*

2) *Mọi nhóm hữu hạn (không nhất thiết giao hoán) cấp 1111 đều cyclic.*

**Bài 1.29**. Trong nhóm tuyến tính đầy đủ $GL(2,\mathbb{R})$ xét các phần tử a, b như sau:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, B = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}.$$

Ta thấy

1) A, B đều có cấp 2 vì chúng khác $I_2$ và $A^2 = B^2 = I_2$.

2) $C := AB = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$ có cấp vô hạn vì $\forall n \in \mathbb{N}^*, C^n = \begin{pmatrix} 1 & -2n \\ 0 & 1 \end{pmatrix} \neq I_2$.

**Bài 1.30**. a) Với n nguyên dương ta có

$$(ab)^n = e \Leftrightarrow a[(ba)^{n-1}b] = e \Leftrightarrow [(ba)^{n-1}b]a = e \Leftrightarrow (ba)^n = e.$$

Từ đây suy ra cấp của ab bằng cấp của ba.

b) Với n nguyên dương ta có

$$(a^{-1})^n = e \Leftrightarrow (a^n)^{-1} = e \Leftrightarrow a^n = e$$

Suy ra cấp của $a^{-1}$ bằng cấp của a.

c) Ta có

- $(ab)^{rs} = (a^r)^s(b^s)^r = e^s e^r = e$.
- Với mọi $k \in \mathbf{Z}$, giả sử $(ab)^k = e$. Khi đó $a^k b^k = e$ nên $a^k = b^{-k}$. Đặt $c = a^k = b^{-k}$.

Ta có $c^r = (a^r)^k = e$ nên c có cấp là ước số của r. Tương tự, c cũng có cấp là ước số của s. Suy ra cấp của c là ước số của (r, s) = 1, nghĩa là c có cấp 1. Vậy c = e. Suy ra $a^k = b^{-k} = e$, do đó k là bội số của r và s, từ đó k là bội số của rs (do r và s nguyên tố cùng nhau).

Suy ra ab có cấp rs.

d) Ta có

- $(ab)^{rs} = (a^r)^s(b^s)^r = e^s e^r = e$.
- Với mọi $k \in \mathbf{Z}$, giả sử $(ab)^k = e$. Khi đó $a^k b^k = e$ nên $a^k = b^{-k}$. Đặt $c = a^k = b^{-k}$.

Ta có $c \in < a > \cap < b > = \{e\}$ nên c = e, nghĩa là $a^k = b^{-k} = e$, do đó k là bội số của r và s, từ đó k là bội số của [r,s].

Suy ra ab có cấp [r,s].

**Bài 1.31**. 1) Chọn $x \in G \setminus \{e\}$. Ta có $< x >$ là nhóm con khác $\{e\}$ của G nên $G = < x >$.

2) Nếu $|G| = +\infty$ thì $G \simeq \mathbb{Z}$ và do đó G có vô số nhóm con, mâu thuẫn.

3) $|G| = o(x) = n \geq 2$. Nếu n không nguyên tố thì n có một ước số nguyên dương k thoả $1 < k < n$, đưa đến $< x^k >$ là một nhóm con thực sự khác {e} của G (do $1 < o(x^k) = n/k < n$, xem Bài 1.34), mâu thuẫn.

Vậy G là nhóm cyclic cấp nguyên tố.

**Bài 1.32**. Điều kiện đủ là hiển nhiên. Ta chứng minh điều kiện cần. Giả sử G vô hạn.

TH 1: Mọi phần tử của G đều có cấp hữu hạn.

Chọn $x_1 \in G$. Khi đó $<x_1>$ hữu hạn nên $< x_1 > \neq G$. Chọn $x_2 \in G\backslash\{x_1\}$, ta có $< x_1 > \neq < x_2 >$ và $< x_2 >$ cũng hữu hạn nên $< x_1 > \cup < x_2 > \neq G$. Chọn $x_3 \in G\backslash (< x_1 > \cup < x_2 >)$. Ta có $< x_3 >$ là nhóm con hữu hạn khác $< x_1 >$ và $< x_2 >$. Cứ tiếp tục như thế ta tìm được vô số các nhóm con của G, do đó G có vô số nhóm con.

TH 2: Tồn tại x thuộc G có cấp vô hạn.

Khi đó $< x >$ đẳng cấu với $\mathbb{Z}$ nên $< x >$ có vô số nhóm con. Suy ra G cũng có vô số nhóm con.

**Bài 1.33**. a) Cho nhóm cyclic $G = < a >$. Khi đó với mọi $x, y \in G$, tồn tại $m, n \in \mathbf{Z}$ sao cho $x = a^m$, $y = a^n$ nên $xy = a^m a^n = a^{m+n} = a^n a^m = yx$.

b) Suy từ Định lý 6.6.

c) Cho nhóm cyclic $G = < a >$ và đồng cấm nhóm $f: G \to G'$. Khi đó

$$f(G) = \{f(x) | x \in G\} = \{f(a^n) | n \in \mathbf{Z}\} = \{[f(a)]^n | n \in \mathbf{Z}\} = < f(a) >.$$

**Bài 1.34**. a) Với $d = (n, k)$, ta có $n = dr$, $k = ds$ với $(r, s) = 1$.

- $(x^k)^{n/d} = (x^n)^s = e^s = e$.
- Với mọi số nguyên dương m, giả sử $(x^k)^m = e$. Khi đó $x^{km} = e$ nên $n|km$, suy ra $r|sm$, từ đó $r|m$ (do $(r,s) = 1$), nghĩa là $(n/d)|m$.

Suy ra $x^k$ có cấp n/d.

b) $< x^k > = < x^l >$ khi và chỉ khi $(n, k) = (n, l)$.

($\Rightarrow$) Theo Câu a ta có

$$\frac{n}{(n,k)} = o(x^k) = |< x^k >| = |< x^l >| = o(x^l) = \frac{n}{(n,l)}.$$

Suy ra $(n, k) = (n, l)$.

($\Leftarrow$) Ta có $k \vdots (n,k)$ nên $< x^k > \subset < x^{(n,k)} >$. Mặt khác, theo Câu a, hai nhóm trên đều có cấp là $n/(n,k)$ nên $< x^k > = < x^{(n,k)} >$. Tương tự, $< x^l > = < x^{(n,l)} >$. Do đó từ giả thiết $(n, k) = (n, l)$ ta suy ra $< x^k > = < x^l >$.

c) Theo Câu b ta có $< x^k > = G = < x >$ khi và chỉ khi $(n, k) = (n,1) = 1$. Từ đó suy ra số phần tử sinh của G là $\varphi(n)$ với $\varphi$ là hàm Euler.

d) Từ Câu c ta suy ra tất cả các nhóm con của G là $< x^k >$ trong đó k là ước số của n..

**Bài 1.35**. ($\Rightarrow$) Giả sử $G_1 \times G_2 = <(x,y)>$. Khi đó $G_1 \times G_2 = \{(x^k, y^k) | k \in \mathbf{Z}\}$ nên

$$G_1 = \{x^k | k \in \mathbf{Z}\} = < x >;$$
$$G_2 = \{y^k | k \in \mathbf{Z}\} = < y >.$$

Vì mỗi nhóm $G_1, G_2$ đều có ít nhất 2 phần tử nên $x \neq e_1$, $y \neq e_2$. Ta chứng minh x, y có cấp hữu hạn và nguyên tố cùng nhau.

• Xét $(x, e_2) \in G_1 \times G_2$. Tồn tại số nguyên k sao cho $(x, e_2) = (x^k, y^k)$ hay $x^{k-1} = e_1$ và $y^k = e_2$. Nếu k = 0 thì $x = e_1$, mâu thuẫn. Nếu k = 1 thì $y = e_2$, mâu thuẫn. Vậy $k \neq 0$ và $k \neq 1$. Điều này chứng tỏ x, y đều có cấp hữu hạn.

• Đặt m = o(x), n = o(y). Khi đó $G_1$ có cấp m, $G_2$ có cấp n nên $G_1 \times G_2$ có cấp mn. Đặt $k = [m,n] \leq mn$. Ta có $(x,y)^k = (x^k,y^k) = (e_1,e_2)$ nên (x,y) có cấp là ước số của k. Suy ra $mn = |G_1 \times G_2| \leq k$. Từ đó [m,n] = k = mn, do đó m và n nguyên tố cùng nhau.

($\Leftarrow$) Giả sử $G_1 = < x >$, $G_2 = < y >$, trong đó $|G_1| = m$, $|G_2| = n$ và m, n nguyên tố cùng nhau. Ta chứng minh $G_1 \times G_2 = <(x,y)>$. Thật vậy, hiển nhiên $<(x,y)> \subset G_1 \times G_2$. Đảo lại, do m, n nguyên tố cùng nhau nên tồn tại các số nguyên r, s sao cho mr + ns = 1, do đó với mọi $(x^k,y^l) \in G_1 \times G_2$, ta có

$$(x, y)^{mrl + nsk} = (x^{mrl + nsk}, y^{mrl + nsk}) = (x^{nsk}, y^{mrl}) = (x^{mrk + nsk}, y^{mrl + nsl}) = (x^k, y^l).$$

suy ra $(x^k, y^l) \in < (x, y) >$. Điều này chứng tỏ $G_1 \times G_2 \subset <(x, y)>$. Do đó $G_1 \times G_2 = < (x, y) >$ là nhóm cyclic.

**Bài 1.36**. Xét nhóm hoán vị $S_4$, đặt K là nhóm K là nhóm Klein

$$K = \{Id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

và

$$H = < (1\ 2)(3\ 4) > = \{Id, (1\ 2)(3\ 4)\}.$$

Khi đó $K \lhd G$ (xem Bài 1.44) và hiển nhiên $H \lhd K$ (do K giao hoán), nhưng H không chuẩn tắc trong G vì

$$(1\ 2\ 3)(1\ 2)(3\ 4)\ (1\ 2\ 3)^{-1} = (1\ 4)(2\ 3) \notin H.$$

**Bài 1.37**. a) $N_G(H) = \{x \in G \mid xH = Hx\} \leq G$ vì

- $e \in N_G(H)$ do $eH = H = He$.
- $\forall x, y \in N_G(H)$, $xy \in N_G(H)$ do
$$(xy)H = x(yH) = x(Hy) = (xH)y = (Hx)y = H(xy).$$
- $\forall x \in N_G(H)$, $x^{-1} \in N_G(H)$ do từ $xH = Hx$ ta suy ra $x^{-1}H = Hx^{-1}$.

b) $H \subset N_G(H)$ vì $\forall x \in H$, $xH = Hx$ và $H \lhd N_G(H)$ do $\forall x \in N_G(H)$, $xH = Hx$.

c) $H \lhd G \Leftrightarrow \forall x \in G, xH = Hx \Leftrightarrow \forall x \in G, x \in N_G(H) \Leftrightarrow N_G(H) = G$.

d) Theo Câu b, $H \lhd N_G(H)$. Nếu $K \leq G$ và $H \lhd K$ thì $\forall x \in K$, $xH = Hx$ nên $x \in N_G(H)$, chứng tỏ $K \subset N_G(H)$. Suy ra $N_G(H)$ là nhóm con lớn nhất của G nhận H làm nhóm con chuẩn tắc.

**Bài 1.38**. Xem Ví dụ trong Dạng toán 6.

**Bài 1.39**. Với mọi $x \in H$, $y \in K$, ta có

$$x^{-1}y^{-1}xy = x^{-1}(y^{-1}xy) \in H;$$
$$x^{-1}y^{-1}xy = (x^{-1}y^{-1}x)y \in K$$

nên $x^{-1}y^{-1}xy \in H \cap K = \{e\}$. Suy ra $x^{-1}y^{-1}xy = e$, nghĩa là $xy = yx$.

**Bài 1.40**. Từ giả thiết $x^{-1}Sx \subset < S >$ ta suy ra $x^{-1}S^{-1}x = (x^{-1}Sx)^{-1} \subset < S >$. Như vậy, với mọi $a \in S \cup S^{-1}$, ta có $x^{-1}ax \in < S >$. Mọi phần tử $y \in < S >$ có dạng $y = a_1 \ldots a_r$

với $a_j \in S \cup S^{-1}$ nên $x^{-1}yx = (x^{-1}a_1x)\ldots(x^{-1}a_rx) \in \langle S \rangle$. Suy ra $\langle S \rangle$ chuẩn tắc trong G.

**Bài 1.41**. Ta chứng minh kết quả tổng quát hơn: *Nếu H là một nhóm con của nhóm hữu hạn G thỏa [G : H] = p với p là ước số nguyên tố bé nhất của |G| thì H chuẩn tắc trong G*.

Ta chứng minh bằng phản chứng. Giả sử H không chuẩn tắc trong G. Khi đó $\exists x \in G$, $x^{-1}Hx \neq H$. Đặt $K = x^{-1}Hx$. Ta có $K \leq G$ (xem Bài 1.18), $K \neq H$ và $|K| = |H|$ nên $H \cap K$ là một nhóm con thực sự của K. Suy ra $\frac{|K|}{|H \cap K|} > 1$ là một ước số của |G| (do đây là ước số của |K|), do đó $\frac{|K|}{|H \cap K|} \geq p$. Từ đây, áp dụng công thức trong Bài 1.25 ta có

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{|G|}{p}\frac{|K|}{|H \cap K|} \geq |G|.$$

Do đó $G = HK$ hay $G = Hx^{-1}Hx$. Suy ra $x = hx^{-1}kx$ với $h, k \in H$ nào đó. Khi đó $x = kh \in H$, dẫn đến $x^{-1}Hx = H$, mâu thuẫn.

**Bài 1.42**. a) ($\Leftarrow$): Nếu G giao hoán thì $C(G) = G$ nên $G / C(G) = \{\bar{e}\}$ và do đó G/C(G) cyclic.

($\Rightarrow$) Giả sử $G / C(G) = \{\bar{a}\}$. Cho $x, y \in G$ tùy ý. Khi đó tồn tại các số nguyên m, n sao cho $\bar{x} = \bar{a}^m = \overline{a^m}, \bar{y} = \bar{a}^n = \overline{a^n}$. Do đó $\exists z, t \in C(G)$, $x = a^mz$, $y = a^nt$. Vì z, t giao hoán với mọi phần tử của G nên

$$xy = (a^mz)(a^nt) = (a^ma^n)(z\,t) = a^n(a^mz)t = (a^nt)(a^mz) = yx.$$

Suy ra G giao hoán.

b) Cho G là một nhóm có cấp $p^2$ với p nguyên tố. Trước hết ta chứng minh $C(G) \neq \{e\}$. Thật vậy, xét quan hệ liên hợp ~ trên G định bởi:

$$\forall x, y \in G, x \sim y \Leftrightarrow \exists a \in G, x = aya^{-1}.$$

Khi đó ~ là một quan hệ tương đương trên G (xem Bài 1.7). Ta có

- $x \in C(G) \Leftrightarrow$ Lớp tương đương chứa x là $[x] = \{x\}$.
- $\forall x \in G \backslash C(G)$, lớp tương đương chứa x là $[x] = \{y^{-1}xy \mid y \in G\}$ có ít nhất 2 phần tử, hơn nữa,

$\forall z, t \in G$, $yxy^{-1} = zxz^{-1} \Leftrightarrow (y^{-1}z)x = x(y^{-1}z) \Leftrightarrow y^{-1}z \in C_G(x) \Leftrightarrow yC_G(x) = zC_G(x)$.

Như vậy trong trường hợp này $|[x]| = [G : C_G(x)]$ là ước số lớn hơn 1 của $|G| = p^2$, do đó |[x]| là một bội số của p.

Từ các kết quả trên, do tập các lớp tương đương khác nhau tạo thành một phân hoạch của G, ta suy ra |C(G)| là bội số của p nên $C(G) \neq \{e\}$.

Áp dụng kết quả trên ta có |C(G)| là một ước số lớn hơn 1 của $p^2$. Nếu $|C(G)| = p$ thì $|G/C(G)| = p$ nên G/C(G) cyclic và do đó theo câu a) ta có G giao hoán, nghĩa là $G = C(G)$, mâu thuẫn. Vậy $|C(G)| = p^2 = |G|$, do đó $G = C(G)$, nghĩa là G giao hoán.

**Nhận xét**. 1) Trong quá trình chứng minh $C(G) \neq \{e\}$, ta đã chứng minh được Công thức Lớp: "*Với G là một nhóm hữu hạn, ta có*

$$|G| = |C(G)| + \sum_{i \in I} [G : C(x_i)],$$

*trong đó* $\{x_i | \ i \in I\}$ *là một tập đầy đủ các phần tử đại diện đôi một không liên hợp với nhau trong G"*

2) Lý luận tương tự như trên ta chứng minh được rằng : *Với mọi nhóm G hữu hạn không tầm thường, có cấp là lũy thừa của một số nguyên tố, ta có tâm C(G) không tầm thường*.

**Bài 1.43**. a) Với mọi $y \in [G,G]$ và $x \in G$, ta có $x^{-1}yx = (x^{-1}(y^{-1})^{-1}xy^{-1})y \in [G,G]$ nên [G,G] chuẩn tắc trong G.

b) Với H là một nhóm con chuẩn tắc bất kỳ của G, ta có

$$\begin{aligned} G/H \text{ giao hoán} &\Leftrightarrow \forall x, y \in G, (xH)(yH) = (yH)(xH) \\ &\Leftrightarrow \forall x, y \in G, x^{-1}y^{-1}xy \in H \\ &\Leftrightarrow [G, G] \subset H. \end{aligned}$$

**Bài 1.44**. Từ bảng nhân sau đây ta thấy $K = \{Id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ là một nhóm con giao hoán của $S_4$:

| | **Id** | **(1 2)(3 4)** | **(1 3)(2 4)** | **(1 4)(2 3)** |
|---|---|---|---|---|
| **Id** | Id | (1 2)(3 4) | (1 3)(2 4) | (1 4)(2 3) |
| **(1 2)(3 4)** | (1 2)(3 4) | Id | (1 4)(2 3) | (1 3)(2 4) |
| **(1 3)(2 4)** | (1 3)(2 4) | (1 4)(2 3) | Id | (1 2)(3 4) |
| **(1 4)(2 3)** | (1 4)(2 3) | (1 3)(2 4) | (1 2)(3 4) | Id |

Tính chuẩn tắc của K được suy từ tính chất sau: Với mọi $\varphi \in S_n$, ta có

$$\varphi\ (i_1\ \ i_2\ ...\ \ i_k)\ \varphi^{-1} = \ (\varphi(i_1)\ \ \varphi(i_2)...\ \ \varphi(i_k)).$$

**Bài 1.45**. a) Được suy từ tính chất: Mọi phép hoán vị đều là tích của các chuyển vị.

b) Xem Ví dụ trong Dạng toán 3.

c) c) Cho $H \lhd A_n$ và H chứa một 3-chu trình. Không mất tính tổng quát, ta có thể giả sử là H chứa (1 2 3). Khi đó $(1\ 3\ 2) = (1\ 2\ 3)^2 \in H$. Cho $\sigma = (i\ j\ k)$ là một 3-chu trình bất kỳ. Ta chứng minh $\sigma \in H$ bằng cách chia thành các trường hợp sau:

- $|\{i, j, k\} \cap \{1, 2, 3\}| = 3$: Ta có $\{i, j, k\} = \{1, 2, 3\}$, từ đó $\sigma = (1\ 2\ 3)$ hay $\sigma = (1\ 3\ 2)$ nên $\sigma \in H$.
- $|\{i, j, k\} \cap \{1, 2, 3\}| = 2$: Ta có thể giả sử $(i = 1, j = 2, k \neq 3)$ hoặc $((i = 1, k = 2, j \neq 3)$. Khi đó

$$\sigma = (1\ 2\ k) = (2\ k\ 3)\ (1\ 3\ 2)\ (2\ k\ 3)^{-1} \in H$$

hoặc

$$\sigma = (1\ \ j\ \ 2) = (2\ j\ 3)\ (1\ 2\ 3)\ (2\ j\ 3)^{-1} \in H.$$

- $|\{i, j, k\} \cap \{1, 2, 3\}| = 1$: Ta có thể giả sử $i = 1$ và $j, k \notin \{1, 2, 3\}$. Khi đó

$$\sigma = (1\ j\ \ k) = \ (2\ j)(3\ k)(1\ 2\ 3)(3\ k)^{-1}(2\ j)^{-1} \in H\ .$$

- $|\{i, j, k\} \cap \{1, 2, 3\}| = 0$. Khi đó

$$\sigma = (i\ j\ k) = \ (1\ 2)(3\ k)(2\ j)(1\ i)(1\ 2\ 3)\ (1\ i)^{-1}(2\ j)^{-1}(3\ k)^{-1}(1\ 2)^{-1} \in H\ .$$

Kết quả trên cho thấy H chứa tất cả các 3-chu trình. Từ đây theo câu b) ta có $H = A_n$.

**Bài 1.46**. f là đồng cấu vì $\forall x, y \in G$, $f(xy) = (xy)^k = x^k y^k = f(x)f(y)$ (do G giao hoán).

$$\text{Ker}(f) = \{x \in G \mid f(x) = e\} = \{x \in G \mid x^k = e\} = \{x \in G \mid o(x) \text{ là ước số của } k\}.$$

**Bài 1.47**. Ánh xạ $f: G \to G$ định bởi $f(x) = x^{-1}$ là một song ánh vì

$$\forall x, y \in G,\ f(x) = y \Leftrightarrow x^{-1} = y \Leftrightarrow x = y^{-1} \in G.$$

Nếu G giao hoán thì $\forall x, y \in G,\ f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$ nên f là một tự đẳng cấu của G.

