TRƯỜNG ĐẠI HỌC TRÀ VINH
KHOA KHOA HỌC CƠ BẢN

ISO 9001 : 2008

TÀI LIỆU GIẢNG DẠY

ĐẠI SỐ ĐẠI CƯƠNG

LƯU HÀNH NỘI BỘ

Chương 1: NỬA NHÓM VÀ NHÓM

1.1. Phép toán hai ngôi

1.1.1. Định nghĩa: Phép toán hai ngôi (gọi tắt là phép toán) trên tập hợp X là một ánh xạ

$$f: X \times X \to X$$
$$(x,y) \mapsto f(x,y)$$

Ta dùng ký hiệu xfy thay cho $f(x,y)$. Như vậy, ứng với các phép toán $*,\circ,\cdot,+,...$ ta có các ký hiệu $x*y, x\circ y, x\cdot y, x+y, ...$ Khi ký hiệu phép toán là . ta gọi đây là phép toán nhân và thường viết xy thay cho $x.y$ mà ta gọi là tích của x và y. Còn khi ký hiệu phép toán là + ta gọi đây là phép toán cộng và $x+y$ là tổng của x và y.

1.1.2. Ví dụ

Ví dụ 1: Phép cộng và phép nhân thông thường trên các tập hợp $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ là các phép toán.

Ví dụ 2: Phép cộng và phép nhân ma trận là các phép toán trên $M(n,\mathbb{R})$ gồm các ma trận vuông cấp n với hệ số thực.

1.1.3. Định nghĩa: Cho phép toán * trên tập hợp X. Ta nói phép toán *

- *Giao hoán*, nếu với mọi $x,y \in X$, $x*y = y*x$

- *Kết hợp*, nếu với mọi $x,y,z \in X$, $(x*y)*z = x*(y*z)$

- Có *phần tử trung hòa trái* (tương ứng *phải*) là e nếu $e \in X$ và với mọi $x \in X$, $e*x = x$ (tương ứng $x*e = x$). Nếu e vừa là phần tử trung hòa trái vừa là phần tử trung hòa phải thì ta nói e là *phần tử trung hòa* của phép toán *.

1.1.4. Mệnh đề: Một phép toán có nhiều nhất một phần tử trung hòa.

Chứng minh: Giả sử e' và e'' là 2 phần tử trung hòa của phép toán *. Xét phần tử $e'*e''$. Vì e' là phần tử trung hòa trái nên $e'*e'' = e''$. Mặt khác vì e'' là phần tử trung hòa phải nên $e'*e'' = e'$. Suy ra $e' = e''$. ***(đpcm)***

Nhận xét: Từ chứng minh của mệnh đề 1.1.4 ta thấy nếu e' là phần tử trung hòa trái và e'' là phần tử trung hòa phải của phép toán * thì $e' = e''$. Đặc biệt, nếu trong X tồn tại phần tử trung hòa e thì đó là phần tử trung hòa trái duy nhất đồng thời cũng là phần tử trung hòa phải duy nhất.

1.1.5. Định nghĩa: Cho * là một phép toán trên tập hợp X có phần tử trung hòa e và x là một phần tử tùy ý của X. Ta nói x *khả đối xứng trái* (tương ứng *phải*) nếu tồn tại $x' \in X$ sao cho $x' * x = e$ (tương ứng $x * x' = e$). Khi đó x' được gọi là *phần tử đối xứng trái* (tương ứng *phải*) của x. Trường hợp x vừa khả đối xứng trái vừa khả đối xứng phải thì ta nói x khả đối xứng và phần tử $x' \in X$ thỏa $x' * x = x * x' = e$ được gọi là *phần tử đối xứng* của x.

1.1.6. Mệnh đề: Nếu phép toán * kết hợp thì một phần tử có nhiều nhất một phần tử đối xứng.

Chứng minh: Giả sử x' và x'' là 2 phần tử đối xứng của x. Khi đó $x' * x = e$ và $x * x'' = e$.

Do đó: $x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$. ***(đpcm)***

Nhận xét: Từ chứng minh của mệnh đề 1.1.6 ta thấy khi phép toán * kết hợp, nếu x' là phần tử đối xứng trái của x và x'' là phần tử đối xứng phải của x thì $x' = x''$. Đặc biệt, nếu x khả đối xứng và x' là phần tử đối xứng của x thì x' là phần tử đối xứng trái duy nhất và cũng là phần tử đối xứng phải duy nhất của x.

1.1.7. Thuật ngữ và ký hiệu

i) Trường hợp phép toán cộng: Phần tử trung hòa được gọi là *phần tử không* và được ký hiệu là 0, tính chất khả đối xứng được gọi là *khả đối*, phần tử đối xứng của x được gọi là *phần tử đối* của x và ký hiệu là $-x$.

ii) Trường hợp phép toán nhân: Phần tử trung hòa được gọi là *phần tử đơn vị* và được ký hiệu là 1, tính chất khả đối xứng được gọi là *khả nghịch*, phần tử đối xứng của x được gọi là *phần tử nghịch đảo* của x và ký hiệu là x^{-1}.

Từ đây trở về sau, ta dùng phép toán nhân để chỉ một phép toán tùy ý trên tập hợp đang khảo sát.

1.2. Nửa nhóm

1.2.1. Định nghĩa: Cho tập hợp X với phép toán nhân. Ta nói $(X,.)$ (gọi tắt là X) là:

i) Một *nửa nhóm* nếu phép toán nhân kết hợp trên X.

ii) Một *vị nhóm* nếu phép toán nhân kết hợp trên X và có phần tử trung hòa trên X.

Một nửa nhóm được gọi là *giao hoán* hay *Abel* nếu phép toán tương ứng giao hoán.

1.2.2. Ví dụ

Ví dụ 1: Với phép cộng thông thường, các tập hợp $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ trở thành các vị nhóm giao hoán.

Ví dụ 2: Với phép cộng thông thường, tập hợp $\mathbb{N}^*$ gồm các số nguyên dương trở thành một nửa nhóm giao hoán nhưng không là vị nhóm.

1.2.3. Ký hiệu: Trong nửa nhóm $(X,.)$, do phép toán nhân kết hợp nên với mọi x,y,z: $(xy)z = x(yz)$

Giá trị chung của hai vế trong đẳng thức trên được ký hiệu là xyz và gọi là *tích* của các phần tử x,y,z theo thứ tự đó. Bằng quy nạp, ta định nghĩa *tích* của *n* phần tử $x_1,x_2,...,x_n$ như sau: $x_1x_2...x_n = x_1(x_2...x_n)$

Ta có định lý sau:

1.2.4. Định lý: Cho $x_1,x_2,...,x_n$ là n phần tử tùy ý của nửa nhóm $(X,.)$ với $n \geq 3$. Khi đó: $x_1x_2...x_n = (x_1...x_i)(x_{i+1}...x_j)...(x_{k+1}...x_n)$, trong đó $1 \leq i < j < ... < k < n$.