Đảo lại, giả sử f là một tự đẳng cấu của G. Khi đó $\forall x, y \in G$ ta có $f(xy) = f(x)f(y)$ nên $(xy)^{-1} = x^{-1}y^{-1} = (yx)^{-1}$, từ đó $xy = yx$. Suy ra G giao hoán.

**Bài 1.48**. a) Vì $\text{Im}f \leq \mathbf{Z}$ nên $\text{Im}f = a\mathbf{Z}$ với $a \in \mathbf{N}$.

b) Do f là một đồng cấu nhóm cộng nên $\forall n \in \mathbf{Z}$, $f(n) = nf(1)$. Nếu $f(1) = 0$ thì $\forall n \in \mathbf{Z}$, $f(n) = 0$ nên $\text{Ker}f = \mathbf{Z}$. Nếu $f(1) \neq 0$ thì $\forall n \in \mathbf{Z}\backslash\{\mathbf{0}\}$, $f(n) \neq 0$ nên $\text{Ker}f = \{0\}$.

c) Nếu f là một tự đồng cấu của nhóm cộng **Z** thì $\forall n \in \mathbf{Z}$, $f(n) = nf(1)$, do đó f có dạng $f_a$ với $a \in \mathbf{Z}$, trong đó $f_a(n) = an, \forall n \in \mathbf{Z}$. Đảo lại, dễ thấy các ánh xạ $f_a$ như trên đều là các tự đồng cấu của nhóm cộng **Z**. Do đó tập các tự đồng cấu của nhóm cộng **Z** là $\{f_a \mid a \in \mathbf{Z}\}$, trong đó $f_a(n) = an, \forall n \in \mathbf{Z}$.

**Bài 1.49**. a) Với mọi $n \in \mathbb{N}^*$ ta có

$$f(1) = f\left(\underbrace{1/n + \ldots + 1/n}_{n}\right) = nf(1/n).$$

b) Kết quả trong Câu a cho thấy $f(1)$ là bội số của n với mọi $n \in \mathbb{N}^*$, do đó $f(1) = 0$. Suy ra $f(1/n) = 0$ với mọi $n \in \mathbb{N}^*$. Từ đó

$$\forall m \in \mathbb{Z}, \forall n \in \mathbb{N}^*, f(m/n) = mf(1/n) = 0,$$

nghĩa là f là đồng cấu tầm thường.

**Bài 1.50**. Với f là một tự đồng cấu của nhóm cộng $\mathbf{Z}_{12}$, ta có

$$\forall \bar{n} \in \mathbb{Z}_{12}, f(\bar{n}) = f(n\bar{1}) = nf(\bar{1}),$$

do đó f có dạng $f_a$ với $a \in \{0, 1, \ldots, 11\}$, trong đó $\forall \bar{n} \in \mathbb{Z}_{12}, f_a(\bar{n}) = n\bar{a}$. Đảo lại, dễ thấy các ánh xạ $f_a : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ như trên đều được xác định và là các tự đồng cấu của nhóm cộng $\mathbf{Z}_{12}$. Do đó tập các tự đồng cấu của nhóm cộng $\mathbf{Z}_{12}$ là $\{f_a \mid a \in \{0, 1, \ldots, 11\}\}$, trong đó $\forall \bar{n} \in \mathbb{Z}_{12}, f_a(\bar{n}) = n\bar{a}$.

**Bài 1.51**. Xem Bài 1.47.

**Bài 1.52**. Xem Hệ quả 8.12.

**Bài 1.53**. 1) Sự tồn tại: Trong nhóm $GL(2, \mathbb{C})$ đặt $Q_8 = \langle A, B \rangle$, trong đó

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Ta có

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = B^2, A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2,$$
$$A^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, BA = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = A^{-1}B.$$

Vậy A, B thỏa các hệ thức sau:

$$A^4 = I_2,\ BA = A^{-1}B,\ A^2 = B^2 \qquad (1)$$

Suy ra $Q_8 = \{I_2, A, A^2, A^3, B, AB, A^2B, A^3B\}$ có cấp 8, trong đó

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, A^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$
$$B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, AB = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, A^2B = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, A^3B = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

2) Sự duy nhất: Giả sử $H = < a, b>$ là một nhóm có cấp 8, trong đó a, b thỏa các hệ thức sau:

$$a^4 = e,\ ba = a^{-1}b,\ a^2 = b^2. \qquad (2)$$

Khi đó $H = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$. Xét ánh xạ $\varphi: Q_8 \to H$ định bởi

$$\varphi(I_2) = e,\ \varphi(A) = a,\ \varphi(A^2) = a^2,\ \varphi(A^3) = a^3,$$
$$\varphi(B) = b,\ \varphi(AB) = ab,\ \varphi(A^2B) = a^2b,\ \varphi(A^3B) = a^3b.$$

Ta có $\varphi$ là song ánh. Hơn nữa, do các hệ thức (1) và (2) ta có

$$\forall i, j \in \mathbf{N},\ \varphi(A^iB^j) = a^ib^j.$$

Suy ra $\forall x, y \in Q_8$, $\varphi(xy) = \varphi(x)\varphi(y)$, nghĩa là $\varphi$ là một đồng cấu. Vậy $\varphi$ là một đẳng cấu. Điều này chứng minh tính duy nhất của nhóm H (sai khác một đẳng cấu).

**Bài 1.54**. Xét nhóm Quaternion $Q_8 = < a, b >$, trong đó

$$a^4 = e,\ ba = a^{-1}b,\ a^2 = b^2.$$

Ta có $Q_8 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$ có cấp 8. Cho H là một nhóm con bất kỳ của $Q_8$. Khi đó $|H| \in \{1, 2, 4, 8\}$.

1) Nếu $|H| = 1$ hay $|H| = 8$ thi hiển nhiên $H \lhd Q_8$.

2) Nếu $|H| = 4$ thi $[Q_8: H] = 2$ nên theo Bài 1.41 $H \lhd Q_8$.

3) Giả sử $|H| = 2$. Khi đó H cyclic. Dễ thấy các phần tử a, $a^3$, b, $a^2b$ (= $b^3$) đều có cấp 4. Hơn nữa,

$$\begin{cases} (a^2)^2 = e, a^2 \neq e; \\ (ab)^2 = (a^3b)^2 = a^2 \end{cases}$$

nên các phần tử ab, $a^3b$ đều có cấp 4 và phần tử $a^2$ có cấp 2. Suy ra $H = < a^2 >$. Vì $aa^2a^{-1} = a^2 \in H$, $ba^2b^{-1} = b^2 = a^2 \in H$ nên H chuẩn tắc trong $Q_8$.

Trong mọi trường hợp ta đều có $H \lhd Q_8$.

**Bài 1.55**. 1) Sự tồn tại: Trong nhóm $GL(2, \mathbb{C})$, đặt $D_n = < A, B >$, trong đó

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Ta có

$$A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = B^n, B^{-1} = \begin{pmatrix} \zeta^{-1} & 0 \\ 0 & \zeta \end{pmatrix},$$

$$AB = \begin{pmatrix} 0 & \zeta^{-1} \\ \zeta & 0 \end{pmatrix} = B^{-1}A.$$

Vậy A, B thỏa các hệ thức sau:

$$A^2 = I_2, B^n = I_2, AB = B^{-1}A. \qquad (1)$$

Suy ra $D_n = \{I_2, B, \ldots, B^{n-1}, A, AB, \ldots, AB^{n-1}\}$ có cấp 2n, trong đó

$$B^k = \begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^{-k} \end{pmatrix}, AB^k = \begin{pmatrix} 0 & \zeta^k \\ \zeta^{-k} & 0 \end{pmatrix}, k = 0, 1, \ldots, n-1.$$

2) Sự duy nhất: Giả sử H = < a, b > là một nhóm có cấp 2n, trong đó a, b thỏa các hệ thức sau:

$$a^2 = e, b^n = e, ab = b^{-1}a. \qquad (2)$$

Khi đó $H = \{e, b, \ldots, b^{n-1}, a, ab, \ldots, ab^{n-1}\}$. Xét ánh xạ $\varphi: D_n \to H$ định bởi

$$\varphi(B^i) = b^i, \varphi(AB^i) = ab^i.$$

Ta có φ là song ánh. Hơn nữa, do các hệ thức (1) và (2) ta có

$$\forall i, j \in \mathbf{N}, \varphi(A^iB^j) = a^ib^j.$$

Suy ra $\forall x, y \in D_n, \varphi(xy) = \varphi(x)\varphi(y)$, nghĩa là φ là một đồng cấu. Vậy φ là một đẳng cấu. Điều này chứng minh tính duy nhất của nhóm H (sai khác một đẳng cấu).

**Bài 1.56**. Xét nhóm nhị diện $D_n = < a, b >$, trong đó

$$a^2 = e, b^n = e, ab = b^{-1}a.$$

Ta có

1) $aba^{-1} = b^{-1} \in < b >$, $bbb^{-1} = b \in < b >$ nên < b > chuẩn tắc trong $D_n$.
2) $bab^{-1} = ab^{-2} = ab^{n-2} \notin < a >$ nên < a > không chuẩn tắc trong $D_n$.

**Nhận xét**. Có thể giải câu a) như sau: < b > là nhóm con có chỉ số 2 trong $D_n$ nên chuẩn tắc trong $D_n$ (xem Bài 1.41).

**Bài 1.57**. a) Cho nhóm G có $|G| \le 5$.

1) Nếu $|G| \in \{1, 2, 3, 5\}$ thi G cyclic nên G giao hoán.
2) Cho |G| = 4. Nếu G cyclic thì G giao hoán. Nếu G không cyclic thi mọi phần tử $x \in G$ khác e đều có cấp 2 nên theo Bài 1.6 G giao hoán.

b) Cho nhóm G có |G| = 6.

1) Trường hợp G giao hoán: Giả sử G không cyclic. Khi đó mọi phần tử $x \in G\backslash\{e\}$ có cấp 2 hoặc 3. Sử dụng kết quả: "*Nếu G là một nhóm giao hoán hữu hạn thỏa tính chất mọi phần tử khác e trong G đều có cấp là số nguyên tố p cho trước thì G có cấp là một lũy thừa của p*" (xem lời giải Bài 1.28), ta suy ra trong G tồn tại các phần tử a và b có các cấp lần lượt là 2 và 3. Khi đó phần tử ab có cấp 6 (xem Bài 1.30) nên G = < ab >, mâu thuẫn. Vậy G cyclic.

2) Trường hợp G không giao hoán: Khi đó mọi phần tử $x \in G\backslash\{e\}$ có cấp 2 hoặc 3. Nếu mọi phần tử $x \in G\backslash\{e\}$ đều có cấp 2 thi G giao hoán (xem Bài 1.6), mâu thuẫn. Do đó tồn tại $b \in G$ có cấp 3. Chọn $a \in G\backslash < b >$. Ta có $< a > \cap < b > = \{e\}$ vì trong

trường hợp ngược lại sẽ có $< a > \cap < b > = < b >$, dẫn đến $< a > = < b >$ (do $|< a >| \le 3 = |< b >|$ ), mâu thuẫn. Áp dụng công thức trong Bài 1.25 ta có

$$\left|\langle a, b\rangle\right| = \left|\langle a\rangle\langle b\rangle\right| = \frac{\left|\langle a\rangle\right|\left|\langle b\rangle\right|}{\left|\langle a\rangle \cap \langle b\rangle\right|} = 3\left|\langle a\rangle\right|.$$

Nếu a có cấp 3 thì $|< a, b>| = 9 > |G|$, mâu thuẫn. Vậy a có cấp 2 và $|< a, b>| = 6 = |G|$, do đó $G = < a, b>$. Vì $[G : < b >] = 2$ nên $< b >$ chuẩn tắc trong G (xem Bài 1.41). Do đó $aba^{-1}$ thuộc $< b >$. Nếu $aba^{-1} = e$ thi $b = e$, mâu thuẫn. Nếu $aba^{-1} = b$ thi $ab = ba$ dẫn đến G giao hoán, mâu thuẫn. Vậy $aba^{-1} = b^2 = b^{-1}$ hay $ab = b^{-1}a$. Như vậy, G là nhóm có cấp 6 và $G = < a, b>$, trong đó a, b thỏa các hệ thức

$$a^2 = e,\ b^3 = e,\ ab = b^{-1}a.$$

Do đó G đẳng cấu với nhóm nhị diện $D_3$.

**Nhận xét.** Nếu dùng Bổ đề Cauchy (xem Nhận xét trong Bài 1.28) ta suy ra ngay sự tồn tại của các phần tử a và b trong G, có các cấp lần lượt là 2 và 3.

**Bài 1.58**. Xem Ví dụ trong Dạng toán 10.

**Bài 1.59**. a) $y^n = (f(x))^n = f(x^n) = f(e) = e$.

b) Đặt Hom(G,G′) là tập hợp tất cả các đồng cấu nhóm từ G vào G′ và

$$Y = \{y \in G' |\ o(y) \text{ là ước của } n\}.$$

Xét ánh xạ $\varphi$: Hom(G, G′) $\to$ Y định bởi $\varphi(f) = f(x)$. Kết quả Câu a cho thấy $\varphi$ được xác định. Ta chứng minh $\varphi$ là song ánh. Thật vậy,

1) $\varphi$ là đơn ánh vì

$$\begin{aligned}\forall f, g \in \mathrm{Hom}(G, G'), \varphi(f) = \varphi(g) &\Rightarrow f(x) = g(x)\\ &\Rightarrow \forall k \in \mathbb{Z}, f(x^k) = g(x^k)\\ &\Rightarrow \forall z \in G, f(z) = g(z)\\ &\Rightarrow f = g.\end{aligned}$$

2) $\varphi$ là toàn ánh: Thật vậy, với mỗi $y \in Y$, đặt $f: G \to G'$ định bởi

$$\forall k \in \mathbf{Z},\ f(x^k) = y^k.$$

- f được xác định vì

$$\begin{aligned}\forall k, l \in \mathbb{Z}, x^k = x^l &\Rightarrow (k - l) \vdots n\\ &\Rightarrow (k - l) \vdots o(y)\\ &\Rightarrow y^k = y^l\\ &\Rightarrow f(x^k) = f(x^l).\end{aligned}$$

- f là đồng cấu nhóm vì

$$\forall k, l \in \mathbb{Z}, f(x^k x^l) = f(x^{k+l}) = y^{k+l} = y^k y^l = f(x^k) f(x^l).$$

Vậy $f \in \mathrm{Hom}(G, G')$. Theo cách đặt, ta có $\varphi(f) = f(x) = y$. Vậy $\varphi$ là toàn ánh.

**Bài 1.60**. a) Vì G hữu hạn nên mọi $x \in G$ có cấp hưu hạn. Đặt $o(x) = n$. Ta có

$$(f(x))^n = f(x^n) = f(e) = e$$

nên f(x) có cấp là ước số của n.

b) Theo Định lý đẳng cấu 1, $G / \mathrm{Ker} f \simeq \mathrm{Im} f$ nên |Imf| = |G|/|Kerf| là ước số của |G|.

**Bài 1.61**. Cho $G = < a >$ có cấp n.

($\Rightarrow$) Cho $G' = f(G)$ với f là một đồng cấu nhóm từ G vào một nhóm nào đó. Khi đó

$$G' = \{f(x)|\ x \in G\} = \{f(a^m)|\ m \in \mathbf{Z}\} = \{f(a)^m|\ m \in \mathbf{Z}\} = < f(a) >$$

nên G′ là nhóm cyclic sinh bởi f(a). Hơn nữa, $f(a)^n = f(a^n) = f(e) = e$ nên f(a) có cấp là ước của n. Suy ra G′ có cấp là ước của n.

($\Leftarrow$) Cho $G' = < b >$ là nhóm cyclic có cấp m với m|n. Xét ánh xạ $f: G \to G'$ định bởi $f(a^k) = b^k$, $\forall k \in \mathbf{Z}$. Khi đó

- f được xác định vì

$$\forall k, l \in \mathbb{Z}, a^k = a^l \Rightarrow (k-l) \vdots n$$
$$\Rightarrow (k-l) \vdots o(b)$$
$$\Rightarrow b^k = b^l$$
$$\Rightarrow f(a^k) = f(a^l).$$

- f là đồng cấu nhóm vì

$$\forall k, l \in \mathbb{Z}, f(a^k a^l) = f(a^{k+l}) = b^{k+l} = b^k b^l = f(a^k) f(a^l).$$

Vậy $f \in \mathrm{Hom}(G,G')$ và ta có $G' = \{b^k \mid k \in \mathbf{Z}\} = \{f(a^k)|\ k \in \mathbf{Z}\} = f(G)$.

**Bài 1.62**. Vì $\mathbb{C}^*$ là một nhóm giao hoán nên mọi nhóm con H của $\mathbb{C}^*$ đều chuẩn tắc. Giả sử H có chỉ số n trong G. Khi đó nhóm thương $\mathbb{C}^*/H$ có cấp n. Do đó với mọi $u \in \mathbb{C}^*$ ta có $\bar{u}^n = \bar{0}$, nghĩa là $u^n \in H$. Chú ý rằng với mọi $z \in \mathbb{C}^*$, tồn tại $u \in \mathbb{C}^*, z = u^n$ nên theo chứng minh trên ta có $z \in H$. Điều này chứng tỏ $H = \mathbb{C}^*$.

**Bài 1.63**. a) Ta có $p_1: G \to G_1$, $p_1(x_1, x_2) = x_1$ và $p_2: G \to G_2$, $p_2(x_1, x_2) = x_2$.

1) $p_1$ là đồng cấu nhóm vì

$$\forall (x_1, x_2), (y_1, y_2) \in G,\ p_1[(x_1, x_2)(y_1, y_2)] = p_1(x_1y_1, x_2y_2)$$
$$= x_1y_1 = p_1(x_1, x_2)p_1(x_2 + y_2).$$

2) $p_1$ là toàn ánhvì $\forall x_1 \in G_1, \exists (x_1, e_2) \in G,\ p_1(x_1, e_2) = x_1$.

3) $\mathrm{Kerp}_1 = \{(x_1, x_2) \in G|\ p_1(x_1, x_2) = e_1\} = \{(x_1, x_2) \in G|\ x_1 = e_1\}$
$= \{(e_1, x_2)|\ x_2 \in G_2\} = H_2$.

Vậy $p_1$ là toàn cấu và $\mathrm{Kerp}_1 = H_2$ chuẩn tắc trong G. Tương tự, $p_2$ là toàn cấu và $\mathrm{Kerp}_2 = H_1$ chuẩn tắc trong G.

b) Ta có $i_1: G_1 \to G$, $i_1(x_1) = (x_1, e_2)$ và $i_2: G_2 \to G$, $i_2(x_2) = (e_1, x_2)$.

1) $i_1$ là đồng cấu nhóm vì

$$\forall x_1, y_1 \in G_1,\ i_1(x_1y_1) = (x_1y_1, e_2) = (x_1, e_2)(y_1, e_2) = i_1(x_1)i_1(y_1).$$

2) $i_1$ là đơn ánhvì $\forall x_1, y_1 \in G_1,\ i_1(x_1) = i_1(y_1) \Rightarrow (x_1, e_2) = (y_1, e_2) \Rightarrow x_1 = y_1$.

3) $\mathrm{Imi}_1 = \{i_1(x_1)|\ x_1 \in G_1\} = \{(x_1, e_2) \mid x_1 \in G_1\} = H_1$.

Vậy $i_1$ là đơn cấu và $\mathrm{Imi}_1 = H_1$. Tương tự, $i_2$ là đơn cấu và $\mathrm{Imi}_2 = H_2$.

c) Từ Câu a, theo Định lý đẳng cấu 1 ta có $G/H_2 \simeq G_1$. Mặt khác, theo Câu b ta có $G_1 \simeq i_1(G_1) = H_1$. Do đó $G/H_2 \simeq H_1$. Tương tự, $G/H_1 \simeq H_2$.

d) $G = \{(x_1, x_2)|\ x_1 \in G_1, x_2 \in G_2\} = \{(x_1, e_2)(e_1, x_2)|\ x_1 \in G_1, x_2 \in G_2\} = H_1H_2$.

$H_1 \cap H_2 = \{(x_1, x_2)|\ \exists\, y_1 \in G_1, y_2 \in G_2, (x_1, x_2) = (y_1, e_2) = (e_1, y_2)\} = \{(e_1, e_2)\}$.

Chứng minh tương tự như trên, ta có kết quả mở rộng cho tích trực tiếp $G_1\times\ldots\times G_n$ như sau: Cho $G_j$ $(1 \le j \le n)$ là các nhóm với các phần tử đơn vị là $e_j$ và $G = G_1\times\ldots\times G_n$.Với mỗi $1 \le k \le n$, đặt

$$H_k = \{(x_1, \ldots, x_n) \in G |\ \forall 1 \le j \ne k \le n, x_j = e_j\},$$
$$p_k: G \to G_k,\ p_k(x_1,\ldots, x_n) = x_k,$$
$$i_k: G_k \to G,\ i_k(x_k) = (e_1, \ldots, e_{k-1}, x_k, e_{k+1}, \ldots, e_n).$$

Khi đó ta có

a′) $H_k \lhd G$, $p_k$ là toàn cấu và $\mathrm{Ker} p_k = \prod_{k\ne j=1}^{n} H_j$.

b′) $i_k$ là đơn cấu và $\mathrm{Im}\, i_k = H_k$.

c′) $G / \prod_{k\ne j=1}^{n} H_j \simeq H_k$.

d′) $G = H_1 \ldots H_n$ và $H_k \cap \left(\prod_{k\ne j=1}^{n} H_j\right) = \{(e_1,\ldots,e_n)\}$.

**Bài 1.64**. a) Aut(G) = {f: G → G là tự đẳng cấu} là một nhóm. Thật vậy, theo Mệnh đề 8.4 tích của hai đẳng cấu cũng là một đẳng cấu nên tích các ánh xạ là một phép toán trên Aut(G).

- Tính kết hợp: $\forall f, g, h \in Aut(G), (fg)h = f(gh)$.
- Aut(G) có phần tử trung hòa là ánh xạ đồng nhất $Id_G$ vì
$$\forall f \in Aut(G), fId_G = Id_G f = f.$$
- Với mỗi f ∈ Aut(G), theo Mệnh đề 8.5 $f^{-1} \in$ Aut(G) và đây chính là phần tử đối xứng của f vì $f f^{-1} = f^{-1} f = Id_G$.

b) Xem Ví dụ trong Dạng toán 8.

c) Inn(G) = $\{\varphi_g |\ g \in G\} \subset$ Aut(G) (do Câu b) là một nhóm con chuẩn tắc của Aut(G). Thật vậy,

- $Id_G = \varphi_e \in$ Inn(G).
- $\forall g, h \in G, \varphi_g\varphi_h = \varphi_{gh} \in Inn(G)$ do
$$\forall x \in G, (\varphi_g\varphi_h)(x) = \varphi_g(\varphi_h(x)) = \varphi_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \varphi_{gh}(x).$$
- $\forall g \in G, (\varphi_g)^{-1} = \varphi_{g^{-1}} \in Inn(G)$ do $\varphi_g\varphi_{g^{-1}} = \varphi_{gg^{-1}} = \varphi_e = Id_G$.
- $\forall g \in G, \forall \psi \in Aut(G), \psi\varphi_g\psi^{-1} = \varphi_{\psi(g)} \in Inn(G)$ do
$$\forall x \in G, (\psi\varphi_g\psi^{-1})(x) = \psi(\varphi_g(\psi^{-1}(x))) = \psi(g\psi^{-1}(x)g^{-1}) = \psi(g)x(\psi(g))^{-1} = \varphi_{\psi(g)}(x).$$

d) Xét ánh xạ ψ: G → Inn(G) định bởi $\psi(g) = \varphi_g$, ∀g ∈ G. Hiển nhiên, ψ là một toàn ánh. Hơn nữa,

- ψ là một đồng cấu vì ∀g, h ∈ G, $\psi(gh) = \varphi_{gh} = \varphi_g\varphi_h = \psi(g)\psi(h)$ (xem lời giải Câu c).
- Ker $\psi = \{g \in G |\ \varphi_g = Id_G\} = \{g \in G |\ \forall x \in G, \varphi_g(x) = x\}$

$= \{g \in G | \forall x \in G, gxg^{-1} = x\} = \{g \in G | \forall x \in G, gx = xg\} = C(G)$.
Do đó theo Định lý đẳng cấu 1, $G / C(G) \simeq \mathrm{Inn}(G)$.

**Bài 1.65**. a) Theo Mệnh đề 8.5, $f^{-1}$ là một đẳng cấu từ G đến G′. Do đó, theo Định lý 8.7, $\forall H \le G$, $f(H) \le G'$ và $\forall H' \le G'$, $f^{-1}(H') \le G$. Hơn nữa, $\forall H \le G$, $(f^{-1}f)(H)) = H$ và $\forall H' \le G'$, $(ff^{-1})(H') = H'$. Từ đó suy ra điều cần chứng minh.
b) Theo Định lý 8.7, $\forall H' \lhd G', f^{-1}(H') \lhd G$ và $\forall H \lhd G, f(H) = (f^{-1})^{-1}(H) \lhd G'$ (do $f^{-1}$ là một đẳng cấu từ G′ đến G). Từ đó kết hợp với Câu a ta có điều cần chứng minh.
c) Giả sử $H \lhd G$. Khi đó theo Câu b, $f(H) \lhd G'$. Xét ánh xạ $\varphi: G \to G'/f(H)$ định bởi $\varphi(x) = f(x)f(H)$. Vì f là một song ánh (do đó f là toàn ánh) nên φ là một toàn ánh . Hơn nữa, φ là một đồng cấu vì

$$\forall x, y \in G, \varphi(xy) = f(xy)f(H) = (f(x)f(y))f(H) = (f(x)f(H))(f(y)f(H)) = \varphi(x)\varphi(y).$$

Do đó φ là một toàn cấu. Mặt khác,

$\mathrm{Ker}\varphi = \{x \in G | f(x)f(H) = f(H)\} = \{x \in G | f(x) \in f(H)\} = \{x \in G | x \in H\} = H$.

nên theo Định lý đẳng cấu 1, $G / H \simeq G' / f(H)$.

**Bài 1.66**. a) Xem Ví dụ trong Dạng toán 9..
b) Theo Câu a, f là một đơn cấu có $\mathrm{Im}f = n\mathbf{Z}$, do đó $f: \mathbf{Z} \to n\mathbf{Z}$ là một đẳng cấu nhóm cộng. Vì tập các nhóm con của **Z** là $\{m\mathbf{Z} | m \in \mathbf{N}^*\}$ nên bằng cách sử dụng Bài 1.65 ta suy ra tập các nhóm con của n**Z** là $\{f(m\mathbf{Z}) | m \in \mathbf{N}^*\} = \{mn\mathbf{Z} | m \in \mathbf{N}^*\}$.
c) Với $m \in \mathbf{N}$, áp dụng Câu c, Bài 1.65 ta có $\mathbb{Z} / m\mathbb{Z} \simeq n\mathbb{Z} / f(m\mathbb{Z}) = n\mathbb{Z} / mn\mathbb{Z}$.

**Bài 1.67**. Xét ánh xạ $\psi: G \to S(G)$ định bởi $\psi(x) = f_x$, $\forall x \in G$, trong đó $f_x(g) = xg$, $\forall g \in G$.

- ψ đươc xác định vì $\forall x \in G$, $f_x \in S(G)$ do $f_x$ là một song ánh từ G vào G. Thật vậy,
$$\forall g, h \in G, f_x(g) = h \Leftrightarrow xg = h \Leftrightarrow g = x^{-1}h \in G.$$
- ψ là một đơn ánh vì
$\forall x, y \in G, \psi(x) = \psi(y) \Rightarrow \forall g \in G, xg = yg$
$\Rightarrow xe = ye$, nghĩa là $x = y$.
- ψ là một đồng cấu vì $\forall x, y \in G, \psi(xy) = f_{xy} = f_x f_y = \psi(x)\psi(y)$ do
$\forall g \in G, f_{xy}(g) = (xy)g = x(yg) = x(f_y(g)) = f_x(f_y(g)) = (f_x(f_y))(g)$.

Vậy ψ là một đơn cấu từ G vào S(G). Suy ra $G \simeq \psi(G) \le S(G)$ và ta có điều cần chứng minh.
**Chú ý**. Kết quả sau cùng trong Bài 1.67 được gọi là Định lý Cayley.

**Bài 1.68**. $G = \langle x \rangle$ có cấp m, $G' = \langle y \rangle$ có cấp n. Xét tương ứng $f: G \to G'$ định bởi $f(x^k) = y^{kl}$, $\forall k \in \mathbf{N}$ ($l \in \mathbf{N}$ cho trước).

a) Xem Ví dụ trong Dạng toán 7..

b) ($\Rightarrow$) Giả sử f là một đẳng cấu. Khi đó $m = |G| = |G'| = n$ và $G' = < f(x) > = < y^l >$. Theo Bài 1.34, $(n, l) = 1$.

($\Leftarrow$) Giả sử $m = n$ và $(n, l) = 1$. Theo Bài 1.34 phần tử $f(x) = y^l$ có cấp n nên $G' = < f(x) >$. Do đó f là toàn cấu. Mà $|G| = |G'| < \infty$ nên f cũng là đẳng cấu.

c1) Xét $G = < x >$ có cấp 8, $G' = < y >$ có cấp 12. Cho $f: G \to G'$ là một đồng cấu nhóm. Đặt $f(x) = y^l$ $(0 \le l \le 11)$. Khi đó $f(x^k) = y^{kl}$, $\forall k \in \mathbf{N}$ và $8l$ chia hết cho 12 (theo Câu a) nên $l \in \{0, 3, 6, 9\}$. Vậy $f = f_l$, $l \in \{0, 3, 6, 9\}$, trong đó $f_l(x^k) = y^{kl}$, $\forall k \in \mathbf{N}$. Đảo lại, cũng theo Câu a, các $f_l$ như trên đều là các đồng cấu nhóm. Vậy tập các tự đồng cấu nhóm từ G đến G′ là $\{f_l \mid l \in \{0, 3, 6, 9\}$, trong đó $f_l(x^k) = y^{kl}$, $\forall k \in \mathbf{N}$.

c2) Xét $G = < x >$ có cấp 12, $G' = < y >$ có cấp 8. Cho $f: G \to G'$ là một đồng cấu nhóm. Đặt $f(x) = y^l$ $(0 \le l < 8)$. Khi đó $f(x^k) = y^{kl}$, $\forall k \in \mathbf{N}$ và $12l$ chia hết cho 8 (theo Câu a) nên $l \in \{0, 2, 4, 6\}$. Vậy $f = f_l$, $l \in \{0, 2, 4, 6\}$, trong đó $f_l(x^k) = y^{kl}$, $\forall k \in \mathbf{N}$. Đảo lại, cũng theo Câu a, các $f_l$ như trên đều là các đồng cấu nhóm. Vậy tập các tự đồng cấu nhóm từ G đến G′ là $\{f_l \mid l \in \{0, 2, 4, 6\}\}$, trong đó $f_l(x^k) = y^{kl}$, $\forall k \in \mathbf{N}$.

d) Xét $G = < x >$ có cấp 8. Cho f là một tự đẳng cấu của G. Đặt $f(x) = y^l$ $(0 \le l \le 8)$. Khi đó $f(x^k) = y^{kl}$, $\forall k \in \mathbf{N}$ và $(8, l) = 1$ (theo Câu b) nên $l \in \{1, 3, 5, 7\}$. Vậy $f = f_l$, $l \in \{1, 3, 5, 7\}$, trong đó $f_l(x^k) = y^{kl}$, $\forall k \in \mathbf{N}$. Đảo lại, cũng theo Câu b, các $f_l$ như trên đều là các tự đẳng cấu nhóm của G. Vậy tập các tự đẳng cấu của G là $\{f_l \mid l \in \{1, 3, 5, 7\}$, trong đó $f_l(x^k) = y^{kl}$, $\forall k \in \mathbf{N}$.

**Bài 1.69**. a) $\forall 1 \le i \ne j \le n$, $G_i$ và $G_j$ là các nhóm con chuẩn tắc của G thỏa $G_i \cap G_j = \{e\}$ nên theo Bài 1.39, $\forall x_i \in G_i$, $\forall x_j \in G_j$, $x_i x_j = x_j x_i$.
i) Do $G = G_1 \ldots G_n$ nên mọi phần tử $x \in G$ được viết dưới dạng $x = x_1 \ldots x_n$ với $x_i \in G_i$, $\forall 1 \le i \le n$. Cho $x = x_1 \ldots x_n = y_1 \ldots y_n$ với $x_i, y_i \in G_i$. Ta chứng minh $x_i = y_i$, $\forall 1 \le i \le n$, bằng qui nạp theo n. Với $n = 1$, hiển nhiên $x_1 = y_1$. Xét $n > 1$. Ta có

$$x_n y_n^{-1} = (x_1 \ldots x_{n-1})^{-1} (y_1 \ldots y_{n-1}) \in G_1 \cap (G_2 \ldots G_n) = \{e\}$$

nên $x_n = y_n$ và $x_1 \ldots x_{n-1} = y_1 \ldots y_{n-1}$. Theo giả thiết qui nạp, $x_i = y_i, \forall 1 \le i \le n-1$. Kết hợp với đẳng thức $x_n = y_n$ ta suy ra tính duy nhất của $x_1, .., x_n$.

ii) Đặt $f: G \to G_1 \times \ldots \times G_n$ định bởi $\forall x_i \in G_i$, $1 \le i \le n$, $f(x_1 \ldots x_n) = (x_1, \ldots, x_n)$. Do i), ánh xạ f được xác định. Hiển nhiên f là đơn ánh. Mặt khác, theo giả thiết $G = G_1 \ldots G_n$ nên f là toàn ánh. Vậy f là song ánh. Hơn nữa, f là đồng cấu nhóm vì $\forall x_i, y_i \in G_i$, $1 \le i \le n$,

$$f[(x_1 \ldots x_n)(y_1 \ldots y_n)] = f[(x_1 y_1) \ldots (x_n y_n)] = (x_1 y_1, \ldots, x_n y_n) = (x_1, \ldots, x_n)(y_1, \ldots, y_n).$$

Vậy f là một đẳng cấu từ G vào $G_1 \times \ldots \times G_n$.
b) Ta có thể giả sử $G = H_1 \times \ldots \times H_n$. Khi đó theo kết quả mở rộng Bài 1.63, G là nội tích trực tiếp của các nhóm con $G_i$, $1 \le i \le n$, trong đó

$$G_i = \{(x_1, \ldots, x_n) \in G \mid \forall 1 \le j \ne i \le n, x_j = e_j \ (e_j \text{ là phần tử đơn vị của } H_j)\}.$$

**Bài 1.70**. Cho nhóm G có $|G| = p^2$ với p nguyên tố.

1) Nếu G cyclic thì $G \simeq \mathbb{Z}_{p^2}$.

2) Giả sử G không cyclic. Khi đó mọi phần tử $x \in G\backslash\{e\}$ có cấp p. Chọn $a \in G\backslash\{e\}$ và $b \in G\backslash< a >$. Khi đó $< a >, < b >$ là các nhóm con cấp p (và do đó có chỉ số p trong G), chuẩn tắc trong G (xem lời giải mở rộng Bài 1.41) và $< a > \cap < b > = \{e\}$. Áp dụng công thức trong Bài 1.25 ta có

$$\left|\langle a\rangle\langle b\rangle\right| = \frac{\left|\langle a\rangle\right|\left|\langle b\rangle\right|}{\left|\langle a\rangle \cap \langle b\rangle\right|} = p^2 = \left|G\right|.$$

Do đó $G = < a >< b >$. Theo a) Bài 1.69, $G \simeq \langle a\rangle \times \langle b\rangle$. Mà $< a >, < b >$ là các nhóm con cyclic cấp p nên chúng đều đẳng cấu với $\mathbb{Z}_p$. Suy ra $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.

**Nhận xét.** Có thể sử dụng Bài 1.42 để thấy G giao hoán. Khi đó tính chuẩn tắc của các nhóm con $< a >, < b >$ trong chứng minh trên là hiển nhiên.

# CHƯƠNG II. VÀNH VÀ TRƯỜNG

## A. TÓM TẮT LÝ THUYẾT

1. Các khái niệm vành, miền nguyên và trường

1.1.*Vành* là một tập hợp $R$ cùng với hai phép toán cộng và nhân thỏa tính chất sau:

($R_1$) ($R$, + ) là nhóm Abel;

($R_2$) ($R$, . ) là nửa nhóm;

($R_3$) Phép nhân phân phối đối với phép cộng, nghĩa là với mọi $x, y, z \in R$ ta có

$x(y + z) = xy + xz$;

$(y + z)x = yx + zx$.

Nếu phép nhân giao hoán thì ta nói vành $R$ *giao hoán*; nếu phép nhân có đơn vị thì vành $R$ được gọi là *vành có đơn vị*. Phần tử đơn vị của $R$ thường được ký hiệu là 1 hoặc $e$.

1.2. Phần tử $a \neq 0$ của vành giao hoán được gọi là *ước của không* nếu tồn tại phần tử $b \neq 0$ của $R$ sao cho $ab = 0$.

1.3. Một vành giao hoán, có đơn vị $e \neq 0$, không có ước của không được gọi là *miền nguyên*.

1.4. Một vành giao hoán, có đơn vị $e \neq 0$, mọi phần tử khác không đều khả nghịch được gọi là *trường*.

2. Vành con, trường con, ideal, vành thương

2.1. Tập con $A$ khác rỗng của vành $R$(t.ư., trường $R$) được gọi là *vành con* của $R$(t.ư., *trường con* của $R$) nếu $A$ ổn định với hai phép toán của vành $R$ và $A$ cùng với hai phép toán cảm sinh là một vành (t. ư., trường).

2.2.Vành con $I$ của vành $R$ được gọi là một *ideal trái*(t.ư. ,*ideal phải*) của $R$ nếu với mọi $r \in R$ và $x \in I$ ta có $rx \in I$ (t.ư., $xr \in I$). Ta nói I là *ideal* của $R$ nếu $I$ vừa là ideal trái vừa là ideal phải của $R$.

2.3.Tập con $A$ khác rỗng của vành $R$ là vành con của vành $R$ khi và chỉ khi với mọi $x$, $y \in A$ ta có $x - y \in A$ và $xy \in A$.

2.4. Tập con $A$ khác rỗng của vành $R$ là ideal của vành $R$ khi và chỉ khi với mọi $x$, $y \in A$ ta có $x - y \in A$ và với mọi $r \in R$, $x \in A$ ta có $rx \in A$, $xr \in A$ .

2.5. Tập con $A$ có nhiều hơn một phần tử là trường con của trường $R$ khi và chỉ khi với mọi $x, y \in A$, $x - y \in A$ và hơn nữa, nếu $x \neq 0$ thì $x^{-1}y \in A$.

2.6. Giao của một họ tùy ý các ideal của vành $R$ là một ideal của vành $R$.

2.7. Cho $S$ là một tập con khác rỗng của vành $R$. Giao của tất cả các ideal của $R$ chứa $S$ được gọi là *ideal sinh bởi tập S*, ký hiệu là $<S>$. Khi đó tập $S$ được gọi là *tập sinh* của $<S>$. Nếu $S$ hữu hạn thì $<S>$ gọi là *ideal hữu hạn sinh*. Đặc biệt , nếu $S = \{a\}$ thì ta viết $<a>$ thay cho $<\{a\}>$. Ta gọi $<a>$ là *ideal chính* sinh bởi $a$. Nếu vành $R$ giao hoán, có đơn vị thì

$$<a> = \{xa \mid x \in R\} = Ra.$$

2.8. Giả sử $I$ là một ideal của vành ($R$, +, .). Trên nhóm thương ($R/I$, +) ta định nghĩa phép nhân như sau:

$$(x + I)(y + I) = xy + I.$$

Khi đó ($R/I$, +, .) là một vành, gọi là *vành thương* của vành $R$ trên ideal $I$.

3. Đồng cấu vành

3.1. Ánh xạ $f$ từ vành $R$ vào vành $R'$ được gọi là *đồng cấu vành* nếu $f$ bảo toàn các phép toán. Đồng cấu từ $R$ vào $R$ được gọi là *tự đồng cấu* của $R$. Một đồng cấu đồng thời là đơn ánh, toàn ánh, song ánh lần lượt được gọi là *đơn cấu* , *toàn cấu*, *đẳng cấu*.Nếu tồn tại một đẳng cấu từ $R$ vào $R'$ thì ta nói $R$ đẳng cấu với $R'$, ký hiệu là $R \cong R'$.

3.2. Cho đồng cấu vành $f: R \to R'$ . Khi đó

i) $f(0_R) = 0_{R'}$.

ii) $f(-x) = -f(x)$.

iii) Nếu $A$ là vành con của $R$ thì $f(A)$ là vành con của $R'$. Nói riêng $Imf = f(X)$ là vành con của $R'$.

iv) Nếu $A'$ là vành con của $R'$ thì $f^1(A')$ là vành con của $R$. Nói riêng $Ker\, f = f^1(0)$ là vành con của $R$.

v) $f$ là đơn cấu khi và chỉ khi $kerf = 0$, $f$ là toàn cấu khi và chỉ khi $Imf = R'$.

3.3. Tích của hai đồng cấu vành là đồng cấu vành. Đặc biệt, tích của hai đơn cấu(tương ứng, toàn cấu, đẳng cấu) vành cũng là đơn cấu(tương ứng, toàn cấu, đẳng cấu) vành.
Ánh xạ ngược của một đẳng cấu cũng là một đẳng cấu.

3.4. Cho đồng cấu vành $f: R \to R'$. Khi đó ánh xạ $\tilde{f}: R/kerf \to R'$ định bởi $\tilde{f}(x + Kerf) = f(x)$ là đơn cấu vành. Đặc biệt $R/ Kerf \cong Imf$.

3.5. Cho $R$ là trường với phần tử đơn vị $e$. Trong nhóm cộng $R$ nếu phần tử $e$ có cấp vô hạn thì ta nói rằng trường $R$ có đặc trưng 0 ( đặc số 0), ký hiệu $charR = 0$, nếu phần tử $e$ có cấp hữu hạn là $p$ thì ta nói trường $R$ có đặc trưng $p$ (đặc số $p$), ký hiệu $charR = p$.

3.6. Cho $R$ là miền nguyên và $\bar{R}$ là một trường. Ta nói $\bar{R}$ là *trường các thương* của miền nguyên R nếu tồn tại đơn cấu vành $f: R \to \bar{R}$ sao cho mọi phần tử của $\bar{R}$ đều có dạng

$f(a)f(b)^{-1}$ với $a, b \in R$, $b \neq 0$.

Trường các thương của miền nguyên $R$ luôn tồn tại và duy nhất ( sai khác một đẳng cấu).