1.2.5. Ký hiệu: Trong nửa nhóm $(X,.)$, tích của n phần tử, mỗi phần tử đều bằng x, được gọi là *lũy thừa* bậc n của x và được ký hiệu là x^n. Ta có:

$$x^m x^n = x^{m+n} \text{ và } (x^m)^n = x^{mn},\ \forall m,n \in \mathbb{N}^*$$

Trường hợp nửa nhóm cộng $(X,+)$, tổng của n phần tử được gọi là *bội* n của x và được ký hiệu là nx. Khi đó: $mx + nx = (m+n)x$ và $m(nx) = (mn)x$

1.2.6. Định lý: Trong nửa nhóm giao hoán, tích của n phần tử tùy ý không phụ thuộc vào thứ tự các phần tử.

1.3. Nhóm

1.3.1. Định nghĩa: *Nhóm* là một vị nhóm mà mọi phần tử đều khả đối xứng. Nói cách khác, tập hợp G khác rỗng với phép toán nhân được gọi là một nhóm nếu các tính chất sau được thỏa:

(G_1) Với mọi $x,y,z \in G$, $(xy)z = x(yz)$;

(G_2) Tồn tại $e \in G$ sao cho với mọi $x \in G$, $ex = xe = x$;

(G_3) Với mọi $x \in G$, tồn tại $x^{-1} \in G$ sao cho $xx^{-1} = x^{-1}x = e$.

Nếu phép toán trên G là phép cộng thì các tính chất trên trở thành:

(G_1) Với mọi $x,y,z \in G$, $(x+y)+z = x+(y+z)$;

(G_2) Tồn tại $0 \in G$ sao cho với mọi $x \in G$, $0+x = x+0 = x$;

(G_3) Với mọi $x \in G$, tồn tại $-x \in G$ sao cho $x+(-x) = (-x)+x = 0$.

Trường hợp phép toán trên nhóm G giao hoán thì ta nói G là *nhóm giao hoán* hay là *nhóm Abel*.

Nhóm G được gọi là *nhóm hữu hạn* khi tập hợp G hữu hạn. Khi đó số phần tử của G được gọi là *cấp* của nhóm G. Nếu nhóm G không hữu hạn thì ta nói G là *nhóm vô hạn*.

1.3.2. Ví dụ

Ví dụ 1: Tập hợp các số nguyên $\mathbb{Z}$ cùng với phép cộng thông thường là một nhóm giao hoán mà ta gọi là nhóm cộng các số nguyên. Tương tự ta có nhóm cộng các số hữu tỷ $\mathbb{Q}$, nhóm cộng các số thực $\mathbb{R}$ và nhóm cộng các số phức $\mathbb{C}$.

Ví dụ 2: Tập hợp các số hữu tỷ khác không $\mathbb{Q}^*$ cùng với phép nhân thông thường là một nhóm giao hoán mà ta gọi là nhóm nhân các số hữu tỷ khác không. Tương tự ta có nhóm nhân các số thực khác không $\mathbb{R}^*$ và nhóm nhân các số phức khác không $\mathbb{C}^*$.

Ví dụ 3: Với $X = \{1,2,...,n\}$, đặt $S_n = \{\sigma \mid \sigma : X \to X\}$ là một song ánh

Khi đó S_n với phép hợp nối ánh xạ là một nhóm (có phần tử đơn vị là ánh xạ đồng nhất Id_X và phần tử nghịch đảo của $\sigma \in S_n$ chính là ánh xạ ngược σ^{-1}). Ta gọi $(S_n, \circ)$ là nhóm hoán vị hay nhóm đối xứng bậc n. Đây là một nhóm hữu hạn có cấp n!

Ví dụ 4: Tập hợp $GL(n,\mathbb{R})$ gồm các ma trận vuông cấp n, khả nghịch với hệ số thực cùng với phép nhân ma trận là một nhóm không giao hoán với mọi $n > 1$ (với phần tử đơn vị là ma trận đơn vị I_n và phần tử nghịch đảo của $A \in GL(n,\mathbb{R})$ chính là ma trận nghịch đảo A^{-1}). Ta gọi $GL(n,\mathbb{R})$ là *nhóm tuyến tính đầy đủ* bậc n (hay *nhóm tuyến tính tổng quát* bậc n) trên $\mathbb{R}$.

1.3.3. Định lý: Cho nhóm $(G,.)$ và $x,y,x_1,...,x_n \in G$. Khi đó:

(i) Phần tử đơn vị e là duy nhất.

(ii) Phần tử nghịch đảo x^{-1} của x là duy nhất và $\left(x^{-1}\right)^{-1} = x$.

(iii) $xy = e$ khi và chỉ khi $yx = e$. Hơn nữa khi đó $y = x^{-1}$.

(iv) $\left(x_1...x_n\right)^{-1} = x_n^{-1}...x_1^{-1}$. Đặc biệt $\left(x^n\right)^{-1} = \left(x^{-1}\right)^n$ với mọi n nguyên dương.

(v) Phép toán nhân có tính giản ước, nghĩa là với mọi $x,y,z \in G$, từ đẳng thức $xy = xz$ hay $yx = zx$ đều dẫn đến $y = z$.

Chứng minh: (i) được suy ra từ mệnh đề 1.1.4

(ii) được suy ra từ mệnh đề 1.1.6

(iii) được suy ra từ nhận xét của mệnh đề 1.1.6

(iv) Chỉ cần nhận xét rằng $\left(x_1...x_n\right)\left(x_n^{-1}...x_1^{-1}\right) = \left(x_1...x_{n-1}\right)\left(x_n x_n^{-1}\right)\left(x_{n-1}^{-1}...x_1^{-1}\right)$

$= \left(x_1...x_{n-1}\right)\left(x_{n-1}^{-1}...x_1^{-1}\right) = \ldots\ldots\ldots\ldots = e$. Sau đó sử dụng (iii).

(v) Từ đẳng thức $xy = xz$ ta suy ra $x^{-1}\left(xy\right) = x^{-1}\left(xz\right)$ hay $\left(x^{-1}x\right)y = \left(x^{-1}x\right)z$, nghĩa là $y = z$. Tương tự, từ đẳng thức $yx = zx$ cũng dẫn đến $y = z$.