## B. CÁC DẠNG BÀI TẬP CƠ BẢN

1. Dạng toán 1

a) Kiểm chứng một tập $X$ với hai phép toán cho trước có lập thành vành không.

- Nếu $X$ thỏa các yêu cầu trong 1.1 thì $X$ là vành. Xem Bài 2.1a)
- Nếu $X$ không thỏa yêu cầu nào đó trong 1.1 thì $X$ không là vành.

b) Kiểm chứng một tập $X$ với hai phép toán cho trước có lập thành miền nguyên không.

- Nếu $X$ thỏa các yêu cầu trong 1.3 thì $X$ là miền nguyên. Xem Bài 2.1b).
- Nếu $X$ không thỏa yêu cầu nào đó trong 1.3 thì $X$ không là miền nguyên. Xem Bài 2.1a).

c) Kiểm chứng một tập $X$ với hai phép toán cho trước có lập thành trường không.

- Nếu $X$ thỏa các yêu cầu trong 1.4 thì $X$ là trường. Xem Bài 2.1b).
- Nếu $X$ không thỏa yêu cầu nào đó trong 1.4 thì $X$ không là trường. Xem Bài 2.1a).

d) Kiểm chứng một tập con $A$ của vành $R$ có là vành con của $R$ không.

- Nếu $A$ thỏa các yêu cầu trong 2.3 thì $A$ vành con của $R$. Xem Bài 2.19.
- Nếu $A$ không thỏa yêu cầu nào đó trong 2.3 thì $A$ không là vành con

Kiểm chứng một tập con $A$ của vành $R$ có là ideal của $R$ không.
- Nếu $A$ thỏa các yêu cầu trong 2.4 thì $A$ là ideal. Xem Bài 2.12, 2.15a).
- Nếu $A$ không thỏa yêu cầu nào đó trong 2.4 thì $A$ không là ideal.

e) Kiểm chứng một tập con $A$ của vành $R$ có là ideal của $R$ không.
- Nếu $A$ thỏa các yêu cầu trong 2.4 thì $A$ là ideal. Xem Bài 2.12, 2.15a).
- Nếu $A$ không thỏa yêu cầu nào đó trong 2.4 thì $A$ không là ideal.

f) Kiểm chứng một tập con $A$ của trường $R$ có là trường con của $R$ không.
- Nếu $A$ thỏa các yêu cầu trong 2.5 thì $A$ trường con của $R$. Xem Bài 2.1g).
- Nếu $A$ không thỏa yêu cầu nào đó trong 2.5 thì $A$ không là trường con.

2. Dạng toán 2. Giải các phương trình trong vành số nguyên modulo $n$.

a) Phương trình $\bar{a}\,x = \bar{b}(trong\ \mathbb{Z}_n)$ với $(a, n) = 1$ có nghiệm duy nhất $x = (\bar{a})^{-1}\bar{b}$. Sử dụng thuật toán Euclid ta tìm được các số nguyên $u,v$ sao cho $au + nv = 1$. Suy ra $(\bar{a})^{-1} = \bar{u}$. Xem Bài 2.3a).

b) Phương trình $\bar{a}\,x = \bar{b}(trong\ \mathbb{Z}_n)$ với $(a, n) = d$ , $d$ là ước của $b$, có $d$ nghiệm. Chia cả hai vế của phương trình này cho $d$ ta đưa về phương trình dạng a). Xem bài 2.3c).

3. Dạng toán 3. Kiểm ánh xạ là đồng cấu, đơn cấu, toàn cấu vành.
Sử dụng 3.1. Xem Bài 2.21, 2.24.

4. Dạng toán 4. Tìm tất cả các tự đồng cấu của vành, của trường.
Sử dụng 3.1. Xem Bài 2.35.

5. Dạng toán 5. Chứng minh một tập là trường các thương của miền nguyên.
Sử dụng 3.6. Xem Bài 2.32.

## C. LỜI GIẢI HOẶC HƯỚNG DẪN ĐÁP SỐ CHƯƠNG 2

**Bài 2.1.**

a) $A \Delta B = (A \setminus B) \cup (B \setminus A)$ được gọi là *hiệu đối xứng* của $A$ và $B$.
Ta chứng minh hiệu đối xứng có tính chất kết hợp, nghĩa là $(A\Delta B)\Delta C = A\Delta(B\Delta C)$. Giả sử $x \in (A\Delta B)\Delta C$. Khi đó, ta có $x \in [(A\setminus B)\cup(B\setminus A)]\setminus C$ hoặc $x \in C\setminus[(A\setminus B)\cup(B\setminus A)]$. Nếu $x \in [(A\setminus B)\cup(B\setminus A)]\setminus C$ thì $x \in (A\setminus B)\cup(B\setminus A)$ và $x \notin C$. Tức là $x \in A\setminus B$, $x \notin C$ hoặc $x \in B\setminus A$, $x \notin C$. Trường hợp thứ nhất $x \in A$, $x \notin B$, $x \notin C$, do đó $x \in A$, $x \notin (B\setminus C)\cup(C\setminus B)$, tức là $x \in A\setminus[(B\setminus C)\cup(C\setminus B)]$, suy ra $x \in A\Delta(B\Delta C)$. Trường hợp thứ hai $x \in B$, $x \notin A$, $x \notin C$, do đó $x \in (B\setminus C)\cup(C\setminus B)$, $x \notin A$, tức là $x \notin [(B\setminus C)\cup(C\setminus B)]\setminus A$, suy ra $x \in A\Delta(B\Delta C)$. Như vậy $(A\Delta B)\Delta C \subseteq A\Delta(B\Delta C)$. Bao hàm thức ngược lại được chứng minh tương tự.

Dễ dàng kiểm tra được các đẳng thức sau đây

$A\Delta B = B\Delta A$

$A\Delta\varnothing = \varnothing\Delta A$

$A\Delta A = \varnothing$

$A\cap(B\cap C) = (A\cap B)\cap C$

$A\cap(B\Delta C) = (A\cap B)\Delta(A\cap C)$

Do đó $(\mathcal{P}(X),\Delta,\cap)$ là vành giao hoán có đơn vị là $X$. Mọi phần tử của $\mathcal{P}(X)$ khác không và khác đơn vị đều là ước của không, vì nếu $A\neq\emptyset$, $A\neq X$, thì $B= X\setminus A$ thỏa $AB =A\cap B =\emptyset$. Như vậy $\mathcal{P}(X)$ không phải là miền nguyên, do đó không phải là trường.

b) Xét $(\mathbb{Q}, \mathsf{T})$.

Dễ dàng thấy rằng phép toán T có tính giao hoán.
Tính kết hợp : $(x \mathsf{T} y) \mathsf{T} z = (x + y - 1) \mathsf{T} z = x + y + z - 2$
$x \mathsf{T} (y \mathsf{T} z) = x \mathsf{T} (y + z - 1) = x + y + z - 2$
Suy ra : $(x \mathsf{T} y) \mathsf{T} z = x \mathsf{T} (y \mathsf{T} z)$ .
Phần tử không của phép toán T là số 1. Phần tử đối của $x$ là $-x$ .

Xét $(\mathbb{Q},\perp)$. Ta có

$(x\perp y)\perp z = (x + y - xy)\perp z = x + y - xy + z - (x + y - xy)z = x + y + z - xy - xz - yz + xy$
$x \perp (y \perp z) = x \perp (y + z - yz) = x + y + z - xy - xz - yz + xy$
suy ra: $(x \perp y) \perp z = x \perp (y \perp z)$ .
Tính phân phối của phép $\perp$ đối với phép T
$(x \mathsf{T} y) \perp z = (x + y - 1) \mathsf{T} z = x + y - 1 + z - (x + y - 1)z = x + y + z - xz - yz + z - 1$ ;
$(x \perp z) \mathsf{T} (y \perp z) = (x + z - xz) \mathsf{T} (y + z - yz) = x + y - 1 + z - (x + y - 1)z = x + y + z - xz - yz + z - 1$ ;
Suy ra $(x \mathsf{T} y) \perp z = (x \perp z) \mathsf{T} (y \perp z)$
Tương tự $x \perp (y \mathsf{T} z) = (x \perp y) \mathsf{T} (x \perp z)$.
Vậy $(\mathbb{Q} , \mathsf{T}, \perp)$ là vành giao hoán. Dễ dàng thấy rằng vành này là có đơn vị là số hữu tỷ 0, mọi phần tử khác phần tử không đều khả nghịch, nghịch đảo của $x$ là $x' = \frac{x}{x-1}$.
Vậy $(\mathbb{Q} , \mathsf{T}, \perp)$ là trường, do đó nó là miền nguyên.

c) Xét $(\mathbb{R}^+, \mathsf{T})$.

Tập hợp số thực dương với phép nhân thông thường là nhóm con của nhóm nhân các số thực khác 0. Phần tử không của phép toán T là số thực 1. Phần tử đối của $x$ đối với phép toán T là $1/x$.

Xét $(\mathbb{R}^+,\perp)$. Ta có

$(x\perp y)\perp z = (x^{lny})\perp z = (x^{lny})^{lnz} = x^{lnylnz}$
$x \perp (y \perp z) = x \perp (y^{lnz}) = x^{lny^{lnz}} = x^{lnylnz}$
suy ra: $(x \perp y) \perp z = x \perp (y \perp z)$ .
Tính phân phối của phép $\perp$ đối với phép T
$(x \mathsf{T} y) \perp z = (xy) \mathsf{T} z = (xy)^{lnz} = x^{lnz}y^{lnz} = (x \perp z) \mathsf{T} (y \perp z)$
Tương tự $x \perp (y \mathsf{T} z) = (x \perp y) \mathsf{T} (x \perp z)$.
Vậy $(\mathbb{R}^+ , \mathsf{T}, \perp)$ là vành giao hoán. Dễ dàng thấy rằng vành này là có đơn vị là số $e$, mọi phần tử khác phần tử không đều khả nghịch, nghịch đảo của $x$ là $x' = e^{\frac{1}{lnx}}$.

Vậy $(\mathbb{R}^+, \mathsf{T}, \perp)$ là trường, do đó nó là miền nguyên.

d) Xét $(\mathbb{R}, \mathsf{T})$. Dễ dàng thấy rằng phép toán T có tính giao hoán.

Tính kết hợp : $(x \mathsf{T} y) \mathsf{T} z = \sqrt[n]{x^n + y^n} \mathsf{T}\, z = \sqrt[n]{x^n + y^n + z^n}$

$x \mathsf{T} (y \mathsf{T} z) = x \mathsf{T} \sqrt[n]{y^n + z^n} = \sqrt[n]{x^n + y^n + z^n}$

Suy ra : $(x \mathsf{T} y) \mathsf{T} z = x \mathsf{T} (y \mathsf{T} z)$ .

Phần tử không của phép toán T là số 0. Phần tử đối của $x$ là $-x$ .

Xét $(\mathbb{R}, \perp)$. Ta có

$(x \perp y) \perp z = (xy) \perp z = xyz$

$x \perp (y \perp z) = x \perp (yz) = xyz$

suy ra: $(x \perp y) \perp z = x \perp (y \perp z)$ .

Tính phân phối của phép $\perp$ đối với phép T

$(x \mathsf{T} y) \perp z = \sqrt[n]{x^n + y^n} \mathsf{T}\, z = \sqrt[n]{x^n + y^n}\ z$

$(x \perp z) \mathsf{T} (y \perp z) = xz \mathsf{T}\, yz = \sqrt[n]{(xz)^n + (yz)^n} = \sqrt[n]{x^n + y^n} \mathsf{T}\, z$ (do $n$ là số nguyên dương lẻ).

$(x \mathsf{T} y) \perp z = (x \perp z) \mathsf{T} (y \perp z)$

$x \perp (y \mathsf{T} z) = x(y \mathsf{T} z) = x\sqrt[n]{y^n + z^n}$

$(x \perp y) \mathsf{T} (x \perp z) = xy \mathsf{T}\, xz = \sqrt[n]{(xz)^n + (yz)^n} = x\sqrt[n]{y^n + z^n}$ .

Vậy $(\mathbb{R}, \mathsf{T}, \perp)$ là vành giao hoán. Dễ dàng thấy rằng vành này là có đơn vị là 1, mọi phần tử khác 0 đều khả nghịch. Vậy $(\mathbb{R}, \mathsf{T}, \perp)$ là trường, do đó nó là miền nguyên.

f) Nếu $(a_1 + b_1\sqrt{2})$ , $(a_2 + b_2\sqrt{2})$ thuộc $\mathbb{Z}(\sqrt{2})$ thì

$(a_1 + b_1\sqrt{2}) - (a_2 + b_2\sqrt{2}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{2}$ và

$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2 + (a_1b_2 + b_1a_2)\sqrt{2}$ thuộc $\mathbb{Z}(\sqrt{2})$

Do đó $\mathbb{Z}(\sqrt{2})$ là vành con của trường số thực $\mathbb{R}$. Đương nhiên nó là vành giao hoán, có đơn vị và không có ước của không, nghĩa là $\mathbb{Z}(\sqrt{2})$ là miền nguyên.

Tuy nhiên $\mathbb{Z}(\sqrt{2})$ không phải là trường vì nghịch đảo của $\sqrt{2}$ không thuộc $\mathbb{Z}(\sqrt{2})$ .

g) $\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \right\}$

Với mọi $x, y \in \mathbb{Q}(\sqrt{2})$ , $x = a + b\sqrt{2}, y = c + d\sqrt{2} (a, b, c, d \in \mathbb{Q})$ ta có:

$x - y = (a - c) + (b - d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ , $xy = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

nếu $x = a + b\sqrt{2} \neq 0$ thì $a - b\sqrt{2} \neq 0$ (vì nếu không thì $a = b = 0$ hoặc $a, b \neq 0, \sqrt{2} = ab^{-1}$ ,vô lý). Suy ra $x^{-1} = (a + b\sqrt{2})^{-1} = (a - b\sqrt{2})(a^2 - 2b^2) \in \mathbb{Q}(\sqrt{2})$ .

Do đó $\mathbb{Q}(\sqrt{2})$ là một trường con của trường $\mathbb{R}$ ,và hiển nhiên nó cũng là vành,miền nguyên.

h) Ta có $K \subset M(2,\mathbb{Q})$

Với mọi $x, y \in K, x = \begin{pmatrix} a & b \\ 4b & a \end{pmatrix}, y = \begin{pmatrix} c & d \\ 4d & c \end{pmatrix}, (c,d \in \mathbb{Q})$

Ta có: $x - y = \begin{pmatrix} a-c & b-d \\ 4(b-d) & a-c \end{pmatrix} \in K$, $xy = \begin{pmatrix} ac+4bd & ad+bc \\ 4(ad+bc) & ac+bd \end{pmatrix} \in K$

Do đó $K$ là một vành con của vành $M(2,\mathbb{Q})$.

Xét $x = \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix}, y = \begin{pmatrix} -2 & 1 \\ 4 & -2 \end{pmatrix}$.Ta có $0 \neq x, y \in K$ nhưng $xy = 0$. Như vậy $K$ có ước của 0 nên nó không phải là miền nguyên hay trường.

i) Ta có:hiệu, tích của hai ma trận(tương ứng, ma trận chéo; ma trận tam giác trên; ma trận tam giác dưới; ma trận tam giác trên ngặt; ma trận tam giác dưới ngặt)vuông cấp $n \geq 2$ cũng là matrận có dạng tương ứng. Do đó nó là vành con của vành các ma trận vuông cấp $n \geq 2$.

Mặt khác phép nhân matrận không có tính chất giao hoán. Do đó các tập trên không phải là miền nguyên, không phải là trường.

j) Nếu $\begin{pmatrix} a & b \\ 6b & a \end{pmatrix}, \begin{pmatrix} c & d \\ 6d & c \end{pmatrix} \in F$ thì

$$\begin{pmatrix} a & b \\ 6b & a \end{pmatrix} + \begin{pmatrix} c & d \\ 6d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ 6(b+d) & a+c \end{pmatrix} \in F$$

$$\begin{pmatrix} a & b \\ 6b & a \end{pmatrix}\begin{pmatrix} c & d \\ 6d & c \end{pmatrix} = \begin{pmatrix} ac+6bd & ad+bc \\ 6bc+6ad & 6bd+ac \end{pmatrix} \in F$$

Vậy $F$ là vành con của vành matrận vuông cấp hai, phép nhân matrận trong $F$ không có tính chất giao hoán, do đó $F$ không thể là miền nguyên hay trường.

k) Kiểm tra $\mathbb{C}$ là vành như các phần trước.

Phép nhân có tính giao hóan, nhận (1,0) là phần tử đơn vị, hơn nữa mỗi phần tử $(x,y)$ đều có phần tử nghịch đảo là $\left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right)$.

Do đó $\mathbb{C}$ là một trường.

**Bài 2.2**

Gọi $e$ là phần tử đơn vị trái duy nhất của $R$, ta có $ex = x$ với mọi $x$ thuộc $R$.

Xét $x$ thuộc $R$, ta chứng minh $xe - x + e$ cũng là phần tử đơn vị trái của $R$. Thật vậy, với mọi $y$ thuộc $R$, ta có

$$(xe - x + e)y = xey - xy + y = xy - xy + y = y$$

nên $xe - x + e$ là phần tử đơn vị trái của $R$.

Do tính duy nhất của $e$ nên ta có $xe - x + e = e$ hay $xe = x$ với mọi $x$ thuộc $R$.

Suy ra $xe = ex = x$ với mọi $x$ thuộc $R$ nên $R$ có phần tử đơn vị là $e$.

**Bài 2.3** Giải phương trình:

$a)\quad 21\overline{x} + \overline{24} = \overline{103} \pmod{103} \Leftrightarrow \overline{21x} = \overline{77} \pmod{103} \quad (*)$

$1 = 19 - 9.2 \quad (1)$

$2 = 21 - 19.1 \quad (2)$

$19 = 103 - 21.4 \quad (3)$

Thế $(2)$ vào $(1)$, ta được: $1 = 19 - 9(21 - 19.1) = 10.19 - 9.21 \quad (4)$

Thế $(3)$ vào $(4)$, ta được: $1 = 10(103 - 21.4) - 9.21 = -49.21 + 10.103$

$Suy\ ra\ \overline{1} = \overline{-49.21 + 10.103} = \overline{-49.21} + \overline{10.103} = \overline{-49}.\overline{21} + \overline{10}.\underbrace{\overline{103}}_{\overline{0}} =$

$\overline{-49}.\overline{21}$. Do đó $\overline{21}^{-1} = \overline{-49}$.

$(*) \Leftrightarrow \overline{x} = \overline{77}.\overline{21}^{-1} = \overline{77}.\overline{-49} = \overline{-3773} = \overline{38}$.

$b)\quad 68(\overline{x} + \overline{24}) = \overline{102} \pmod{492} \Leftrightarrow \overline{68x} + \overline{68}.\overline{24} = \overline{102} \pmod{492}$

$\Leftrightarrow \overline{68x} = \overline{-1530} \pmod{492} \Leftrightarrow \overline{68x} = \overline{-54} \pmod{492} \Leftrightarrow \overline{34x} = \overline{-27} \pmod{246}$.

$\Leftrightarrow 34x + 27 \vdots 246$. Suy ra $2|(34x + 27)$. Do đó $2|27$ (Vôlý).

Vậy phương trình vô nghiệm.

$c)\quad \overline{78x} - \overline{13} = \overline{35} \pmod{666} \Leftrightarrow \overline{78x} = \overline{48} \pmod{666} \Leftrightarrow \overline{13x} = \overline{8} \pmod{111} \quad (*)$

$1 = 7 - 6.1 \quad (1)$

$6 = 13 - 7.1 \quad (2)$

$7 = 111 - 13.8 \quad (3)$

Thế $(2)$ vào $(1)$, ta được: $1 = 7 - (13 - 7) = 2.7 - 13 \quad (4)$

Thế $(3)$ vào $(4)$, ta được: $1 = 2(111 - 13.8) - 13 = -17.13 + 2.111$

Ta có $\overline{1} = \overline{-17.13 + 2.111} = \overline{-17.13} + \overline{2.111} = \overline{-17}.\overline{13} + \overline{2}.\underbrace{\overline{111}}_{\overline{0}} = \overline{-17}.\overline{13}$

Do đó $\overline{13}^{-1} = \overline{-17}$.

$(*) \Leftrightarrow \overline{x} = \overline{-17}.\overline{8} = \overline{-136} = \overline{86}$.

**Bài 2.4**

a)

Theo phép chia Euclide, ta có:

$133 = 4.27 + 25,$

$27 = 1.25 + 2,$

$25 = 12.2 + 1,$

$2 = 1.2 + 0.$

Do đó $1 = 25 - 12.2 = 25 - 12.(27 - 1.25) = 13.25 - 12.27$

$= 13.(133 - 4.27) - 12.27 = 13.133 - 64.27$. Suy ra

$27.(-64) \equiv 1 \pmod{133}$

$\Leftrightarrow$ 27.(-64).18 $\equiv$18 (mod 133)
$\Leftrightarrow$ 27.45 $\equiv$18 (mod 133).
Từ đó ta có: (27n – 18) ⋮ 133 $\Leftrightarrow$(27.$n$ – 27.45) ⋮ 133
$\Leftrightarrow$27.($n$ – 45) ⋮ 133
$\Leftrightarrow$($n$ – 45) ⋮ 133 ( do (27,133)=1 )
Vậy tập hợp các giá trị của $n$ thỏa yêu cầu là 45 + 133$\mathbb{Z}$

b)
Để 92$n$ + 18 chia hết cho 100 thì 92$n$ + 18 phải chia hết cho 4. Mà ta có 92 chia hết cho 4 và 18 không chia hết cho 4 nên 92$n$ + 18 không chia hết cho 4, do đó không tồn tại số nguyên $n$ nào thỏa yêu cầu đề bài.

d) 95$n$ – 15 ⋮ 335 $\Leftrightarrow$ 19$n$ – 3 ⋮ 67
Thực hiện tương tự như câu a) ta được tập hợp các giá trị của $n$ thỏa yêu cầu là 46 + 67$\mathbb{Z}$

**Bài 2.5**

a) Với mọi $x\in R$ ta có
$-x = (-x)^2 = x^2 = x$.

b) Với mọi $x, y \in R$ ta có
$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$ . Suy ra $xy + yx = 0$. Do đó $xy = - yx = yx$.

c) Giả sử $x\in R, x \neq 0$. Với $y$ là phần tử tùy ý của $R$ ta có $xy = x^2 y = x(xy)$. Vì $R$ không có ước của không nên ta có thể giản ước cho $x$ ở hai vế của đẳng thức trên và ta được $xy = y$. Như vậy $x$ là phần tử đơn vị của $R$. Suy ra $R$ chỉ gồm hai phần tử là phần tử không và phần tử đơn vị.

**Bài 2.6**

Từ giả thiết suy ra $x^4 = x^2$ với mọi $x$ thuộc $R$ . Đặt $t = x^2$ , ta có $t^2 = t$ .
Ta thấy với $y$ thuộc $R$ thì
$(yt – tyt)^2 = ytyt – yttyt – tytyt + tyttyt = ytyt – ytyt –tytyt + tytyt = 0$
nên $(yt – tyt) = (yt – tyt)^3 = 0$ hay $yt = tyt$ .
Tương tự ta cũng có $ty = tyt$ . Suy ra $ty = yt$ hay $x^2y = yx^2$.
Từ đó ta có
$xy = (xy)^3 = xyxyxy = x(yx)^2y = xy(yx)^2 = xy^2xyx = y^2xxyx = y^2x^2yx = y^3x^3 = yx$
với mọi $x$ , $y$ thuộc $R$.Vậy $R$ là vành giao hoán .

**Bài 2.7**

a)
Hiển nhiên $C(a) \subset R$ và $a \in C(a)$. Với mọi $z, t \in C(a)$ ta có:
$a(zt) = (az)t = (za)t = z(at) = z(ta) = (zt)a$ . Do đó $zt \in C(a)$.
$a(z - t) = az - at = za - ta = (z - t)a$. Do đó $z - t \in C(a)$.
Suy ra $C(a)$ là vành con của $R$ có chứa $a$.

b) Dễ thấy $C(R)$ là một tập con khác rỗng của $R$.

Giả sử $a, b \in C(R)$, khi đó hiển nhiên $ab = ba$ , hơn nữa với mọi $x \in C(R)$ ta có
$(a-b)x = ax - bx = xa - xb = x(a-b)$,
$(ab)x = a(bx) = a(xb) = x(ab)$.
Vậy $a-b, ab \in C(X)$. Do đó $C(R)$ là vành con giao hoán của $R$.

c) Gọi $I_n$ là matrận đơn vị cấp $n$. Dễ dàng thấy rằng $aI_n \in C(M(n,\mathbb{R}))$ với mọi $a \in \mathbb{R}$. Gọi $A$ là một ma trận thuộc $C(M(n,\mathbb{R}))$. Gọi $T_{ij}$ là matrận có các phần tử trên đường chéo chính và ở vị trí $(i, j)$ bằng 1 còn các vị trí còn lại đều bằng 0. Vì $T_{ij}A = AT_{ij}$ suy ra $a_{ij} = 0$ và $a_{ii} = a_{jj}$. Vậy $A = aI_n$ với $a$ thuộc $\mathbb{R}$ .

Vậy $C\big(M(n,\mathbb{R})\big) = \{aI_n \mid a \in \mathbb{R}\}$ .

**Bài 2.8**

$(e - yu^{-1}x)(e + yx) = e + yx - yu^{-1}x - yu^{-1}xyx = e + yx - y(u^{-1} + u^{-1}xy)x = e + yx - y\big(u^{-1}(e + xy)\big)x = e + yx - yex = e + yx - yx = e.$
Tương tự $(e + yx)(e - yu^{-1}x) = e.$

**Bài 2.9**

Nếu $I = R$ thì đương nhiên $I$ chứa đơn vị $e$ của $R$. Đảo lại, giả sử $I$ là ideal chứa đơn vị $e$ của $R$. Với mọi $x \in R$ ta có $x = xe \in I$, suy ra $R \subseteq I$, do đó $I = R$. Khẳng định vẫn còn đúng khi $I$ là ideal trái, ideal phải, nhưng không đúng khi $I$ là vành con mà không phải là ideal hay ideal trái, phải. Chẳng hạn $\mathbb{Z}$ là vành con chứa đơn vị của $\mathbb{Q}$, nhưng $\mathbb{Z}$ không trùng với $\mathbb{Q}$.

**Bài 2.10**

Hiển nhiên $I + J \subset R$ . Xét $x + y$ và $x' + y' \in I + J$ và $r \in R$.
Ta thấy $(x + y) - (x' + y') = (x - x') + (y - y') \in I + J$ ,
$r(x + y) = rx + ry \in I + J$,
$(x + y)r = xr + yr \in I + J$.
Suy ra $I + J$ cũng là ideal của $R$.

Nếu $R = \mathbb{Z}$ , $I = m\mathbb{Z}$ , $J = n\mathbb{Z}$ thì theo kết quả Bài 1.16b , ta có $I + J = (m,n)\,\mathbb{Z}$ .

**Bài 2.11**

a) Ta có: IJ $\neq \phi$ vì $0 \in$ IJ.
Đặt $u = \sum_{i=1}^{n} x_i y_i \in IJ$ và $v = \sum_{i=1}^{m} z_i t_i \in IJ$.
Khi đó $u - v = \sum_{i=1}^{n} x_i y_i - \sum_{j=1}^{m} z_j t_j = \sum_{i=1}^{n} x_i y_i + \sum_{j=1}^{m} (-z_j) t_j \in IJ$.
Với $r \in R$, ta có:
$ru = r\sum_{i=1}^{n} x_i y_i = \sum_{i=1}^{n} r(x_i y_i) = \sum_{i=1}^{n} (rx_i) y_i \in IJ$,
$ur = (\sum_{i=1}^{n} x_i y_i) r = \sum_{i=1}^{n} (x_i y_i) r = \sum_{i=1}^{n} x_i (y_i r) \in IJ$.
Vậy $IJ$ là một ideal của $X$.

b) IJ $= \{\sum_{i=1}^{q} x_i y_i \mid q \in \mathbb{N}, x_i \in mZ, y_i \in nZ\}$
$= \{\sum_{i=1}^{q} mk_i nl_i \mid q \in \mathbb{N}, k_i \in Z, l_i \in Z\}$

$= \{\sum_{i=1}^{q} m\, n\, h_i | q \in \mathbb{N}, h_i \in Z\}$
$= \{mn \sum_{i=1}^{q} h_i | q \in \mathbb{N}, h_i \in Z\}$.

Trong đó các $h_i$ có dạng tích $k_i l_i$. Từ đẳng thức trên suy ra $IJ$ là tập con của $mn\mathbb{Z}$, hơn nữa với mọi số nguyên có dạng $mnl$, ta có $mnl = (m.1)(n.l)$ thuộc $IJ$. Vậy $IJ = mn\mathbb{Z}$.

**Bài 2.12**

Với $x,y \in I$, ta có : $nx = 0$ và $ny = 0$, ta có $nx - ny = 0 \Rightarrow n(x - y) = 0$ .
Suy ra $x - y \in I$.
Với $r \in R, x \in I$, ta có : $n(rx) = r(nx) = r.0 = 0$ ,$n(xr) = (nx).r = 0.r = 0$.
Do đó $rx$ và $xr$ đều thuộc $I$. Như vậy, $I$ là ideal của $R$.

**Bài 2.13**

$\forall ax,ay \in aR$ ta có : $ax-ay = a(x-y) \in aR$ và
$\forall r \in R, ax \in aR$ : $(ax)\, r = a(xr) \in aR$ .Vậy $aR$ là ideal phải của $R$.
Tương tự ta cũng có $Ra$ là 1 ideal trái của $R$.
Nếu $R$ giao hoán thì $Ra = aR$. Suy ra : $Ra = aR$ là ideal của $R$.
Nếu $R$ giao hoán, có đơn vị thì ideal chính sinh bởi $a$ là $<a> = Ra = aR$ .

**Bài 2.14**

a) Hiển nhiên $aR \subset R$ .
Nếu $a$ khả nghịch phải thì tồn tại $b$ thuộc $R$ sao cho $ab = e$. Khi đó với mọi $r$ thuộc $R$, ta có $r = er = (ab)r = a(br) \in aR$ , suy ra $R \subset aR$ . Vậy $R = aR$ .
Nếu $aR = R$ thì tồn tại $b$ sao cho $ab = e$ hay $a$ khả nghịch phải .
b) Hiển nhiên $aR \subset R$ .
Nếu $a$ khả nghịch trái thì tồn tại $b$ thuộc $R$ sao cho $ba = e$. Khi đó với mọi $r$ thuộc $R$ , ta có $r = re = r(ba) = (rb)a \in Ra$ , suy ra $R \subset Ra$ . Vậy $R = Ra$ .
Nếu $Ra = R$ thì tồn tại $b$ sao cho $ba = e$ hay $a$ khả nghịch trái .
c) Suy ra từ a) và b).

**Bài 2.15**

a) $Ann(a) \neq \emptyset$ vì $0 \in Ann(a)$.
Với $u, v \in Ann(a), r \in R$ ta có
$a(u - v) = au - av = 0$ . Do đó $u - v \in Ann(a)$.
$a(ru) = a(ur) = (au)r = 0$ . Do đó $ru \in Ann(a)$ . Vậy $Ann(a)$ là ideal của $R$.
b)

$Ann(\bar{4}) = \{\bar{x} \in \mathbb{Z}_{32} \mid \bar{4}\bar{x} = 0\} = \{\bar{x} \in \mathbb{Z}_{32} \mid 4x \equiv 0 (mod 32)\} =$

$\{\bar{x} \in \mathbb{Z}_{32} \mid x \equiv 0 (mod 8)\} = \{\bar{0}, \bar{8}, \overline{16}, \overline{24}\}$.

**Bài 2.16**

a) Do $x$ lũy linh nên tồn tại số nguyên dương $n$ thỏa $x^n = 0$
Ta có $e = e + x^{2n+1}$ (do $x^{2n+1} = x^n\, x^{n+1} = 0$)
$= (e + x).(e - x + x^2 - \ldots + x^{2n})$

$= (e - x + x^2 - \ldots + x^{2n}).(e + x).$

Vậy $e + x$ khả nghịch phải và khả nghịch trái, do đó $e + x$ khả nghịch.

b) Do $R$ giao hoán nên $(x.u^{-1})^n = x^n.u^{-n} = 0.$

Theo câu a) thì $e + x.u^{-1}$ khả nghịch. Gọi nghịch đảo của nó là $a$.

Ta có $e = (e + x.u^{-1})a$

$= (u.u^{-1} + x.u^{-1})a$

$= (u + x)u^{-1}a.$

Do đó $u + x$ khả nghịch phải, tương tự ta cũng có $u + x$ khả nghịch trái.

Vậy $u + x$ khả nghịch.

c)

i) Chứng minh $N(R)$ là idean của $R$.

Dễ thấy $N(R) \neq \varnothing$ do $0 \in N(R)$. Với mọi $x, y \in N(R)$ và $r \in R$, ta có 2 số nguyên dương $m, n$ thỏa $x^m = y^n = 0$. Khi đó

$$(x-y)^{m+n} = \sum_{k=0}^{m+n} (-1)^k . C_{m+n}^k x^k y^{m+n-k}$$

Trong tổng trên $0 \leq k \leq m + n$. Nếu $k \geq n$ thì $x^k = 0$, nếu $k < n$ thì $m + n - k > m$ nên $y^{m+n-k} = 0$. Do đó $x^k y^{m+n-k} = 0 \quad \forall k = \overline{0, m+n}$

Từ đó suy ra $(x-y)^{m+n} = 0$. Vậy $x - y$ lũy linh.

Do $R$ giao hoán nên $(xr)^n = x^n.r^n = 0$ . Vậy $xr$ lũy linh. Suy ra $N(R)$ là idean của $R$.

ii)

Gọi $\bar{x}$ là một phần tử lũy linh của $R/N(R)$.Tồn tại một số nguyên dương $n$ sao cho $(\bar{x})^n = \bar{0}$

$(\bar{x})^n = \bar{0} \Leftrightarrow \overline{x^n} = \bar{0} \Leftrightarrow x^n \in N(R) \Leftrightarrow \exists m, (x^n)^m = 0 \Leftrightarrow x \in N(R) \Leftrightarrow \bar{x} = \bar{0}$

Từ đó suy ra điều phải chứng minh.

**Bài 2.17**

a) Chứng minh $R \times \mathbb{Z}$ là vành có đơn vị:

Theo Ví dụ 1.3 thì $(R \times \mathbb{Z}, +)$ là nhóm Abel.

Với mọi $x, y, z \in R$ và $m, n, p \in \mathbb{Z}$, ta có

$$\begin{aligned}
((x,m)(y,n))(z,p) &= (xy + my + nx, mn)(z,p) \\
&= ((xy + my + nx)z + mnz + p(xy + my + nz), mnp) , \\
(x,m)((y,n)(z,p)) &= (x,m) + (yz + nz + py, np) \\
&= (x(yz + nz + py) + m(yz + nz + py) + npx, mnp) . \\
((x,m) + (y,n))(z,p) &= (x+y, m+n)(z,p) \\
&= ((x+y)z + (m+n)z + p(x+y), (m+n)p) \\
(x,m)(z,p) + (y,n)(z,p) &= (xz + mz + px, mp) + (yz + nz + py, np) \\
&= ((x+y)z + (m+n)z + p(x+y), (m+n)p)
\end{aligned}$$

Vậy $((x,m) + (y,n))(z,p) = (x,m)(z,p) + (y,n)(z,p)$.

Tương tự ta cũng chứng minh được:

$(x,m)((y,n) + (z,p)) = (x,m)(y,n) + (x,m)(z,p)$

Phần tử đơn vị của $R \times \mathbb{Z}$ là e = (0,1) .

Ta suy ra $R \times \mathbb{Z}$ là vành giao hoán có đơn vị.

b) Chứng minh ánh xạ $f : x \mapsto (x, 0)$ là đơn cấu.

$f(x+y) = (x+y,0) = (x,0) + (y,0) = f(x) + f(y)$

$f(xy) = (xy,0) = (xy + 0y + 0x,0) = (x,0)(y,0) = f(x)f(y)$.

$\ker f = \{x \in R | f(x) = (x,0) = (0,0)\}$

$= \{0\}$.

Vậy $f$ là đơn cấu.

**Bài 2.18**

a) Giả sử $X$ là vành có đơn vị $e$ và có $p$ phần tử với $p$ nguyên tố. Khi đó $(X,+)$ là nhóm cyclic nên nó sinh bởi một phần tử bất kì khác 0 . Ta thấy nếu $e = 0$ thì với mọi $x$ thuộc $X$ , $x = xe = x0 = 0$ nên nhóm $(X , + )$ chỉ có 1 phần tử, trái giả thiết , suy ra $e$ khác 0 .Vậy $X = \langle e \rangle = \{ 0 , e , 2e , ... , (p-1)e \}$.

Khi đó ta thiết lập tương ứng $f : \mathbb{Z}_p \to X$

$\bar{k} \mapsto ke$

Hiển nhiên $f$ là ánh xạ và là toàn ánh . Hơn nữa $f(\bar{k} + \bar{h}) = (k + h)e = ke + he = \bar{k}\,e + \bar{h}\,e = f(\bar{k}) + f(\bar{h})$ nên $f$ là đồng cấu . Lại có $\ker f = \{\bar{k} \in \mathbb{Z}_p \mid ke = 0 = \bar{0}$ nên $f$ là đơn cấu . Suy ra $f$ là đẳng cấu nên $\mathbb{Z}_p \cong X$ .

b) Nếu $m$ không nguyên tố thì $m = nk$ ( $1 < n , k < m$ ).

Giả sử $(n,k) > 1$, khi đó theo kết quả Bài 1.35 thì $\mathbb{Z}_m$ là nhóm cyclic nhưng $\mathbb{Z}_n \times \mathbb{Z}_k$ không cyclic .Vì vậy $\mathbb{Z}_m$ không đẳng cấu với $\mathbb{Z}_n \times \mathbb{Z}_k$ .

**Bài 2.19** .

Vì $f(0) = 0$ nên $I \neq \varnothing$. Với mọi $a, b \in I$, ta có

$f( a - b ) = f(a) + f(-b) = a - b$ ,

$f(ab) = f(a)f(b) = ab$,

suy ra $a – b$ và $ab \in I$. Vậy $I$ là vành con của $R$.

**Bài 2.20**

a) $T$ là vành tích trực tiếp của các vành $R$ và $S$ ( xem Ví dụ 1.3).

b) Với $(a, 0), (b, 0) \in \bar{R}$, $(x, y) \in T$ ta có

$(a,0) - (b,0) = (a - b,0) \in \bar{R}, (a,0)(b,0) = (ab,0) \in \bar{R},$

$(x,y)(a,0) = (xa,0) \in \bar{R}, (a,0)(x,y) = (ax,0) \in \bar{R}.$

Suy ra $\bar{R}$ là ideal của $T$. Ánh xạ $R \to \bar{R}$, xác định bởi $a \mapsto (a, 0)$ là đẳng cấu.

c) Theo định nghĩa ta có $\bar{R} \cap \bar{S} = 0$. Ngoài ra nếu $(x, y) \in T$ thì

$(x, y) = (x, 0) + (0, y) \in \bar{R} + \bar{S}$. Nên $T = \bar{R} + \bar{S}$.

d) Đơn vị của $T$ là $(e_R, e_S)$.

**Bài 2.21**

a)

• Với mọi $f, g, h \in E$ ta có:

$$\left[(f+g)+h\right](x) = (f+g)(x) + h(x) = f(x) + g(x) + h(x) = f(x) + (g+h)(x) = \left[f + (g+h)\right](x)$$

$$;(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x), \forall x \in R$$

cho nên $(f+g)+h = f+(g+h)$, và $f+g = g+f$.

Gọi $(-f)$ là ánh xạ định bởi $(-f)(x) = -f(x), \forall x \in R$ ta có được $(-f) \in E$,

$f + 0 = f, f + (-f) = 0$ (trong đó 0 là ánh xạ không).

Suy ra $(E, +)$ là một nhóm Abel.

• Với mọi $f, g, h \in E$ ta có :

$$\left[(fg)h\right](x) = (fg)(h(x)) = f\left[g(h(x))\right] = f\left[(gh)(x)\right] = \left[f(gh)\right](x), \forall x \in R$$

cho nên $(fg)h = f(gh)$.

Suy ra $(E, .)$ là một nửa nhóm.

• Với mọi $f, g, h \in E$ ta có:

$$\left[f(g+h)\right](x) = f\left[(g+h)(x)\right] = f(g(x) + h(x)) = f(g(x)) + f(h(x)) = (fg)(x) + (fh)(x) = (fg + fh)(x)$$

và

$$\left[(g+h)f\right](x) = (g+h)(f(x)) = g(f(x)) + h(f(x)) = (gf)(x) + (hf)(x) = (gf + hf)(x),$$

$\forall x \in R$

Suy ra: $f(g+h) = fg + fh, (g+h)f = gf + hf$ .Tức là phép nhân phân phối đối với phép cộng. Vậy $(E, +)$ là một vành.

b)

Nếu $x = y \in R$ thì $h_a(x) = a\,x = ay = h_a(y) \in R$ , nên $h_a$ là ánh xạ từ $(R, +)$ vào $(R, +)$.

Với mọi $x, y \in R$ ta có $h_a(x+y) = a(x+y) = ax + ay = h_a(x) + h_a(y)$. Suy ra $h_a$ là một tự đồng cấu của nhóm cộng Abel $R$.

c)

Nếu $a = b \in R$ thì ta có $h_a(x) = a.x = bx = h_b(x), \forall x \in R$ nên $h_a = h_b$ hay $h(a) = h(b)$ , do đó $h$ là ánh xạ từ vành $R$ vào vành $E$.

Với mọi $a, b \in R$ ta có :

$$h_{a+b}(x) = (a+b)x = ax + bx = h_a(x) + h_b(x) = (h_a + h_b)(x)$$

$$h_{ab}(x) = (ab)x = a(bx) = a(h_b(x)) = h_a(h_b(x)) = h_a h_b(x), \forall x \in R$$ .Suy ra $h_{a+b} = h_a + h_b$ và $h_{ab} = h_a h_b$ .Hay $h(a+b) = h(a) + h(b)$ và $h(ab) = h(a)h(b)$.

Vậy $h$ là đồng cấu vành từ $R$ vào $E$.

d)

Ta có $K\text{erh} = \{b \in R \mid h(b) = h_b = 0\} = \{b \in R \mid bx = 0, \forall x \in R\}$.
Nếu $R$ có đơn vị là $e$ thì với $b \in \text{Kerh}$ ta có $b = be = 0$. Ngược lại khi $b = 0$ thì $bx = 0, \forall x \in R$.Vậy nếu $R$ có đơn vị thì Ker$h$=$\{b \in R \mid bx = 0, \forall x \in R\} = \{0\}$ do đó $h$ là đơn cấu.