1.3.4. Ký hiệu: Trong nhóm nhân $(G,.)$ ta dùng ký hiệu x^{-n} để chỉ phần tử $\left(x^{-1}\right)^n$ với mọi n nguyên dương và đặt $x^0 = e$. Như vậy ta đã định nghĩa lũy thừa bậc n của một phần tử bất kỳ trong một nhóm nhân với n nguyên.

Chú ý rằng, do tính chất (iv) trong định lý 1.3.3, các công thức $x^m.x^n = x^{m+n}$ và $\left(x^m\right)^n = x^{mn}$ (hay $mx + nx = \left(m+n\right)x$ và $m\left(nx\right) = \left(mn\right)x$ đối với nhóm cộng) vẫn còn đúng với mọi m,n nguyên.

1.3.5. Định lý: Cho $(G,.)$ là một nửa nhóm khác rỗng. Các mệnh đề sau tương đương

(i) $(G,.)$ là một nhóm;

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

(iii) Trong G có phần tử đơn vị trái e và với mọi $x \in G$, tồn tại $x' \in G$ sao cho $x'x = e$;

(iv) Trong G có phần tử đơn vị phải e' và với mọi $x \in G$, tồn tại $x'' \in G$ sao cho $xx'' = e'$.

Chứng minh: $(i) \Rightarrow (ii)$ Ta có $x = a^{-1}b$ và $y = ba^{-1}$ lần lượt là các nghiệm của phương trình $ax = b$ và $ya = b$.

$(ii) \Rightarrow (iii)$ Do $G \neq \phi$ nên tồn tại $a_0 \in G$. Gọi e là nghiệm của phương trình $ya_0 = a_0$. Khi đó e là phần tử đơn vị trái. Thật vậy, với b là một phần tử tùy ý của *G*, gọi c là nghiệm của phương trình $a_0 x = b$, khi đó $a_0 c = b$ nên $eb = e(a_0 c) = (ea_0)c = a_0 c = b$. Vậy e là phần tử đơn vị trái.

Tính chất sau cùng trong (iii) được suy từ giả thiết mọi phương trình dạng $ya = e$ đều có nghiệm trong *G*.

$(iii) \Rightarrow (i)$ Giả sử trong *G* có phần tử đơn vị trái e và với mọi $x \in G$, tồn tại $x' \in G$ sao cho $x'x = e$. Ta chứng minh e là phần tử đơn vị và x' là phần tử nghịch đảo của x. Theo giả thiết với x' như trên tồn tại $x'' \in G$ sao cho $x''x' = e$. Do đó:
$xx' = e(xx') = (x''x')(xx') = x''(x'x)x' = x''ex' = x''x' = e$

Suy ra $xe = x(x'x) = (xx')x = ex = x$.

Các kết quả trên chứng tỏ e là phần tử đơn vị và $x' = x^{-1}$. Do đó $(G,.)$ là một nhóm.

Tương tự ta cũng có $(i) \Rightarrow (ii)$, $(ii) \Rightarrow (iv)$ và $(iv) \Rightarrow (i)$. Do đó định lý được chứng minh.

1.4. Nhóm con

1.4.1. Định nghĩa:

- Một tập con H của nhóm $(G,.)$ được gọi là *tập con ổn định* của nhóm G nếu với mọi $x, y \in H, xy \in H$. Khi đó phép toán nhân thu hẹp trên H xác định một phép toán trên H mà ta gọi là phép toán cảm sinh trên H (từ phép toán trên G).

- *Nhóm con H* của nhóm G là một tập con ổn định của nhóm G sao cho cùng với phép toán cảm sinh H là một nhóm. Ký hiệu $H \leq G$ để chỉ H là một nhóm con của G.

Định lý sau đây cho ta dấu hiệu để nhận biết nhóm con của một nhóm cho trước.

1.4.2. Định lý: Cho H là một tập con khác rỗng của nhóm $(G,.)$. Các mệnh đề sau tương đương:

i) $H \le G$;

ii) Với mọi $x,y \in H, xy \in H$ và $x^{-1} \in H$;

iii) Với mọi $x,y \in H, x^{-1}y \in H$.

Chứng minh: $(i) \Rightarrow (ii)$ Trước hết ta chứng minh phần tử đơn vị e' của nhóm con H cũng chính là phần tử đơn vị e của G. Thật vậy, $\forall x \in H$ ta có $e'x = x = ex$ nên do tính giản ước ta suy ra $e' = e$. Bây giờ gọi x' là phần tử nghịch đảo của x trong nhóm con H, ta có $x'x = e = x^{-1}x$, do đó $x^{-1} = x' \in H$. Tính chất $xy \in H$ được suy từ tính chất nhóm con H là một tập hợp con ổn định của G.

$(ii) \Rightarrow (iii)$ $\forall x,y \in H$, giả thiết (ii) cho ta $x^{-1} \in H$ và do đó $x^{-1}y \in H$.

$(iii) \Rightarrow (i)$ Vì $H \neq \phi$ nên tồn tại $a \in H$ và do đó $e = a^{-1}a \in H$. Bây giờ $\forall x \in H, x^{-1} = x^{-1}e \in H$. Cuối cùng, $\forall x,y \in H$, do $x^{-1} \in H$ nên $xy = \left(x^{-1}\right)^{-1} y \in H$. Suy ra $H \le G$.

1.4.3. Ví dụ

Ví dụ 1: Các tập hợp $\{e\}$ và G đều là các nhóm con của G. Ta gọi đây là các nhóm con tầm thường của G.

Ví dụ 2: $\mathbb{Z} \le \mathbb{Q} \le \mathbb{R} \le \mathbb{C}$ và $\mathbb{Q}^* \le \mathbb{R}^* \le \mathbb{C}^*$.

Ví dụ 3: Tập hợp $SL(n,\mathbb{R})$ gồm các ma trận vuông cấp n với hệ số thực có định thức bằng 1 là một nhóm con của nhóm tuyến tính đầy đủ $GL(n,\mathbb{R})$. Ta gọi nhóm $SL(n,\mathbb{R})$ là nhóm tuyến tính đặc biệt bậc n trên $\mathbb{R}$.

1.4.4. Định lý: Giao của một họ không rỗng các nhóm con của một nhóm G cũng là nhóm con của G.

Chứng minh: Giả sử $\{H_i\}_{i \in I}$ là một họ không rỗng các nhóm con của nhóm $(G,.)$.

Đặt $H=\bigcap_{i\in I}H_i$. Khi đó $H\neq\phi$ vì $e\in H$. Với mọi $x,y\in H$ ta có $x,y\in H_i,\forall i\in I$ nên theo định lý 1.4.2 thì $x^{-1}y\in H_i,\forall i\in I$, nghĩa là $x^{-1}y\in H$. Suy ra $H\leq G$. ***(đpcm)***

Bây giờ cho S là một tập hợp con của nhóm G. Ta xét họ tất cả các nhóm con của G chứa S. Họ này không rỗng vì chứa G. Theo định lý 1.4.4 giao của họ đó là một nhóm con của G. Hiển nhiên đây là một nhóm con nhỏ nhất của G chứa S. Ta có định nghĩa sau:

1.4.5. Định nghĩa: Cho S là một tập con của nhóm G. *Nhóm con sinh bởi S* là nhóm con nhỏ nhất của G chứa S và được ký hiệu là $\langle S\rangle$. Tập hợp S được gọi là *tập sinh* của nhóm $\langle S\rangle$. Nếu S hữu hạn $S=\{x_1,...,x_n\}$ thì ta nói $\langle S\rangle$ là *nhóm hữu hạn sinh* với các phần tử sinh $x_1,...,x_n$ mà ta thường ký hiệu nhóm này là $\langle x_1,...,x_n\rangle$.

Định lý sau đây mô tả các nhóm con sinh bởi một tập hợp:

1.4.6. Định lý: Cho S là một tập con của nhóm G. Khi đó

i) Nếu $S=\phi$ thì $\langle S\rangle=\{e\}$.

ii) Nếu $S=\phi$ thì $\langle S\rangle=\{x_1^{\alpha_1}...x_n^{\alpha_n}\mid n\in\mathbb{N}^*,x_i\in S,\alpha_i=\pm1\}$.

Chứng minh: Khẳng định (i) là hiển nhiên.

Ta chứng minh (ii). Thật vậy, ký hiệu vế phải của đẳng thức trong (ii) là H. Vì nhóm con $\langle S\rangle$ chứa tất cả các phần tử x_i của S nên $\langle S\rangle$ chứa H. Mặt khác, do cách đặt H ta thấy nếu $x,y\in H$ thì $xy\in H$ và $x^{-1}\in H$ nên H là một nhóm con của G. Từ đây, do H chứa S nên ta có H chứa $\langle S\rangle$. Suy ra $H=\langle S\rangle$.

1.4.7. Ví dụ

Ví dụ 1: Ta có $\mathbb{Z}=\langle 1\rangle$ và $\mathbb{Q}=\left\langle\frac{1}{n}\mid n\in\mathbb{N}^*\right\rangle$.

Ví dụ 2: Ta có $\mathbb{Q}^*=\langle P\rangle$, trong đó $P=\{-1\}\cup\{p\}$ với p nguyên tố dương.

1.4.8. Chú ý: Nếu H và K là hai nhóm con của nhóm G thì $H\cup K$ không nhất thiết là một nhóm con của G. Ta ký hiệu $H\vee K$ để chỉ nhóm con sinh bởi $H\cup K$.

1.5. Nhóm con cyclic và nhóm cyclic

1.5.1. Định nghĩa: Cho G là một nhóm. Nhóm con $\langle a \rangle$ của G sinh bởi phần tử $a \in G$ được gọi là *nhóm con cyclic sinh bởi a*. Nếu tồn tại phần tử $a \in G$ sao cho $\langle a \rangle = G$ thì ta nói G là một *nhóm cyclic* và a là *phần tử sinh* của G.

Từ định lý 1.4.6 ta suy ra mệnh đề sau:

1.5.2. Mệnh đề: *Nhóm con cyclic sinh bởi a là tập hợp gồm tất cả các lũy thừa* a^n *với* $n \in Z$, *nghĩa là* $\langle a \rangle = \{a^n \mid n \in Z\}$.

Cho $(G,.)$ là một nhóm và $a \in G$. Xét nhóm con cyclic $\langle a \rangle$. Khi đó có 2 trường hợp có thể xảy ra

Trường hợp 1: Tất cả các lũy thừa $a^n (n \in Z)$ đều khác nhau từng đôi một. Trong trường hợp này $\langle a \rangle$ là nhóm vô hạn.

Trường hợp 2: Tồn tại những lũy thừa của a bằng nhau, chẳng hạn $a^k = a^l (k > l)$. Khi đó $a^{k-l} = e$ với $k - l > 0$. Do đó tồn tại những số nguyên dương m sao cho $a^m = e$. Gọi n là số nguyên dương nhỏ nhất sao cho $a^n = e$. Khi đó các phần tử $e, a, ..., a^{n-1}$ đôi một khác nhau và $\langle a \rangle = \{e, a, ..., a^{n-1}\}$.

Tóm lại, nếu tất cả các lũy thừa của a đều khác nhau thì $\langle a \rangle$ là nhóm vô hạn, còn nếu tồn tại những lũy thừa của a bằng nhau thì $\langle a \rangle$ là nhóm hữu hạn cấp n: $\langle a \rangle = \{e, a, ..., a^{n-1}\}$, trong đó n là số nguyên dương nhỏ nhất sao cho $a^n = e$. Từ đây ta có định nghĩa sau:

1.5.3. Định nghĩa: *Cấp* của một phần tử a trong nhóm G là cấp của nhóm con cyclic $\langle a \rangle$. Ta thường ký hiệu $o(a)$ hay $|a|$ để chỉ cấp của phần tử a.

Từ định nghĩa 1.5.3 và theo lý luận trên ta có hệ quả sau:

1.5.4. Hệ quả: Cho $(G,.)$ là một nhóm và $a \in G$. Ta có

i) a có cấp vô hạn khi và chỉ khi với mọi $k \in \mathbb{Z}$, nếu $a^k = e$ thì $k = 0$.

ii) a có cấp hữu hạn khi và chỉ khi tồn tại $k \in \mathbb{Z}^*$ sao cho $a^k = e$.

iii) Nếu a có cấp hữu hạn thì cấp của a là số nguyên dương n nhỏ nhất sao cho $a^n = e$. Hơn nữa, khi đó với mọi $k \in \mathbb{Z}$, $a^k = e$ khi và chỉ khi k là bội số của n.

1.5.5. Ví dụ

Ví dụ 1: Nhóm cộng các số nguyên $\mathbb{Z}$ là nhóm cyclic sinh bởi 1.

Ví dụ 2: Với mỗi n nguyên dương, quan hệ đồng dư modulo n trên $\mathbb{Z}$ định bởi: $x \equiv y(mod\, n) \Leftrightarrow x - y$ chia hết cho n.