**Bài 2.22**

a) Giả sử $n$ không nguyên tố , khi đó $n = mk$ ( $1 < m$ , $k < n$).
Khi đó $ne = (mk)e = (me)(ke) = 0$ , và do $R$ là miền nguyên nên $me = 0$ hoặc $ke = 0$ , trái giả thiết của $n$ . Vậy $n$ nguyên tố.

b) Xét $x$ khác 0 , ta có $nx = (ne)x = 0$. Hơn nữa nếu $kx = 0$ thì $0 = kx = k(ex) = (ke)x$ và do $R$ là miền nguyên nên $ke = 0$, suy ra $k \vdots n$ .Vậy cấp của mọi phần tử khác không của $R$ đều là $n$ .

b) Ta chứng minh $mR$ là ideal của $R$ . Hiển nhiên $\varnothing \neq mR \subset R$ . Với $mx$ , $my \in mR$ và $r \in R$ thì $mx - my = m(x-y) \in mR$ , $r(mx) = m(rx) \in mR$, $(mx)r = m(xr) \in mR$ . Do đó $mR$ là ideal của $R$.
Nếu $m \vdots n$ thì $mR = \{0\}$. Suy ra $R / mR \cong R$.
Nếu $m$ không chia hết cho $n$ thì $(m,n) = 1$ do $n$ nguyên tố. Suy ra tồn tại $u$ và $v$ nguyên sao cho $mu + nv = 1$. Với $a \in R$ thì $a = (mu + nv)a = mua + nva = mua \in mR$ ( do $nva = 0$ ), suy ra $a \in mR$ . Vậy $mR = R$ .Từ đó $R / mR \cong \{0\}$.

**Bài 2.23**

a) Chứng minh$\mathbb{Q}(\sqrt{2})$ là trường con của $\mathbb{C}$

$\mathbb{Q}(\sqrt{2})$ khác rỗng vì 0 thuộc $\mathbb{Q}(\sqrt{2})$, $\mathbb{C}$ chứa $\mathbb{Q}(\sqrt{2})$. Với mọi $x,y \in \mathbb{Q}(\sqrt{2})$, ta có

$x = a+b\sqrt{2}$ và $y=c+d\sqrt{2}$,trong đó $a, b, c, d \in \mathbb{Q}$. Khi đó

$x-y = (a-c)+ (b-d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ (vì $a-c \in \mathbb{Q}$ và $b-d \in \mathbb{Q}$).

Nếu $y = c+d\sqrt{2} \neq 0$ thì $c-d\sqrt{2} \neq 0$. Vì nếu $c- d\sqrt{2} = 0$ thì $c = 0$ và $d = 0$, suy ra $c+d\sqrt{2} = 0$ (trái giả thiết).

Ta có

$$xy^{-1} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{c^2-2d^2} = \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

( vì $\frac{ac-2bd}{c^2-2d^2} \in \mathbb{Q}$ và $\frac{bc-ad}{c^2-2d^2} \in \mathbb{Q}$).
Vậy $\mathbb{Q}(\sqrt{2})$ là trường con của $\mathbb{C}$.

Tương tự $\mathbb{Q}(i)$ là trường con của $\mathbb{C}$.

b) Chứng minh $\mathbb{Q}(i)$ và $\mathbb{Q}(\sqrt{2})$ không đẳng cấu với nhau

Giả sử tồn tại đẳng cấu $f$: $\mathbb{Q}(i) \to \mathbb{Q}(\sqrt{2})$. Đặt $f(i) = a$ ( $a \in \mathbb{Q}(\sqrt{2})$ ) . Ta có

$f(ii) = f(i)\ f(i) = a^2$

$f(ii) = f(-1) = -f(1) = -1$.

Do đó $a^2 = -1$.Suy ra $a = i$, hoặc $a = -i$ đều không thuộc $\mathbb{Q}(\sqrt{2})$. Vậy không tồn tại đẳng cấu $f$: $\mathbb{Q}(i) \to \mathbb{Q}(\sqrt{2})$. Suy ra $\mathbb{Q}(i) \ncong \mathbb{Q}(\sqrt{2})$

c) Tìm tất cả các trường con của $\mathbb{Q}(\sqrt{2})$

Ta có $\mathbb{Q}$ là trường con của $\mathbb{Q}(\sqrt{2})$. Ta chứng minh nếu $K$ là trường con của $\mathbb{Q}(\sqrt{2})$ thì $K = \mathbb{Q}$ hoặc $K = \mathbb{Q}(\sqrt{2})$

Ta có $1 \in K$ nên với mọi $n$ nguyên dương thì $n = 1+1+\ldots+1$($n$ lần) . Suy ra $n \in K$ . Do đó $-n \in K$ và $n^{-1} \in K$. Mọi số hữu tỉ $\in \mathbb{Q}$ có dạng $rs^{-1}$ ( với $r \in \mathbb{Z}$ và $s \in \mathbb{N}^*$), ta có $r \in K$ và $s^{-1} \in K$ . Suy ra $rs^{-1} \in K$ . Vậy $K$ chứa $\mathbb{Q}$. Nếu $K \neq \mathbb{Q}$ thì tồn tại phần tử $x = a + b\sqrt{2} \in K$, mà $a \in \mathbb{Q}$, $0 \neq b \in \mathbb{Q}$. Suy ra $b\sqrt{2} \in K$. Do đó $\sqrt{2} \in K$.

Vậy $K = \mathbb{Q}$.

Tương tự $\mathbb{Q}(i)$ có 2 trường con là $\mathbb{Q}$ và $\mathbb{Q}(i)$.

d) Chứng minh $A = \{a+b\sqrt[3]{2}+c\sqrt[3]{4} | a,b,c \in \mathbb{Q}\}$ là trường con của $\mathbb{C}$

Ta có $A \neq \varnothing$ vì $0 \in A$. Dễ thấy $\mathbb{C}$ chứa $A$. Với mọi $x, y \in A$ có dạng

$x = a+b\sqrt[3]{2}+c\sqrt[3]{4}$ và $y = d+e\sqrt[3]{2}+f\sqrt[3]{4}$ thì

$x+y = (a+d)+(b+e)\sqrt[3]{2}+(c+f)\sqrt[3]{4} \in A$ ,vì $a+d \in \mathbb{Q}$, $b+e \in \mathbb{Q}$, $c+f \in \mathbb{Q}$

$-x = -a+(-b)\sqrt[3]{2}+(-c)\sqrt[3]{4} \in A$, vì $-a \in \mathbb{Q}$, $-b \in \mathbb{Q}$, $-c \in \mathbb{Q}$

$$xy = ad+ae\sqrt[3]{2} + af\sqrt[3]{4} + bd\sqrt[3]{2} + be\sqrt[3]{4} + 2bf + \sqrt[3]{4}cd + 2ce + 2\sqrt[3]{2}cf$$
$$= (ad+2bf+2ce) + \sqrt[3]{2}(ae+bd+2cf) + \sqrt[3]{4}(af+be+cd) \in A ,$$

vì $ad+2bf+2ce \in \mathbb{Q}$, $ae+bd+2cf \in \mathbb{Q}$, $af+be+cd \in \mathbb{Q}$

Ta cần chứng minh $x^{-1} \in A$ với $x \in A$, $x \neq 0$. Trước hết ta có hằng đẳng thức $a^3 + b^3 + c^3 - 3abc = (a+b)^3 + c^3 - 3ab(a+b+c) = (a+b+c)(a^2 + b^2 + c^2 - ab - ac - bc)$. Áp dụng hằng đẳng thức này cho các số $a, b\sqrt[3]{2}$ và $c\sqrt[3]{4}$ ta có $a^3 + 2b^3 + 4c^3 - 6abc = (a + b\sqrt[3]{2} + c\sqrt[3]{4})(a^2 + b^2\sqrt[3]{4} + 2c^2\sqrt[3]{2} - ab\sqrt[3]{2} - ac\sqrt[3]{4} - 2bc)$. Ta chứng minh nếu $x = a + b\sqrt[3]{2} + c\sqrt[3]{4} \neq 0$ thì $a^3 + 2b^3 + 4c^3 - 6abc \neq 0$.

Thật vậy, nếu $a^3+2b^3+4c^3-6abc=0$ thì $a^2+b^2\sqrt[3]{4}+2c^2\sqrt[3]{2}-ab\sqrt[3]{2}-ac\sqrt[3]{4}-2bc=0$ hay $a^2-2bc+(2c^2-2ab)\sqrt[3]{2}+(b^2-ac)\sqrt[3]{4}=0$. Suy ra
$a^2-2bc=0$ hay $a^2=2bc$;
$2c^2-2ab=0$ hay $2c^2=2ab$;
$b^2-ac=0$.
Do đó $a^3=4c^3$. Vô lý. Bây giờ ta có

$$\frac{1}{a+b\sqrt[3]{2}+c\sqrt[3]{4}}=\frac{a^2+b^2\sqrt[3]{4}+2c^2\sqrt[3]{2}-ab\sqrt[3]{2}-ac\sqrt[3]{4}-2bc}{a^3+2b^3+4c^3-6abc}$$
$$=\frac{a^2-2bc}{a^3+2b^3+4c^3-6abc}+\frac{2c^2-2ab}{a^3+2b^3+4c^3-6abc}\sqrt[3]{2}+\frac{b^2-ac}{a^3+2b^3+4c^3-6abc}\sqrt[3]{4}$$

Do đó phần tử nghịch đảo của $x$ cũng thuộc $A$. Vậy$A$ là trường con của $\mathbb{R}$.

**Bài 2.24**

a) Xét ánh xạ $f:K\to\mathbb{Q}(i)$ như sau: $f\begin{pmatrix}a & b\\ -b & a\end{pmatrix}=a+bi\ \forall a,b\in\mathbb{Q}$

Ta có

$$f(\begin{pmatrix}a & b\\ -b & a\end{pmatrix}+\begin{pmatrix}c & d\\ -d & c\end{pmatrix})=f\begin{pmatrix}a+c & b+d\\ -(b+d) & a+c\end{pmatrix}=(a+c)+(b+d)i$$

$$f\begin{pmatrix}a & b\\ -b & a\end{pmatrix}+f\begin{pmatrix}c & d\\ -d & c\end{pmatrix}=a+bi+c+di=(a+c)+(b+d)i$$

Suy ra $f(\begin{pmatrix}a & b\\ -b & a\end{pmatrix}+\begin{pmatrix}c & d\\ -d & c\end{pmatrix})=f\begin{pmatrix}a & b\\ -b & a\end{pmatrix}+f\begin{pmatrix}c & d\\ -d & c\end{pmatrix}$

Tương tự $f(\begin{pmatrix}a & b\\ -b & a\end{pmatrix}.\begin{pmatrix}c & d\\ -d & c\end{pmatrix})=f(\begin{pmatrix}ac-bd & ad+bc\\ -(ad+bc) & ac-bd\end{pmatrix})=(ac-bd)+(ad+bc)i$

$$f\begin{pmatrix}a & b\\ -b & a\end{pmatrix}.f\begin{pmatrix}c & d\\ -d & c\end{pmatrix}=(a+bi)(c+di)=(ac-bd)+(ad+bc)i$$

Suy ra $f(\begin{pmatrix}a & b\\ -b & a\end{pmatrix}.\begin{pmatrix}c & d\\ -d & c\end{pmatrix})=f\begin{pmatrix}a & b\\ -b & a\end{pmatrix}.f\begin{pmatrix}c & d\\ -d & c\end{pmatrix}$.

Do đó $f$ là 1 đồng cấu nhóm.

$f$ là đơn cấu vì

$$f\begin{pmatrix}a & b\\ -b & a\end{pmatrix}=f\begin{pmatrix}c & d\\ -d & c\end{pmatrix}\Leftrightarrow(a+bi)=c+di\Leftrightarrow a=c,b=d$$

$$\Leftrightarrow\begin{pmatrix}a & b\\ -b & a\end{pmatrix}=\begin{pmatrix}c & d\\ -d & c\end{pmatrix}.$$

$f$ là toàn cấu vì với mỗi $a+bi \in \mathbb{Q}(i)$ thì ta luôn chọn được ma trận $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ sao cho $f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a+bi$

Vậy $f$ là 1 đẳng cấu. Do đó $K$ đẳng cấu với $\mathbb{Q}(i)$

b) Ánh xạ $g : F \to \mathbb{Q}(\sqrt{2})$ xác định bởi $g(\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}) = a+\sqrt{2}b \ \forall a,b \in \mathbb{Q}$

là đẳng cấu . Do đó $F$ đẳng cấu với $\mathbb{Q}(\sqrt{2})$ .

**Bài 2.25**

$a) \Leftrightarrow b)$

Ta có $\mathbb{Z}_n$ là hữu hạn nên theo Định lý 4.4 thì $\mathbb{Z}_n$ là trường khi và chỉ khi nó là miền nguyên.

$b) \Leftrightarrow c)$

Nếu $\mathbb{Z}_n$ là trường thì $n$ là số nguyên tố vì char $\mathbb{Z}_n = n$.

Nếu $n$ là số nguyên tố thì đương nhiên là $\mathbb{Z}_n$ trường.

**Bài 2.26**

a) Giả sử $I$ là ideal nguyên tố của vành $R$. Dễ dàng thấy rằng $R/I$ là vành giao hoán, có đơn vị, có nhiều hơn một phần tử. Bây giờ giả sử $(x+I)(y+I) = 0 = I$. Khi đó $xy + I = I$ hay $xy \in I$. Vì $I$ là ideal nguyên tố nên $x \in I$ hay $y \in I$. Do đó $x + I = I$ hay $y + I = I$. Suy ra $R/I$ không có ước của không.

Đảo lại, giả sử $R/I$ là miền nguyên. Khi đó $R/I$ nhiều hơn một phần tử. Do đó $I \neq R$. Giả sử $xy \in I$. Khi đó $(x+I)(y+I) = xy + I = I$. Mà $R/I$ là miền nguyên nên $x+I = I$ hay $y+I = I$. Suy ra $x \in I$ hay $y \in I$.

b)

Giả sử $R/I$ là trường khi đó $R/I$ có nhiều hơn một phần tử do đó $R \neq I$ . Giả sử $J$ là ideal của $R$ chứa thực sự $I$, như vậy có phần tử $c \in J \setminus I$. Ta có $c + I$ là phần tử khác không của $R/I$ nên khả nghịch. Tức là tồn tại $c'+I$ sao cho $(c + I)(c'+I) = e + I$.
Suy ra $e = cc' + d \in J$ ($d \in I$, $cc' \in J$). Do đó $J = R$.
Đảo lại, giả sử $I$ là ideal tối đại của $R$ thì $R/I$ là vành giao hoán, có đơn vị, có nhiều hơn một phần tử. Bây giờ nếu $x + I$ là phần tử khác không thì $x \notin I$ . Xét ideal $J = I + xR$. Dễ dàng thấy $J$ là ideal của $R$ chứa thực sự $I$ nên $J = R$.
Suy ra $e = a + x x'$ với $a \in I$. Khi đó $(x+I)(x'+I) = I$ .

**Bài 2.27**

(a) => (b)

Ta có {0} là ideal của *R*. Giả sử *I* là một ideal của *R* và $I \neq \{0\}$ .Vì *R* là một trường nên mọi phần tử khác 0 trong R đều khả nghịch. Do đó trong *I* tồn tại ít nhất một phần tử khả nghịch, thế thì *I* = *R*.

(b)=>(c)

Gọi *f* là đồng cấu vành từ *R* vào một vành bất kì. Ta có Ker *f* là ideal của *R* nên Ker *f* = {0} hay Ker *f* = *R*. Nếu Ker *f* = {0} thì *f* là đơn cấu. Nếu Ker *f* = *R* thì *f* là đồng cấu 0.

(c)=>(a)

Ta chỉ cần chứng minh tính chất mọi phần tử khác không trong *R* đều có phần tử nghịch đảo. Giả sử *x* là phần tử khác 0 bất kì của *R*. Xét *I* = <x> = *x* R là ideal sinh bởi *x*. Gọi *f* là toàn cấu chính tắc $R \to R/I$ . Ta có Ker(*f*) = $I \neq \{0\}$ nên *f* không là đơn cấu, theo giả thiết thì *f* là đồng cấu 0, tức là *I* = *R*. Vậy tồn tại *x'* thuộc *R* sao cho *xx'* = 1, suy ra *x* khả nghịch.

**Bài 2.28**

a) Ta có: $x^2 = 1 \Leftrightarrow (x-1)(x+1) = 0$ (vì 1 là phần tử đơn vị).Vì *F* là trường nên *F* là miền nguyên. Do đó, *F* không có ước của 0 nên đẳng thức trên xảy ra khi và chỉ khi *x* – 1 = 0 hay *x* +1 = 0, tương đương *x* =1 hay *x* = –1 .

b) Vì mỗi phần tử khác 0 thuộc trường *F* đều khả nghịch nên với $x_i \neq 0$ thì luôn tồn tại $x_i^{-1} = x_j$ ( $j \in \{1,2,...,p-1\}$ ).

Ta thấy rằng nếu $x_i$ =1 thì $x_i^{-1}$=1, nếu $x_i$ = –1 thì $x_i^{-1}$=–1, nếu $x_i \neq \pm 1$ thì $x_i \neq x_i^{-1}$ (theo Câu a)). Nếu $x_i \neq x_j$ thì $x_i^{-1} \neq x_j^{-1}$.

Do đó: $x_1.x_2...x_{(p-1)}$=1.(-1). $\prod(x_i.x_i^{-1})$=1.(-1)1= -1 .

Với $x_i$ bất kỳ ta có $x_i.x_k \neq x_i.x_j \ \ \forall k \neq j$ (vì $x_k \neq x_j$ ), nên

$\{x_i.x_1, x_i.x_2, ..., x_i.x_{(p-1)}\} = \{x_1, x_2, ..., x_{(p-1)}\}$ .

Do đó: $x_i.x_1.x_i.x_2....x_i.x_{(p-1)} = x_1.x_2...x_{(p-1)}$ . Suy ra $x_i^{(p-1)}.x_1.x_2...x_{(p-1)} = x_1.x_2...x_{(p-1)}$ . Vì vậy $x_i^{(p-1)} = 1$.

c) Áp dụng kết quả câu b) cho F=$\mathbb{Z}_p$

$\overline{1.2.3...(p-1)} = \overline{-1}$ (theo câu b). Do đó $(p-1)! \equiv -1 (\mathrm{mod}\ p)$ .

Đồng thời $(\overline{k})^{p-1} = \overline{k^{p-1}} = 1 \ \Leftrightarrow \ k^{(p-1)} \equiv 1 (\mathrm{mod}\ p)$ (khi $k \not\equiv 0 (\mathrm{mod}\ p)$ ) $\Leftrightarrow$ $k^p \equiv k (\mathrm{mod}\ p)$ (khi $k \not\equiv 0 (\mathrm{mod}\ p)$ ).

Nếu: $k \equiv 0 (\mathrm{mod}\ p)$ thì hiển nhiên $k^p \equiv k (\mathrm{mod}\ p)$

Tóm lại $k^p \equiv k (\mathrm{mod}\ p) \ \forall k \in \mathbb{Z}$

**Bài 2.29**

a)

Lấy $me, ne \in A$ bất kì, ta có:

i) $me - ne = (m-n)e \in A$

ii) $(me)(ne) = mne \in A$

Do đó $A$ là vành con của $F$. Dễ dàng thấy rằng $A$ là miền nguyên.

b)

- Giả sử $e$ có cấp vô hạn, ta chứng minh $A \cong \mathbb{Z}$:

Xét $f : A \to \mathbb{Z}$ thỏa mãn $f(ne) = n, \forall n \in \mathbb{Z}$. Ta có

$me = ne \Leftrightarrow (m-n)e \Leftrightarrow m-n = 0 \Leftrightarrow m = n \Leftrightarrow f(me) = f(ne) \Leftrightarrow f$ là ánh xạ và là đơn ánh. Vì

$f(ne+me) = f((m+n)e) = m+n = f(me) + f(ne)$

$f((me)(ne)) = f(mne) = mn = f(me)f(ne)$

nên $f$ là đồng cấu, đương nhiên $f$ toàn ánh. Vậy $f$ là đẳng cấu nên $A \cong \mathbb{Z}$.

- Giả sử $e$ *có* cấp $p$, ta chứng minh $A \cong \mathbb{Z}_p$.

Xét $f : A \to \mathbb{Z}_p$ thỏa mãn $f(ne) = \overline{n} \pmod p$

$ne = me \Leftrightarrow (m-n)e = 0 \Leftrightarrow m-n \vdots p \Leftrightarrow \overline{m} = \overline{n} \Leftrightarrow f(me) = f(ne)$ nên $f$ là ánh xạ và là đơn ánh. Vì

$f(ne+me) = f((m+n)e) = \overline{m+n} = \overline{m} + \overline{n} = f(me) + f(ne)$

$f((me)(ne)) = f(mne) = \overline{mn} = \overline{m}.\overline{n} = f(me)f(ne)$

nên $f$ là đồng cấu, đương nhiên $f$ toàn ánh.Vậy $f$ là đẳng cấu nên $A \cong \mathbb{Z}_p$.

c) Nếu $e$ có cấp $p$ hữu hạn trong trường $F$ thì theo tính chất cơ bản $p$ phải nguyên tố, theo Bài **2.25** thì $\mathbb{Z}_p$ là một trường. Hơn nữa theo Câu b) thì $A \cong \mathbb{Z}_p$. Suy ra $A$ là một trường.