Đây là một quan hệ tương đương trên $\mathbb{Z}$ với các lớp tương đương là $\bar{x} = \{x + kn \mid k \in Z\}$.

Tập thương của $\mathbb{Z}$ theo quan hệ đồng dư modulo n định bởi $\mathbb{Z}_n = \{\bar{x} \mid x \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}$.

Trên $\mathbb{Z}_n$ ta định nghĩa phép toán cộng như sau $\bar{x} + \bar{y} = \overline{x+y}$

Kiểm chứng dễ dàng rằng định nghĩa trên được hoàn toàn xác định và $\mathbb{Z}_n$ trở thành một nhóm giao hoán. Hơn nữa, $\mathbb{Z}_n$ là nhóm cyclic hữu hạn cấp n sinh bởi $\bar{1}$. Ta gọi $\mathbb{Z}_n$ là *nhóm cộng các số nguyên modulo n*.

1.5.6. Định lý: Mọi nhóm con của nhóm cyclic đều là nhóm cyclic. Hơn nữa, nếu $H \le \langle a \rangle$ và $H \ne \{e\}$ thì $H = \langle a^n \rangle$ trong đó n là số nguyên dương nhỏ nhất sao cho $a^n \in H$.

Chứng minh: Giả sử $H \subset \langle a \rangle$. Nếu $H = \{e\}$ thì hiển nhiên H là nhóm con cyclic sinh bởi e.

Xét trường hợp $H \ne \{e\}$. Khi đó tồn tại $k \in \mathbb{Z}^*$ sao cho $a^k \in H$. Vì a^k và $a^{-k} = (a^k)^{-1}$ đều thuộc H nên có thể khẳng định rằng tồn tại $l \in \mathbb{N}^*$ sao cho $a^l \in H$. Gọi n là số nguyên dương nhỏ nhất sao cho $a^n \in H$. Ta chứng minh $H = \langle a^n \rangle$. Thật vậy, hiển nhiên $\langle a^n \rangle \subseteq H$. Ngược lại, cho $x = a^m \in H$. Lấy m chia cho n ta tìm được $q, r \in \mathbb{Z}$ sao cho $m = qn + r$ với $0 \le r < n$. Vì $a^r = a^m (a^n)^{-q} \in H$ nên theo định nghĩa của n ta phải có $r = 0$, nghĩa là $m = qn$ và $x = (a^n)^q \in \langle a^n \rangle$. Điều này chứng tỏ $H \subset \langle a^n \rangle$. Vậy $H = \langle a^n \rangle$.

Từ định lý 1.5.6 ta suy ra hệ quả sau:

1.5.7. Hệ quả: H là một nhóm con của nhóm cộng các số nguyên $\mathbb{Z}$ khi và chỉ khi H có dạng $n\mathbb{Z}$ với $n \in \mathbb{N}$, trong đó $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.

1.6. Nhóm con chuẩn tắc và nhóm thương

1.6.1. Định lý: Cho $(G,.)$ là một nhóm và H là một nhóm con của G. Xét quan hệ $\sim$ trên G như sau: $x \sim y \Leftrightarrow x^{-1}y \in H$. Khi đó

i) $\sim$ là một quan hệ tương đương trên G.

ii) Lớp tương đương chứa x là $\bar{x} = xH$, trong đó $xH = \{xh \mid h \in H\}$.

Ta gọi xH là *lớp ghép trái* của H (bởi phần tử x). Tập hợp thương của G theo quan hệ $\sim$, ký hiệu là G/H được gọi là *tập thương* của G trên H và $|G/H|$ là *chỉ số* của nhóm con H trong G, ký hiệu là $[G:H]$.

Chứng minh: i) Tính phản xạ: $\forall x \in G, x \sim x$ vì $x^{-1}x = e \in H$.

Tính đối xứng: $\forall x,y \in G$, nếu $x \sim y$ thì $x^{-1}y \in H$ nên $y^{-1}x = \left(x^{-1}y\right)^{-1} \in H$, nghĩa là $y \sim x$.

Tính bắc cầu: $\forall x,y,z \in G$, nếu $x \sim y$ và $y \sim z$ thì $x^{-1}y \in H$ và $y^{-1}z \in H$ nên $x^{-1}z = \left(x^{-1}y\right)\left(y^{-1}z\right) \in H$, nghĩa là $x \sim z$.

Vậy $\sim$ là một quan hệ tương đương trên G.

(ii) Ta có: $x \sim y \Leftrightarrow x^{-1}y \in H \Leftrightarrow \exists h \in H, x^{-1}y = h \Leftrightarrow \exists h \in H, y = xh$

Suy ra $\bar{x} = \{y \in G \mid x \sim y\} = \{xh \mid h \in H\} = xH$. ***(đpcm)***

1.6.2. Chú ý: Hoàn toàn tương tự ta định nghĩa được quan hệ $\sim'$ trên G như sau: $x \sim' y \Leftrightarrow xy^{-1} \in H$. Khi đó $\sim'$ cũng là một quan hệ tương đương trên G và lớp tương đương chứa x là $\bar{x} = Hx$, trong đó $Hx = \{hx \mid h \in H\}$. Ta gọi Hx là *lớp ghép phải* của H (bởi phần tử x).

Định lý sau đây cho ta thông tin về cấp của các nhóm con của các nhóm hữu hạn.

1.6.3. Định lý Lagrange: Cho G là một nhóm hữu hạn và H là một nhóm con của G. Khi đó $|G| = |H|[G:H]$.

Chứng minh: Nếu xH là một lớp ghép trái thì ánh xạ

$\varphi: \begin{array}{l} H \to xH \\ h \mapsto xh \end{array}$ là một song ánh. Thật vậy, φ là toàn ánh do định nghĩa của tập hợp xH, φ là đơn ánh vì nếu $xh = xk$ thì $h = k$ do tính giản ước của phép toán nhân trong nhóm G. Như vậy số phần tử của các lớp ghép trái đều bằng nhau và bằng $|H|$, số lớp ghép là $[G:H]$. Do đó: $|G| = |H|[G:H]$ ***(đpcm)***

Từ định lý Lagrange ta suy ra hệ quả sau:

1.6.4. Hệ quả: Cho G là một nhóm hữu hạn. Khi đó

i) Cấp của mỗi nhóm con của G là một ước số của cấp của G.

ii) Cấp của mỗi phần tử thuộc G là một ước số của cấp của G.

iii) Nếu G có cấp nguyên tố thì G là nhóm cyclic và G được sinh bởi một phần tử bất kỳ khác e.

Chú ý rằng nếu H là một nhóm con tùy ý của G thì tập thương G/H như đã xây dựng trong định lý 1.6.1 không nhất thiết là một nhóm. Sau đây chúng ta đề cập đến một loại nhóm con đặc biệt mà ứng với nhóm con loại đó tập hợp thương trở thành một nhóm.

1.6.5. Định nghĩa: Một nhóm con H của nhóm $(G,.)$ được gọi là *chuẩn tắc* nếu với mọi $x \in G$ và $h \in H$, $x^{-1}hx \in H$. Ký hiệu $H \lhd G$ để chỉ H là một nhóm con chuẩn tắc của G.

1.6.6. Mệnh đề: Cho H là một nhóm con của nhóm $(G,.)$. Các mệnh đề sau tương đương:

i) $H \lhd G$;

ii) $\forall x \in G, x^{-1}Hx \subset H$;

iii) $\forall x \in G, x^{-1}Hx = H$;

iv) $\forall x \in G, xH = Hx$; trong đó $x^{-1}Hx = \{x^{-1}hx \mid h \in H\}$.

Chứng minh: $(i) \Rightarrow (ii)$: Hiển nhiên do định nghĩa.

$(ii) \Rightarrow (iii)$: Với giả thiết (ii) ta có $x^{-1}Hx \subset H$.

Mặt khác $xHx^{-1} = \left(x^{-1}\right)^{-1} Hx^{-1} \subset H$ nên $H \subset x^{-1}Hx$. Từ đó $x^{-1}Hx = H$.

$(iii) \Rightarrow (iv)$: Theo giả thiết (iii), $x^{-1}Hx = H$ nên $xH = x\left(x^{-1}Hx\right) = Hx$.

$(iv) \Rightarrow (i)$: $\forall x \in G$ và $h \in H$ ta có $hx \in Hx = xH$ nên $\exists k \in H$ sao cho $hx = xk$. Suy ra $x^{-1}hx = k \in H$. Điều này chứng tỏ $H \lhd G$. ***(đpcm)***

1.6.7. Nhận xét:

i) Nếu G giao hoán thì mọi nhóm con của G đều chuẩn tắc.

ii) Các nhóm con tầm thường $\{e\}$ và G đều chuẩn tắc trong G.

1.6.8. Ví dụ: Nhóm tuyến tính đặc biệt $SL(n,\mathbb{R})$ là nhóm con chuẩn tắc của nhóm tuyến tính đầy đủ $GL(n,\mathbb{R})$ vì $\forall X \in GL(n,\mathbb{R})$ và $A \in SL(n,\mathbb{R})$ ta có:

$det(X^{-1}AX) = det(X^{-1})det(A)det(X) = det(A) = 1$, nghĩa là $X^{-1}AX \in SL(n,\mathbb{R})$.

Khi H là một nhóm con chuẩn tắc của G thì tập thương G/H trở thành một nhóm như trong định lý sau:

1.6.9. Định lý: Cho G là một nhóm và H là nhóm con chuẩn tắc của G. Khi đó: **i)** Lớp xyH chỉ phụ thuộc vào các lớp xH và yH mà không phụ thuộc vào sự lựa chọn của các phần tử đại diện x, y của các lớp đó.

ii) Tập thương G/H cùng với phép toán nhân định bởi $(xH)(yH) = xyH$ là một nhóm, gọi là nhóm thương của G trên H.

Chứng minh: i) Giả sử $x_1H = xH$ và $y_1H = yH$, nghĩa là $x^{-1}x_1 \in H$ và $y^{-1}y_1 \in H$. Ta cần chứng minh: $x_1y_1H = xyH$, nghĩa là $(xy)^{-1}x_1y_1 \in H$

Thật vậy, $(xy)^{-1}x_1y_1 = y^{-1}x^{-1}x_1y_1 = \left[y^{-1}x^{-1}x_1y\right]\left[y^{-1}y_1\right]$. Phần tử sau cùng thuộc H do $x^{-1}x_1$ và $y^{-1}y_1$ đều thuộc H và $H \lhd G$.

ii) Do (i) phép toán nhân được định nghĩa như trong (ii) được hoàn toàn xác định. Tính kết hợp của phép toán nhân trên G/H được suy từ tính kết hợp của phép toán nhân trên G. Phần tử đơn vị trong G/H chính là lớp $eH = H$, trong đó e là phần tử đơn vị của G, còn phần tử nghịch đảo của lớp xH chính là $x^{-1}H$.

1.6.10. Nhận xét:

i) Nếu G là một nhóm giao hoán thì nhóm thương G/H cũng giao hoán. Chiều ngược lại không đúng.

ii) Với $H \le G$, nếu tập thương G/H là một nhóm với phép toán được định nghĩa như trên $\left((xH)(yH)=xyH\right)\left((xH)(yH)=xyH\right)$ thì $H \lhd G$.

1.6.11. Ví dụ:

Vì nhóm cộng các số nguyên $\mathbb{Z}$ giao hoán nên với mỗi n nguyên dương nhóm con $n\mathbb{Z}$ chuẩn tắc trong $\mathbb{Z}$. Ứng với nhóm con $H = n\mathbb{Z}$, quan hệ $\sim$ trong định lý 1.6.1 định bởi: $x \sim y \Leftrightarrow x - y \in n\mathbb{Z} \Leftrightarrow x - y$ chia hết cho n.

Như vậy $\sim$ chính là quan hệ đồng dư modulo n trên $\mathbb{Z}$ và nhóm thương $\mathbb{Z}/n\mathbb{Z}$ chính là nhóm cộng $\mathbb{Z}_n$ các số nguyên modulo n.

1.7. Đồng cấu

1.7.1. Định nghĩa: Một ánh xạ f từ nhóm G vào nhóm G' được gọi là một *đồng cấu (nhóm)* nếu f bảo toàn phép toán, nghĩa là với mọi $x,y \in G$, $f(xy) = f(x)f(y)$.

Một đồng cấu từ nhóm G vào G được gọi là một *tự đồng cấu* của G.

Một đồng cấu đồng thời là đơn ánh, toàn ánh hay song ánh được gọi lần lượt là *đơn cấu, toàn cấu* hay *đẳng cấu*. Một tự đồng cấu song ánh được gọi là một tự đẳng cấu. Nếu tồn tại một đẳng cấu từ nhóm G vào nhóm G' thì ta nói G đẳng cấu với G', ký hiệu $G \simeq G'$.

1.7.2. Ví dụ

Ví dụ 1: Ánh xạ đồng nhất id_G của nhóm G là một tự đẳng cấu, gọi là *tự đẳng cấu đồng nhất* của G.