**Bài 2.30** Xét trường con $A$ của $\mathbb{Q}$

Vì $A$ là trường con của $\mathbb{Q}$ nên 1 thuộc $A$. Với $n$ nguyên dương ta có

$n = 1+1+\ldots+1 \in A$ , $-n \in A$,và $\frac{1}{n} \in A$.

Lấy $\frac{p}{q} \in \mathbb{Q}$ ($p$ nguyên dương, $q$ nguyên , $q \neq 0$) . Ta có

$\frac{p}{q} = p.\left(\frac{1}{q}\right) \in A$ ( Do $p \in A$ , $\frac{1}{q} \in A$) . Suy ra $\mathbb{Q} \subset$ A. Vậy $A = \mathbb{Q}$.

**Bài 2.31**

Xét trường $F$. Ta biết tùy theo char $F = 0$ hay char$F \neq 0$ mà $F$ có một trường con $T$ đẳng cấu với $\mathbb{Q}$ hoặc $\mathbb{Z}_p$ với $p$ nguyên tố. Ta chứng minh là $\mathbb{Q}$ và $\mathbb{Z}_p$ với $p$ nguyên tố không có trường con thực sự nào.

Gọi $H$ là trường con của $\mathbb{Q}$, suy ra 1 thuộc $H$, do đó $m$ thuộc $H$ với $m$ thuộc $\mathbb{Z}$, nên $n^{-1}$ thuộc $H$ với $n$ thuộc $\mathbb{Z}^*$, vậy $mn^{-1}$ thuộc $H$, hay $H = \mathbb{Q}$.

Gọi $H$ là trường con của $\mathbb{Z}_p$, suy ra $\bar{1}$ thuộc $H$, nên $\bar{n}$ thuộc $H$ với mọi $n$, do đó $H = \mathbb{Z}_p$. Do $T$ đẳng cấu với $\mathbb{Q}$ hoặc $\mathbb{Z}_p$ nên trường con thực sự của $T$ qua phép đẳng cấu cũng là trường con thực sự của $\mathbb{Q}$ hoặc $\mathbb{Z}_p$. Vậy $T$ không có trường con thực sự nào.Vậy $T$ là trường nhỏ nhất theo quan hệ bao hàm.

**Bài 2.32**.

a) Gọi $e$ là phần tử đơn vị của $F$ và $e'$ là phần tử đơn vị của $A$. Vì $F$ là một trường nên F cũng là một miền nguyên. Do đó, $\forall a,b \in F$, $a.b = 0$ khi và chỉ khi $a = 0$ hay $b = 0$. Vì $A$ có nhiều hơn 1 phần tử nên tồn tại $x \in A$ sao cho $x \neq 0$.

Ta có : $e'.x = x$ và $e.x = x$, nên $(e' - e).x = 0$ . Mà $e' - e$ , $x$ đều thuộc $F$ nên ta suy ra được $e - e' = 0$ hay $x = 0$. Tuy nhiên, $x \neq 0$ do cách chọn $x$, nên $e' - e = 0$. Vậy $e' = e$.

Dễ thấy $A$ là vành giao hoán và không có ước của 0 (vì $A$ là vành con của trường $F$). $A$ lại có phần tử đơn vị, có nhiều hơn 1 phần tử. Do đó, $A$ là miền nguyên.

b) Xét 2 phần tử $x, y \in P$, $x = ab^{-1}$ và $y = cd^{-1}, b \neq 0, d \neq 0$.

Ta có : $ab^{-1} - cd^{-1} = ab^{-1}.e - cd^{-1}.e = ab^{-1}.d.d^{-1} - cd^{-1}.b.b^{-1} = (ad - bc).(bd)^{-1}$ . Đẳng thức này tồn tại vì $A$ là miền nguyên nên $A$ có tính chất giao hoán và $bd \neq 0$.

Như thế là $x - y = ab^{-1} - cd^{-1} = (ad - bc).(bd)^{-1}$, mà $ad - bc$ và $bd$ đều thuộc $A$. Do đó, $x - y \in P$.

Xét $x, y \in P$, $x \neq 0$, $x = ab^{-1}$ và $y = cd^{-1}, a \neq 0, b \neq 0, d \neq 0$.. Vì $x \neq 0$ nên tồn tại $x^{-1}$ và $x^{-1} = (ab^{-1})^{-1} = ba^{-1}$. Khi đó $x^{-1}y = ba^{-1}.cd^{-1} = bc.(a^{-1}d^{-1}) = bc.(da)^{-1} \Rightarrow x^{-1}y \in P$.

Vậy $P$ là trường con của $F$.

Xét $f : A \to P$, $f(x) = x.e^{-1} = x$ . Dễ thấy $f$ là một ánh xạ được xác định.

Ta có:

$$f(x + y) = x + y = f(x) + f(y)$$

$$f(xy) = xy = f(x).f(y)$$

Như vậy $f$ là một đồng cấu vành, đồng thời $f$ là một đơn cấu. Mỗi phần tử của $P$ đều có dạng $ab^{-1} = f(a).f(b)^{-1}$ với $a,b \in A$ và $b \neq 0$.Vậy $P$ là trường các thương của $A$.

c) Dễ thấy nếu $a \in A$ thì $a = a.e^{-1} \in P \Rightarrow A \subset P$.

Xét một trường con $B$ của $F$ sao cho $B$ chứa $A$.

Với 1 phần tử $ab^{-1}$ bất kỳ của P,với $a,b \in A$ và $b \neq 0$,vì $A \subset B$ nên $a,b \in B$ ,đồng thời trong $B$ tồn tại phần tử $b^{-1}$. Do đó , $ab^{-1} \in B$. Như vậy $P \subseteq B$, ta được đpcm.

**Bài 2.33**

Đặt $A = \left\{ \frac{m}{n} \mid m,n \in \mathbb{Z}; n \neq 0; (n,p) = 1 \right\}$, ta chứng minh $A$ là miền nguyên.

Với $\frac{m}{n}, \frac{a}{b} \in A$ bất kì ta có

$\frac{m}{n}-\frac{a}{b}=\frac{mb-na}{nb}$

Vì $(n,p)=1,(b,p)=1\Rightarrow(nb,p)=1$ do đó $\frac{mb-na}{nb}\in A$ tức là $\frac{m}{n}-\frac{a}{b}\in A$.

$\frac{m}{n}.\frac{a}{b}=\frac{ma}{nb}$

Vì $(n,p)=1,(b,p)=1\Rightarrow(nb,p)=1$ do đó $\frac{ma}{nb}\in A$ tức là $\frac{m}{n}.\frac{a}{b}\in A$.

Suy ra $A$ là vành con của trường số hữu tỷ. Đương nhiên phép nhân có tính chất giao hoán, có phần tử đơn vị là 1, mọi phần tử đều không là ước của 0. Như vậy $A$ là một miền nguyên.

Gọi $P$ là trường các thương của $A$ thì $P$ là trường con của trường hữu tỷ $\mathbb{Q}$. Trường số hữu tỷ không có trường con thực sự, do đó $P=\mathbb{Q}$.

**Bài 2.34**

a) Ta thấy với $p$ nguyên tố thì $(k,p)=1 \Leftrightarrow (k,p^m)=1$($m$ nguyên dương )
Ta sẽ tìm tất cả các $k$ sao cho $(k,p)\neq 1$ với $1\le k\le p^m$.

Đặt $k=tp$ ( $1\le t$ ), ta có $1\le tp\le p^m \Leftrightarrow 1\le t\le p^{m-1}$, suy ra có tất cả $p^{m-1}$ giá trị $k$ với $1\le k\le p^m$ sao cho $(k,p)\neq 1$.

Vậy $\varphi(p^m)=p^m-p^{m-1}=p^{m-1}(p-1)$

b) Ta có $n=p_1^{m_1}p_2^{m_2}....p_k^{m_k}$ và $\varphi(n)=\varphi(p_1^{m_1})\dots\varphi(p_k^{m_k})$.

Suy ra $\varphi(n)=n(1-p_1^{-1})(1-p_2^{-1})\dots(1-p_k^{-1})$.

**Bài 2.35**

Gọi $f$ là đồng cấu trường từ trường $F$ vào trường $F$'. Khi đó $f$ có thể là đồng cấu không, nên ta chỉ phải tìm thêm đồng cấu không tầm thường, nghĩa là tồn tại $x$ thuộc $F$ sao cho $f(x)\neq 0$.
Ta có $f(1x)=f(x)1=f(x).f(1)$, giản ước cho $f(x)$ ta được $f(1)=1$.
Vậy $f(0)=0; f(1)=1$.

a) Trường hợp $F$ là $\mathbb{Q}$.

Với $m$, $n$ thuộc $\mathbb{Z}$ và $n\neq 0$, ta có $f(1)=1$, nên $f(m)=m$,

Do đó $n\,f(mn^{-1})=f(n.mn^{-1})=f(m)=m$. Suy ra $f(mn^{-1})=mn^{-1}$. Vậy $f$ chính là ánh xạ đồng nhất. Vậy chỉ có hai tự đồng cấu của trường số hữu tỷ là đồng cấu không và đồng cấu đồng nhất.

b) Trường hợp $F$ là $\mathbb{Q}(\sqrt{2})$.

Ta có $2=f(2)=f((\sqrt{2})^2)=(f(\sqrt{2}))^2$.
Do đó $f(\sqrt{2})=\sqrt{2}$ hoặc $f(\sqrt{2})=-\sqrt{2}$.
Nếu $f(\sqrt{2})=\sqrt{2}$ thì $f(a+b\sqrt{2})=f(a)+f(b)\sqrt{2}=a+b\sqrt{2}$.

Nếu $f(\sqrt{2}) = -\sqrt{2}$ thì $f(a + b\sqrt{2}) = f(a) + f(b)\sqrt{2} = a - b\sqrt{2}$.

Vậy có 3 tự đồng cấu của $\mathbb{Q}(\sqrt{2})$ là đồng cấu không, đồng cấu đồng nhất và đồng cấu liên hợp.

c) Trường hợp $F$ là $\mathbb{Q}(i)$.

Hoàn toàn tương tự Câu $b$, ta có $f(i) = i$ hoặc $f(i) = -i$ , do đó có 2 đồng cấu không tầm thường là $f(x) = x$ với mọi $x$, hoặc $f(x) = \bar{x}$ trong đó $\bar{x}$ là số phức liên hợp của $x$. Vậy có 3 tự đồng cấu của $\mathbb{Q}(i)$ là đồng cấu không, đồng cấu đồng nhất và đồng cấu liên hợp.

d) Trường hợp F là $\mathbb{R}$

Theo Câu a, $f(x) = x$, với mọi $x$ thuộc $\mathbb{Q}$.

Với mọi số thực $x > 0$ thì $f(x) = (f(\sqrt{x}))^2$, hơn nữa mọi đồng cấu trường không tầm thường đều là đơn cấu nên $f(x) > 0$. Xét $x$, $y$ thuộc $\mathbb{R}$ sao cho $x > y$ thì $f(x) - f(y) = f(x - y) > 0$. Suy ra $f$ là hàm số tăng trên $\mathbb{R}$.

Khi này với mọi số thực $x$, xét dãy số hữu tỉ $(a_n)$ và $(b_n)$ tiến tới $x$ với $a_n < x < b_n$.
Khi đó $f(a_n) < f(x) < f(b_n)$ với mọi $n$, hay $a_n < f(x) < b_n$ với mọi $n$, cho $n$ tiến tới vô cùng suy ra $x \leq f(x) \leq x$. Suy ra $f(x) = x$ với mọi số thực $x$. Do đó $f$ là ánh xạ đồng nhất. Vậy chỉ có hai tự đồng cấu của trường số thực là đồng cấu không và đồng cấu đồng nhất.

e) Trường hợp $F$ là $\mathbb{C}$ và sao cho $f(x) = x$ với mọi $x$ thuộc $\mathbb{R}$.

Lúc này hoàn toàn tương tự Câu c, ta có hai đồng cấu là $f(x) = x$ với mọi $x \in \mathbb{C}$ hoặc $f(x) = \bar{x}$ với mọi $x \in \mathbb{C}$. Vậy có hai tự đồng cấu của trường số phức giữ nguyên các số thực là đồng cấu đồng nhất và đồng cấu liên hợp.

# CHƯƠNG III. VÀNH ĐA THỨC

## A. TÓM TẮT LÝ THUYẾT

1. Vành đa thức một ẩn

1.1. Định nghĩa

Giả sử $R$ là vành giao hoán có đơn vị 1. Gọi $A$ là tập tất cả các dãy $(a_0, a_1, a_2, \ldots, a_n,\ldots)$, trong đó các $a_i \in R$ với mọi $i \in \mathbb{N}$ và bằng không tất cả trừ một số hữu hạn. Trong $A$ phép cộng và phép nhân được định nghĩa như sau:

Giả sử $f = (a_0, a_1, \ldots, a_n,...)$, $g = (b_o, b_1\ldots, b_n, \ldots)$ là các phần tử tùy ý của $A$. Khi đó

$f + g = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n,\ldots)$, $fg = (c_o, c_1,\ldots,c_n,\ldots)$,

trong đó $c_k = \sum_{i+j=k} a_i b_j$, k= 0,1,….

Với hai phép toán này thì $A$ là vành giao hoán, có đơn vị. đặt $x = (0, 1, 0,0,\ldots.)$. Ánh xạ

$R \to A$

$a \mapsto (a, 0,0, \ldots, )$

là đơn cấu, do vậy ta đồng nhất phần tử $a \in R$ với dãy $(a,0,0, \ldots)$. Khi đó

$(a_0, a_1, \ldots, a_n, 0,0,\ldots 0) = a_0 + a_1 x + \ldots + a_n x^n$, và thường được viết là

$f(x) = a_n x^n + \ldots + a_1 x + a_0$ . Nếu $a_n \neq 0$, $(n \geq 0)$ thì $n$ được gọi là bậc của đa thức $f(x)$ và ký hiệu là deg$f(\mathbf{x})$. Vành $A$ được gọi là vành đa thức của ẩn $x$ và được ký hiệu là $R[x]$.

1.2. Giả sử $K$ là một trường và $f(x)$, $g(x) \in K[x]$, $g(x) \neq 0$. Khi đó tồ tại duy nhất các đa thức $q(x)$, $r(x) \in K[x]$ sao cho $f(x) = g(x)q(x) + r(x)$, với deg $r(x)$ < deg $g(x)$. Các đa thức $q(x)$ và $r(x)$ được gọi tương ứng là thương và dư trong phép chia $f(x)$ cho $g(x)$. Nếu $r(x) = 0$, thì ta nói $f(x)$ chia hết cho $g(x)$ hay $g(x)$ là ước của $f(x)$ trong $K[x]$.

1.3. Một đa thức $d(x) \in K[x]$ là ước của của hai đa thức $f(x)$ và $g(x)$ được gọi là ước chung của $f(x)$ và $g(x)$. Nếu $d(x)$ là ước chung của $f(x)$ và $g(x)$, đồng thời chia hết cho mọi ước chung khác của $f(x)$ và $g(x)$ thì $d(x)$ được gọi là ước chung lớn nhất của $f(x)$ và $g(x)$, ký hiệu là $d(x) = (f(x), g(x))$. Thường qui ước lấy hệ số cao nhất của ước chung lớn nhất bằng 1.

1.4. Thuật toán Euclide tìm ước chung lớn nhất

Để tìm UCLN của hai đa thức $f(x)$, $g(x) \in K[x]$ ta dùng thuật chia Euclide bằng cách thực hiện một số hữu hạn phép chia liên tiếp như sau

$f(x) = g(x)q(x) + r(x)$ deg$r(x)$ < deg $g(x)$

$g(x) = r(x)\, q_1(x) + r_1(x)$ deg$r_1(x)$ < deg $r(x)$

……

$r_{k-2}(x) = r_{k-1}(x)\, q_k(x) + r_k(x)$, deg $r_k(x)$ < deg $r_{k-1}(x)$

$r_{k-1}(x) = r_k(x) q_{k+1}(x)$.

Đa thức dư cuối cùng khác 0 trong dãy phép chia nói trên chính là $r_k(x)$. UCLN $d(x)$ là thương của phép chia $r_k(x)$ cho hệ số cao nhất của nó.

Cũng từ thuật toán Euclide ta tìm được hai đa thức $u(x)$ và $v(x)$ sao cho

$$f(x)u(x) + g(x)\, v(x) = d(\mathbf{x}).$$

1.5. Cho $D$ là miền nguyên. Đa thức $f(x) \in D[x]$ khác không, không khả nghịch được gọi là bất khả qui trong $D[x]$ ( hay còn gọi là bất khả qui trên $D$) nếu nó không có ước thực sự trong $D[x]$, tức là nếu $f(x) = g(x)\, h(x)$ thì $g(x)$ hay $h(x)$ phải là phần tử khả nghịch của $D$.

2. Đa thức trên trường $K$

2.1. Cho đa thức $f(x)$ bậc $n$ trên $K$ và $c \in K$. Khi đó $f(x)$ có thể khai triển duy nhất thành dạng $f(x) = \sum_{k=0}^{n} c_k(x-c)^k$, ta gọi là khai triển Taylor của $f(x)$ theo các lũy thừa của $x - c$.

2.2. Giả sử $k$ là số tự nhiên khác không. Phần tử $c \in K$ được gọi là nghiệm bội $k$ của $f(x) \in K[x]$, nếu $f(x)$ chia hết cho $(x-c)^k$ nhưng không chia hết cho $(x-c)^{k+1}$.

2.3. Cho $x_1, x_2, \ldots, x_n, c_1, c_2, \ldots, c_n$ là các phần tử của trường $K$, trong đó $x_i \neq x_j$, $\forall i \neq j$. Đặt $\varphi(x) = (x-x_1)(x-x_2)\ldots(x-x_n)$

$\varphi_i(x) = \frac{\varphi(x)}{x-x_i}$, $\rho_i(x) = \frac{\varphi_i(x)}{\varphi_i(x_i)}$, $f_0(x) = c_1\rho_1(x) + c_2\rho_2(x) + \ldots + c_n\rho_n(x)$.

Khi đó đa thức $f(x) \in K[x]$ thỏa mãn điều kiện $f(x_i) = c_i$, $i = 1,2,\ldots, n$ khi và chỉ khi $f(x)$ có dạng $f(x) = f_0(x) + g(x)\,\varphi(x)$, với $g(x)$ là đa thức nào đó của $K[x]$.

3. Đa thức bất khả qui trên các trường số

3.1. Đa thức $f(x)$ của vành $\mathbb{C}[x]$ là bất khả qui trên $\mathbb{C}$ khi và chỉ khi $f(x)$ bậc nhất

3.2. Đa thức $f(x)$ của vành $\mathbb{R}[x]$ là bất khả qui trên $\mathbb{R}$ khi và chỉ khi $f(x)$ bậc nhất hoặc bậc hai với biệt số âm.

3.3. Tiêu chuẩn Eisenstien

Giả sử $f(x) = a_n x^n + \ldots + a_1 x + a_0$ ($n > 1$) là đa thức với hệ số nguyên và giả sử tồn tại số nguyên tố $p$ sao cho

i) Hệ số cao nhất $a_n$ không chia hết cho $p$, tất cả các hệ số còn lại đều chia hết cho $p$.

ii) Hệ số tự do $a_0$ không chia hết cho $p^2$.

Khi đó $f(x)$ là đa thức bất khả qui trong $Q[x]$.

## B. CÁC DẠNG TOÁN

1. Dạng toán 1. Các bài toán liên quan đến tính chất chia hết trong vành đa thức

   Muốn chứng minh một đa thức $g(x)$ chia hết cho đa thức $f(x)$ chỉ cần chứng minh mọi nghiệm của $f(x)$ đều là nghiệm của $g(x)$ và mọi nghiệm bội $k$ của $f(x)$ đều là nghiệm bội cấp $l$ với $l \geq k$ của $g(x)$. Xem Bài 3.6, 3.7.

2. Dạng toán 2. Tìm ước chung lơn nhất của hai đa thức

   Sử dụng 1.4. Xem Bài 3.9

3. Dạng toán 3. Khai triển Taylor, nghiệm bội
   Sử dụng 2.1,2.2. Xem Bài 3.10.
4. Dạng toán 4. Tìm các đa thức biết giá trị của chúng tại *n* điểm phân biệt
   Sử dụng 2.3. Xem Bài 3.11.
5. Dạng toán 5. Đa thức bất khả qui trên trường số.
   Sử dụng 3.1,3.2,3.3. Xem Bài 3.14, 3.15, 3.20.

## C. LỜI GIẢI HOẶC ĐÁP SỐ HƯỚNG DẪN BÀI TẬP CHƯƠNG 3

**Bài 3.1**

Bằng cách thử trực tiếp ta tìm được 4 nghiệm là $x = \overline{1}, \overline{4}, \overline{11}, \overline{14}$.

**Bài 3.2**. Vì $f(x)$ chia hết cho $x + 2$ nên $f(-2) = 0$ . Vì $f(x)$ chia cho $x^2 - 1$ thì dư $x$ nên $f(x) = (x^2 - 1)\, q(x) + x$. Do đó $f(1) = 1$, $f(-1) = -1$. Vậy ta có hệ phương trình

$$\begin{cases} 32 + 4a - 2b + c = 0 \\ 2 + a + b + c = 1 \\ 2 + a - b + c = -1 \end{cases}$$

Giải hệ này ta được $a = -\frac{28}{3}, b = 1, c = \frac{22}{3}$. Vậy $f(x) = 2x^4 - \frac{28}{3}x^2 + x + \frac{22}{3}$.