Ví dụ 2: Giả sử H là một nhóm con của nhóm G. Khi đó ánh xạ bao hàm $i_H : H \to G$ $\left(i_H(x) = x\right)$ là một đơn cấu, gọi là *đơn cấu chính tắc*.

Ví dụ 3: Giả sử H là một nhóm con chuẩn tắc của nhóm G. Khi đó ánh xạ $\pi : G \to G/H$ định bởi $\pi(x) = xH$ là một toàn cấu, gọi là *toàn cấu chính tắc*.

Ví dụ 4: Giả sử G và G' là hai nhóm tùy ý. Khi đó ánh xạ $f : G \to G'$ định bởi $f(x) = e'$ (e' là phần tử trung hòa của G') là một đồng cấu, gọi là *đồng cấu tầm thường*.

Ví dụ 5: Ánh xạ $x \mapsto cos2\pi x + i\,sin2\pi x$ là một đồng cấu từ nhóm cộng các số thực $\mathbb{R}$ vào nhóm nhân các số phức khác không $\mathbb{C}^*$.

Ví dụ 6: Ánh xạ $x \mapsto e^x$ là một đẳng cấu từ nhóm cộng các số thực $\mathbb{R}$ lên nhóm nhân $\mathbb{R}^+$ các số thực dương.

Ví dụ 7: Ánh xạ $x \mapsto \ln x$ là một đẳng cấu từ nhóm nhân $\mathbb{R}^+$ các số thực dương lên nhóm cộng các số thực $\mathbb{R}$.

Ví dụ 8: Ánh xạ $det : GL(n,\mathbb{R}) \to \mathbb{R}^*$ là một toàn cấu.

Ví dụ 9: Cho $(G,.)$ là một nhóm và $a \in G$. Ánh xạ $\varphi_a : G \to G$ định bởi $\varphi_a(x) = axa^{-1}$ là một tự đẳng cấu của G.

Từ định nghĩa 1.7.1 ta suy ra các tính chất cơ bản của đồng cấu nhóm như sau:

1.7.3. Mệnh đề: Nếu $f : G \to G'$ là một đồng cấu nhóm thì $f(e) = e'$ và $f(x^{-1}) = (f(x))^{-1}$ với mọi $x \in G$ (e và e' lần lượt là các phần tử đơn vị của các nhóm G và G').

Chứng minh: Từ đẳng thức $ee = e$ ta có $f(e)f(e) = f(e)$ và tính giản ước của phép nhân trong nhóm G' cho ta $f(e) = e'$. Mặt khác, $\forall x \in G$, từ đẳng thức $x^{-1}x = e$ ta suy ra $f(x^{-1})f(x) = e'$ nên $f(x^{-1}) = (f(x))^{-1}$.

1.7.4. Mệnh đề: Tích của hai đồng cấu nhóm là một đồng cấu nhóm. Đặc biệt, tích của hai đơn cấu (tương ứng: toàn cấu, đẳng cấu) là một đơn cấu (tương ứng: toàn cấu, đẳng cấu).

Chứng minh: Giả sử $f : G \to G'$ và $g : G' \to G''$ là các đồng cấu nhóm. Xét ánh xạ tích $g \circ f$ ta có $\forall x,y \in G$, $(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y))$

$= g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$ nên $g \circ f$ vẫn còn là đồng cấu nhóm.

1.7.5. Mệnh đề: Ánh xạ ngược của một đẳng cấu nhóm là một đẳng cấu nhóm.

Chứng minh: Giả sử $f : G \to G'$ là một đẳng cấu nhóm. Vì $f^{-1} : G' \to G$ cũng là song ánh nên ta chỉ cần chứng minh f^{-1} là đồng cấu. Thật vậy, $\forall x',y' \in G'$ tồn tại $x,y \in G$ sao cho $x' = f(x)$ và $y' = f(y)$ nên

$f^{-1}(x'y') = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = (f^{-1} \circ f)(xy) = xy$

$= f^{-1}(x')f^{-1}(y')$. Vậy f^{-1} là đồng cấu và do đó là đẳng cấu.

1.7.6. Chú ý: Do các mệnh đề 1.7.4 và 1.7.5 ta thấy quan hệ đẳng cấu $\simeq$ giữa các nhóm là một quan hệ tương đương, nghĩa là có ba tính chất phản xạ, đối xứng và bắc cầu.

1.7.7. Định lý: Cho đồng cấu nhóm $f: G \to G'$ và H là một nhóm con của nhóm G, H' là một nhóm con của nhóm G'. Khi đó:

i) $f(H)$ là một nhóm con của nhóm G'.

ii) $f^{-1}(H')$ là một nhóm con của nhóm G. Hơn nữa, nếu H' là nhóm con chuẩn tắc của nhóm G' thì $f^{-1}(H')$ là nhóm con chuẩn tắc của nhóm G.

Đặc biệt, $Im\, f = f(G)$ là nhóm con của nhóm G' và $Kerf = f^{-1}(\varepsilon')$ là nhóm con chuẩn tắc của nhóm G.

Ta gọi Imf là ảnh của f và $Kerf$ là hạt nhân của f.

Chứng minh: i) Vì $e \in H$ nên $e' = f(e) \in f(H)$. Với mọi $x', y' \in f(H)$, $\exists\, x, y \in H$ sao cho $x' = f(x)$, $y' = f(y)$ nên $(x')^{-1} y' = f(x)^{-1} f(y)$

$= f(x^{-1}) f(y) = f(x^{-1}y) \in f(H)$ do $x^{-1}y \in H$. Theo định lý 1.4.2 thì $f(H) \le G'$.

ii) Vì $f(e) = e' \in H'$ nên $e \in f^{-1}(H')$. Với mọi $x, y \in f^{-1}(H')$ ta có $f(x) \in H'$ và $f(y) \in H'$ nên $f(x^{-1}y) = (f(x))^{-1} f(y) \in H'$, nghĩa là $x^{-1}y \in f^{-1}(H')$. Điều này chứng tỏ $f^{-1}(H') \le G$. Bây giờ giả sử $H' \lhd G'$. Khi đó $\forall x \in G$ và $h \in f^{-1}(H')$ ta có $f(h) \in H'$ nên $f(x^{-1}hx) = (f(x))^{-1} f(h) f(x) \in H'$ do H' chuẩn tắc. Từ đó $x^{-1}hx \in f^{-1}(H')$. Lý luận trên chứng tỏ $f^{-1}(H') \lhd G$.