**Bài 3.3**

a) Nếu $f(x^n)$ chia hết cho $x - 1$ thì $f(1^n) = f(1) = 0$, tức là $f(x)$ chia hết cho $x - 1$ hay $f(x) = (x - 1)\, g(x)$ .Thay $x$ bởi $x^n$ thì $f(x^n) = (x^n - 1).g(x^n)$.Vậy $f(x^n)$ chia hết cho $x^n - 1$.

b) Nếu $F(x) = f(x^n)$ chia hết cho $(x - a)^k$ , thì $F'(x) = f'(x^n) n x^{n-1}$ chia hết cho $(x - a)^{k-1}$, do đó $f'(x^n)$ chia hết cho $(x - a)^{k-1}$.Tương tự , $f''(x^n)$ chia hết cho $(x - a)^{k-2}$, …, $f^{(k-1)}(x^n)$ chia hết cho $x - a$. Do đó,
   $f(a^n) = f'(a^n) = \ldots = f^{(k-1)}(a^n) = 0$
   Điều đó chứng tỏ rằng $f(x)$ chia hết cho $(x - a^n)^k$ , thay $x$ bởi $x^n$ thì $f(x^n)$ chia hết cho $(x^n - a^n)^k$.

c) Gọi $z$ là nghiệm của $x^2 + x + 1$ thì $z^3 = 1$, nghĩa là $z$ có thể lấy 2 giá trị phức liên hợp của $\sqrt[3]{1}$ . Nếu gọi $y$ là một trong hai giá trị phức của $\sqrt[3]{1}$ thì giá trị phức liên hợp với nó sẽ là $y^2$. Vì $f(x) = g(x^3) + x h(x^3)$ chia hết cho $x^2 + x + 1$ nên
   $f(z) = g(z^3) + z h(z^3) = g(1) + z h(1) = 0$
   $f(z^2) = g(z^6) + z^2 h(z^6) = g(1) + z^2 h(1) = 0$
   Từ đó rút ra $g(1) = h(1) = 0$, nghĩa là $g(x)$và $h(x)$ chia hết cho $x - 1$.

**Bài 3.4**

($\Rightarrow$) Nếu $f(x)$ là ước của $g(x)$ trong $K[x]$ thì tồn tại $h(x) \in K[x]$ sao cho $g(x) = f(x)h(x)$ , nhưng $h(x)$ cũng thuộc $F[x]$ nên đẳng thức này cũng khẳng

định rằng $f(x)$ là ước của $g(x)$ trong $F[x]$.

($\Leftarrow$) Nếu $f(x)$ là ước của $g(x)$ trong $F[x]$ thì tồn tại $h(x) \in F[x]$ sao cho

$g(x) = f(x)h(x)$ (1)

Vì $K$ là trường nên ta có $q(x), r(x) \in K[x]$ sao cho

$g(x) = f(x)q(x) + r(x)$ , $deg\ r(x) < deg\ f(x)$ (2)

Từ (1) và (2) : $f(x)\ [h(x) - q(x)] = r(x)$. Suy ra $h(x) = q(x)$ và $r(x) = 0$.

**Bài 3.5**

Sử dụng định nghĩa nghiệm bội trang 99 SGK.

**Bài 3.6**.

Phương pháp: Muốn chứng minh một đa thức $g(x)$ chia hết cho đa thức $f(x)$ chỉ cần chứng minh mọi nghiệm của $f(x)$ đều là nghiệm của $g(x)$ và mọi nghiệm bội $k$ của $f(x)$ đều là nghiệm bội cấp $l$ với $l \geq k$ của $g(x)$.

c) Nếu gọi $z$ là nghiệm của $f(x) = x^2+x+1$ thì

$z^2 = -z - 1$

$z^3 = -z^2 - z = z + 1 - z = 1$.

Thay $z$ vào đa thức $f(x) = x^{3k} + x^{3m+1} + x^{3n+2}$ với chú ý $z^3 = 1$, ta có

$z^{3k}+z^{3m+1}+z^{3n+2} = 1+z+z^2 = 0$

Vậy $z$ cũng là nghiệm của đa thức $g(x)$.

Cách khác:

Ta có $g(x) - f(x) = x^{3k} - 1 + x^{3m+1} - x + x^{3n+2} - x^2$

$= (x^3 - 1)h(x) + x(x^3 - 1)k(x) + x^2(x^3 - 1)p(x)$.

Mà $x^3 - 1$ chia hết cho $x^2 + x + 1 = f(x)$. Suy ra $g(x)$ chia hết cho $f(x)$.

**Bài 3.7**

a) Gọi $z$ là nghiệm của $f(x)$ ta nhận thấy $z^3 = 1$. Chia $n$ cho 3 ta được

$n = 3q + r$

Ta có $g(z) = z^{2n} + z^n + 1 = z^{2(3q+r)} + z^{3q+r} + 1 = z^{2r} + z^r + 1$

Nếu $r = 0$ thì $g(z) = 3$

$r = 1$ thì $g(z) = z^2 + z + 1 = 0$

$r = 2$ thì $g(z) = z^4 + z^2 + 1 = z + z^2 + 1 = 0$

Vậy điều kiện để $g(z) = 0$ là $n$ không chia hết cho 3.

b) Chia $n$ cho 6 ta được $n = 6q + r$. Thay vào $g(z)$ nhận $r = 2, 4$.

c) Như b).

d) ĐS $k, m, n$ cùng chẵn hoặc cùng lẻ.

**Bài 3.8**.

a) ($\Rightarrow$) Nếu $m|n$ thì $n = mk$ . Do đó $f_n(x) = x^{mk} - 1 = (x^m)^k - 1 = (x^m - 1)g(x)$.

($\Leftarrow$) Nếu $f_m \mid f_n$ . Đặt $n = mk + r$ .Ta có $f_n = x^{mk+r} - 1 = x^{mk+r} - x^r + x^r - 1 =$

$= x^r(x^{mk} - 1\ ) + x^r\ - 1$ . Vì $x^{mk} - 1$ và $f_n$ chia hết cho $f_m$ nên $x^r - 1$ chia hết cho $f_m$ . Vậy $r = 0$.

b) Dùng thuật toán Euclid .
Thực hiện phép chia : $x^m - 1 = (x^n - 1\ )q(x) + r(x)$ ta thấy $r(x) = x^r - 1$ , với $m = nq + r\ (0 \le r < n)$.
Tiếp tục $x^n - 1 = (x^r - 1\ )q_1(x) + r_1(x)$.
$r_1(x) = x^r{}_1 - 1$ với $n = rq_1 + r_1\ (0 \le r_1 < r)$
Tiếp tục như thế mãi , ta thấy dư cuối cùng khác không sẽ là
$r_k(x) = x^r{}_k - 1$ với $r_{k-2} = r_{k-1}q_k + r_k$ . Theo thuật toán Euclid tìm ước chung lớn nhất của $m$ và $n$ thì $r_k = (m, n)$.
Chú ý : a) suy ra từ b) nên thật ra ta chỉ phải chứng minh b).

**Bài 3.9**

a) Trên $\mathbb{Q}$

$f(x) = q(x)g(x) + r(x)$ với $q(x) = 2x$ và $r(x) = -6x^2 - 3x + 9;$
$g(x) = q_1(x)r(x) + r_1(x)$ với $q_1(x) = \frac{1-x}{3}$ và $r_1(x) = 1 - x;$
$r(x) = q_2(x)r_1(x)$ $q_2(x) = 6x + 9.$

Vậy $h = (f, g) = \dfrac{r_1(x)}{-1} = x - 1.$

Ta có $r_1(x) = g(x) - q_1(x)r(x)$
$= g(x) - q_1(x)\big(f(x) - q(x)g(x)\big) =$
$= g(x) - q_1(x)f(x) + q_1(x)q(x)g(x) =$
$= g(x)\left(1 + \frac{1-x}{3}2x\right) - \frac{1-x}{3}f(x)$

Vậy $u(x) = \frac{1}{3}(2x^2 - 2x - 3), v(x) = \frac{1}{3}(1 - x).$

$$k = \frac{fg}{h} = \frac{(4x^4 - 2x^3 - 16x^2 + 5x + 9)(2x^3 - x^2 - 5x + 4)}{x - 1} =$$
$$= (4x^4 - 2x^3 - 16x^2 + 5x + 9)(2x^2 + x - 4).$$

Trên $\mathbb{Z}_5$

$f(x) = \bar{4}x^4 - \bar{2}x^3 - x^2 + \bar{4},\ g(x) = \bar{2}x^3 - x^2 + \bar{4}.$
$f(x) = q(x)g(x) + r(x)$ với $q(x) = \bar{2}x + \bar{1}, r(x) = \bar{3};$
$g(x) = q_1(x)r(x)$ với $q_1(x) = \bar{4}x^3 + \bar{2}x^2 + \bar{3}.$
Vậy $h = (f, g) = \bar{1}$. Suy ra $k = fg.$
Ta có $r(x) = f(x) - q(x)g(x)$ . Do đó $h(x) = \bar{2}\,r(x) = \bar{2}f(x) - \bar{2}q(x)g(x).$
Vậy $u(x) = \bar{2}$ và $v(x) = \bar{2}q(x) = \bar{2}(x + \bar{1}).$

**Bài 3.10**

a) $f(x) = (x-2)^5 + 8(x-2)^4 + 19(x-2)^3 + 17(x-2)^2$.

Suy ra 2 là nghiệm bội cấp 2 của $f(x)$ và $f'(2) = 0$, $f''(2) = 2!17$, $f^{(3)}(2) = 3!19$, $f^{(4)}(2)$ ,$=4!8$, $f^{(5)}(2) = 5!$, $f^{(6)}(2) = 0$.

b) $f(x) = (x-3)^5 + 10(x-3)^4 + 34(x-3)^3 + 40(x-3)^2$.

Suy ra 2 là nghiệm bội cấp 2 của $f(x)$ và $f'(3) = 0$, $f''(3) = 2!40$, $f^{(3)}(3) = 3!34$, $f^{(4)}(3)$ ,$=4!10$, $f^{(5)}(3) = 5!$, $f^{(6)}(3) = 0$.

c) $f(x) = (x-2)^6 + 6(x-2)^5 + 13(x-2)^4 + 9(x-2)^3$.

Suy ra 2 là nghiệm bội cấp 3 của $f(x)$ và $f'(2) = 0$, $f''(2) = 0$, $f^{(3)}(2) = 3!9$, $f^{(4)}(2)$ ,$=4!13$, $f^{(5)}(2) = 5!6$, $f^{(6)}(2) = 6!$.

d) $f(x) = 8(x-\frac{1}{2})^6 + 12(x-\frac{1}{2})^5 + 6(x-\frac{1}{2})^4 + 9(x-\frac{1}{2})^3$.

Suy ra $\frac{1}{2}$ là nghiệm bội cấp 3 của $f(x)$ và $f'(\frac{1}{2}) = 0$, $f''(\frac{1}{2}) = 0$, $f^{(3)}(\frac{1}{2}) = 3!9$, $f^{(4)}(\frac{1}{2})$ ,$=4!6$, $f^{(5)}(\frac{1}{2}) = 5!12$, $f^{(6)}(\frac{1}{2}) = 6!8$.

**Bài 3.11**

a) Đặt

$\varphi(x) = (x-2)(x-3)(x-4)$,

$\varphi_1(x) = (x-3)(x-4)$,

$\varphi_2(x) = (x-2)(x-4)$,

$\varphi_3(x) = (x-2)(x-3)$.

Suy ra $\varphi_1(2) = 2, \varphi_2(3) = -1, \varphi_3(4) = 2$. Đặt $\rho_1 = \frac{1}{2}\varphi_1$, $\rho_2 = -\varphi_2$, $\rho_3 = \frac{1}{2}\varphi_3$.

Khi đó tất cả các đa thức cần tìm có dạng

$f(x) = 4\rho_1(x) + 6\rho_2(x) + 8\rho_3(x) + g(x)\varphi(x)$, với $\varphi(x) \in \mathbb{R}[x]$.

b) Đặt

$\varphi(x) = (x-\bar{2})(x+\bar{1})(x-\bar{3})$,

$\varphi_1(x) = (x+\bar{1})(x-\bar{3})$,

$\varphi_2(x) = (x-\bar{2})(x-\bar{3})$,

$\varphi_3(x) = (x-\bar{2})(x+\bar{1})$.

Suy ra $\varphi_1(\bar{2}) = \bar{4}$ $\varphi_2(-\bar{1}) = \overline{12} = \bar{2}, \varphi_3(\bar{3}) = \bar{4}$. Đặt $\rho_1 = \frac{1}{4}\varphi_1 = -\bar{1}\varphi_1$,

$\rho_2 = \frac{1}{2}\varphi_2 = -\bar{2}\varphi_2$, $\rho_3 = \frac{1}{4}\varphi_3 = -\bar{1}\varphi_3$.

Khi đó tất cả các đa thức cần tìm có dạng

$f(x) = \bar{1}\rho_1(x) + \bar{3}\rho_2(x) + \bar{2}\rho_3(x) + g(x)\varphi(x)$, với $\varphi(x) \in \mathbb{Z}_5[x]$.

c) Đặt

$\varphi(x) = (x-\bar{2})(x-\bar{5})(x-\bar{3})$,

$\varphi_1(x) = (x-\bar{5})(x-\bar{3})$,

$\varphi_2(x) = (x-\bar{2})(x-\bar{3})$,

$\varphi_3(x) = (x-\bar{2})(x-\bar{5})$.

Suy ra $\varphi_1(\bar{2}) = \bar{3}\ \varphi_2(\bar{5}) = \bar{6} = \bar{2}, \varphi_3(\bar{3}) = -\bar{2}$. Đặt $\rho_1 = \frac{1}{\bar{3}}\varphi_1 = \overline{34}\varphi_1$, $\rho_2 = \frac{1}{6}\varphi_2 = \overline{17}\varphi_2$, $\rho_3 = -\frac{1}{\bar{2}}\varphi_3 = \overline{50}\varphi_3$.

Khi đó tất cả các đa thức cần tìm có dạng

$f(x) = \overline{30}\rho_1(x) + \overline{21}\rho_2(x) - \overline{13}\rho_3(x) + g(x)\varphi(x)$, với $\varphi(x) \in \mathbb{Z}_{101}[x]$.

**Bài 3.12**

- Nếu $f(x)$ không bất khả qui thì $f(x) = g(x)\,h(x)$ với $g(x)$, $h(x)$ không khả nghịch . Suy ra $f(ax + b) = g(ax + b)\,h(ax + b)$ với $g(ax + b)$ và $h(ax + b)$ không khả nghịch. Như vậy $f(ax + b)$ không bất khả qui.
- Ngược lại nếu $h(x) = f(ax + b)$ không bất khả qui thì theo trên $h(\frac{x-b}{a}) = f(x)$ cũng không bất khả qui.

**Bài 3.13**

a) Giả sử $f(x) = g(x).h(x)$ với $g(x)$, $h(x)$ có hệ số nguyên.Vì $f(a_i) = -1$ nên: hoặc $g(a_i) = 1$, $h(a_i) = -1$ hoặc $g(a_i) = -1$, $h(a_i) = 1$.

Khi đó $g(a_i) + h(a_i) = 0$, nếu $g(x)$ và $h(x)$ không phải là hằng số thì bậc của $g(x) + h(x)$ bé hơn $n$ do đó $g(x) + h(x) = 0$.Vì vậy $f(x) = -g(x)^2$. Đó là điều không thể được vì hệ số cao nhất của $f(x)$ là $1>0$.

b) Đa thức $f(x)$ không có nghiệm thực, vì nó là số dương với mọi giá trị của $x$. Do đó nếu nó phân tích được thì các nhân tử $g(x)$, $h(x)$ của nó cũng không có nghiệm thực cho nên không đổi dấu với mọi giá trị của $x$. Có thể coi $g(x) > 0$, $h(x) > 0$ với mọi giá trị của $x$. Vì $f(a_k) = 1$ nên $g(a_k) = h(a_k) = 1$. Nếu bậc của $g$ hoặc của $h$ bé hơn $n$ thì chúng phải là các đa thức đồng nhất bằng 1, do đó cả $g$ và $h$ đều phải có bậc là $n$.

Ta có:

$g = 1 + a(x - a_1) \ldots (x - a_n)$,

$h = 1 + b(x - a_1)\ldots(x - a_n)$.

Trong đó $a$ và $b$ là những số nguyên nào đó. Nhưng như thế thì

$f = (x - a_1)^2\ldots(x - a_n)^2 + 1 = 1 + (a+b)(x - a_1)\ldots(x - a_n) + ab(x - a_1)^2\ldots(x - a_n)^2$

So sánh hệ số cao nhất ở hai vế ta được $ab = 1$. So sánh hệ số tự do ở hai vế ta được $a_1^2\ldots a_n^2 + 1 = 1 + (-1)^n a_1\ldots a_n\,(a+b) + a_1^2 \ldots a_n^2$.

Như vậy $ab = 1$, $a+b = 0$. Vô lý.

**Bài 3.14** Trên $\mathbb{R}$

a) $f(x) = (x + 1)(x + 3)(x - 2)(x^2 + 3)$.
b) $f(x) = (x + 2)(x + 3)(x - 3)(x^2 + 2)$.
c) $f(x) = (x - 1)(x + 2)(x - 3)(x^2 + 1)$.
d) $f(x) = (x + 1)^3(4x - 1)(2x - 5)^2$.

**Bài 3.15**

a) Phân tích theo lũy thừa của $x-1$ , áp dụng Eisensteinvới $p=2$
b) Phân tích theo lũy thừa của $x-1$ , áp dụng Eisenstein với $p=3$
c) $f(x)=\dfrac{x^p-1}{x-1}$ . Suy ra

$$f(x+1)=\frac{(x+1)^p-1}{x+1-1}=\frac{x^p+px^{p-1}+\ldots+C_p^kx^k+\ldots+px}{x}=$$

$$=x^p+px^{p-2}+\ldots+C_p^kx^{k-1}+\ldots+p$$

Áp dụng Eisenstein với $p$.
d) $f(x)$ bậc 3 bất khả qui khi và chỉ khi không có nghiệm hữu tỷ.
e) như d)
f) $x^3-3n^2x+n^3=0\Leftrightarrow(x/n)^3-3(x/n)+1=0$ không có nghiệm hữu tỷ.
g) Kiểm tra thấy rằng $f(x)$ không có nghiệm hữu tỷ . Do đó nếu $f(x)$ khả qui thì $f(x)$ là tích của hai đa thức bậc 2 hệ số nguyên.
$f(x)=(3x^2+ax+1)(x^2+bx+1)$ (1)
hoặc $f(x)=(3x^2+ax-1)(x^2+bx-1)$ (2)
Nếu xảy ra (1) cân bằng hệ số hai vế suy ra $2b=9$. Vô lý.
Nếu xảy ra (2) cân bằng hệ số hai vế suy ra $2b=1$. Vô lý.
h) Như g)
i) Như h).

**Bài 3.19**.

Giả sử $p/q$ là nghiệm của $f(x)$ . Vì $p$ là ước của $f(0)$ và $p-q$ là ước của $f(1)$ (tính chất) mà cả hai số đều lẻ nên $q$ là số chẵn , do đó $p/q$ không thể là số nguyên.

Cách khác: Ta dễ chứng minh rằng $f(a)-f(b)$ chia hết cho $a-b$ với mọi $a, b$.
Giả sử $f(x)$ có nghiệm nguyên $x_0$ .Ta có $f(1)=f(1)-f(x_0)\vdots x_0-1$ và $f(0)=f(0)-f(x_0)\vdots x_0$ . Hai số nguyên liên tiếp $x_0$ và $x_0-1$ có một số chẵn , suy ra $f(0)$ hay $f(1)$ chẵn.

**Bài 3.20**

a) Điều kiện cần.
Phản chứng:
- Nếu $p^2-4q$ là bình phương của số hữu tỷ thì tam thức bậc hai $X^2+pX+q$ có hai nghiệm hữu tỷ là $x_1$ và $x_2$ , khi đó $x^4+px^2+q$ khả qui vì có sự phân tích $(x^2-x_1)(x^2-x_2)$.
- Nếu $2\sqrt{q}-p=a^2$ là bình phương của số hữu tỷ $a$ thì $q=n^2$ là bình phương của số hữu tỷ $n=\dfrac{1}{2}(p+a^2)$ và $x^4+px^2+q$ khả qui vì có sự phân tích $x^4+px^2+q=(x^2+ax+n)(x^2-ax+n)$.

b) Điều kiện đủ.

Phản chứng:

Giả sử $x^4+px^2+q$ khả qui, ta chứng minh $p^2-4q$ hoặc $2\sqrt{q}-p$ là bình phương của số hữu tỷ. Giả sử $x^4+px^2+q=(x^2+ax+m)(x^2+bx+n)$. Khi đó ta có hệ

$$\begin{cases} a+b=0 \\ m+n+ab=p \\ an+bm=0 \\ mn=q \end{cases}$$

- Nếu $a=0$, suy ra $b=0$ và $m+n=p$, $mn=q$, do đó $m, n$ là hai nghiệm hữu tỷ của tam thức bậc hai $X^2-pX+q$ vì vậy $\Delta=p^2-4q$ là bình phương của số hữu tỷ.

- Nếu $a\neq 0$ thì $a=-b\neq 0$ suy ra $m=n$ và $n^2=q$, $2n-a^2=p$ do đó $2\sqrt{q}-p$ là bình phương của số hữu tỷ.

---