Cuối cùng nhận xét rằng $G \le G$ và $\{e'\} \lhd G'$ nên theo kết quả trên ta có khẳng định sau cùng của định lý. ***(đpcm)***

Theo lý thuyết ánh xạ, hiển nhiên một đồng cấu nhóm $f: G \to G'$ là toàn cấu khi và chỉ khi $Im\, f = G'$. Định lý sau đây cho ta một dấu hiệu rất đơn giản để nhận biết một đồng cấu có là đơn cấu hay không.

1.7.8. Định lý: Đồng cấu nhóm $f : G \to G'$ là đơn cấu khi và chỉ khi $Kerf = \{e\}$.

Chứng minh: Chiều thuận là hiển nhiên vì $Kerf \leq G$ và $Kerf$ chứa không quá 1 phần tử do f là đơn ánh. Đảo lại, giả sử $Kerf = \{e\}$. Khi đó $\forall x, y \in G$ thỏa $f(x) = f(y)$ ta có $f(x^{-1}y) = (f(x))^{-1} f(y) = e'$ nên $x^{-1}y \in Kerf$, suy ra $x^{-1}y = e$, nghĩa là $x = y$. Vậy f đơn ánh. ***(đpcm)***

1.7.9. Định lý đẳng cấu 1: Cho đồng cấu nhóm $f : G \to G'$. Khi đó ánh xạ $\overline{f} : G / Kerf \to G'$ định bởi $\overline{f}(xKerf) = f(x)$ là một đơn cấu. Đặc biệt, $G / Kerf \simeq Im f$.

Chứng minh: Đặt $H = Kerf$. Vì $H \lhd G$ nên ta lập được nhóm thương G / H. Xét tương ứng $f : G / H \to G'$ định bởi $\overline{f}(xH) = f(x)$, ta có $\forall x, y \in G$:

$\overline{f}(xH) = \overline{f}(yH) \Leftrightarrow f(x) = f(y) \Leftrightarrow (f(x))^{-1} f(y) = e'$

$\Leftrightarrow f(x^{-1}) f(y) = e' \Leftrightarrow f(x^{-1}y) = e' \Leftrightarrow x^{-1}y \in H \Leftrightarrow xH = yH$.

Chiều $(\Leftarrow)$ chứng tỏ $\overline{f}$ là một ánh xạ, chiều $(\Rightarrow)$ chứng tỏ $\overline{f}$ là một đơn ánh. Bây giờ ta kiểm chứng $\overline{f}$ là một đồng cấu. Thật vậy, $\forall x, y \in G$:

$\overline{f}((xH)(yH)) = \overline{f}(xyH) = f(xy) = f(x) f(y) = \overline{f}(xH) \overline{f}(yH)$. Vậy $\overline{f}$ là đơn cấu. Khẳng định sau cùng trong định lý được suy từ lý thuyết về ánh xạ.

1.7.10. Định lý đẳng cấu 2: Cho G là một nhóm và H, K là hai nhóm con của nhóm G, hơn nữa H chuẩn tắc trong G. Khi đó $HK \leq G$, $H \lhd HK$, $H \cap K \lhd K$ và $K / H \cap K \simeq HK / H$ qua đẳng cấu $k(H \cap K) \mapsto kH$, trong đó $HK = \{hk \mid h \in H, k \in K\}$.

Chứng minh: **1/** $HK \leq G$: Hiển nhiên $e = ee \in HK$. Giả sử h_1k_1, h_2k_2 là 2 phần tử của HK. Khi đó $(h_1k_1)^{-1}(h_2k_2) = k_1^{-1}h_1^{-1}h_2k_2 = \left[k_1^{-1}(h_1^{-1}h_2)k_1\right]\left[k_1^{-1}k_2\right]$.

Chú ý rằng $h_1^{-1}h_2 \in H$ nên $k_1^{-1}(h_1^{-1}h_2)k_1 \in H$ do $H \lhd G$, hơn nữa $k_1^{-1}k_2 \in K$ do $K \leq G$. Do đó $(h_1k_1)^{-1}(h_2k_2) \in HK$. Suy ra $HK \leq G$.

2/ $H \lhd HK$: Vì $H \subset HK$ và $H \lhd G$ nên $H \lhd HK$.

3/ Xét ánh xạ $f : K \to HK / H$ định bởi $f(k) = kH$. Hiển nhiên f là một đồng cấu nhóm, hơn nữa f còn là toàn cấu vì $\forall hkH \in HK / H$ ta có $hkH = (hH)(kH) = H(kH) = kH = f(k)$.

Mặt khác, $Kerf = \{k \in K \mid f(k) = H\}$

$= \{k \in K \mid kH = H\} = \{k \in K \mid k \in H\} = H \cap K$. Do đó $H \cap K \lhd K$ và theo định lý 1.7.9 ta có đẳng cấu $K / H \cap K \simeq HK / H$, trong đó $k(H \cap K) \mapsto kH$. ***(đpcm)***

1.7.11. Định lý đẳng cấu 3: Cho G là một nhóm và H là một nhóm con chuẩn tắc của G. Ta có:

i) κ là một nhóm con của G / H khi và chỉ khi κ có dạng $\kappa = K / H$ với $K \le G$ và $H \le K$.

ii) κ là một nhóm con chuẩn tắc của G / H khi và chỉ khi κ có dạng $\kappa = K / H$ với $K \lhd G$ và $H \le K$. Hơn nữa, khi đó $(G / H) / (K / H) \simeq G / K$ qua đẳng cấu $xH(K / H) \mapsto xK$.

Chứng minh: Xét toàn cấu chính tắc $\pi : G \to G / H$. Với $\kappa \le G / H$, đặt $K = \pi^{-1}(\kappa)$ thì $H \le K \le G$ và $\pi(K) = \kappa$. Do đó khẳng định (i) được chứng minh.

Mặt khác, nếu $\kappa \lhd G / H$ thì $K \lhd G$ nên ta có khẳng định đầu trong (ii). Hơn nữa, khi đó xét tương ứng $f : G / H \to G / K$ định bởi $f(xH) = xK$ ta thấy ngay f là một ánh xạ vì nếu $xH = yH$ thì $x^{-1}y \in H$, từ đó $x^{-1}y \in K$, nghĩa là $xK = yK$. Hiển nhiên f là toàn ánh.

Ngoài ra do $f((xH)(yH)) = f(xyH) = xyK = (xK)(yK) = (xK)(yK) = f(xH) f(yH)$

Nên f là đồng cấu.

Cuối cùng ta có $Kerf = \{xH \in G / H \mid f(xH) = K\} = \{xH \in G / H \mid xK = K\}$

$= \{xH \in G / H \mid x \in K\} = K / H$ nên theo định lý 1.7.9 $(G / H) / (K / H) \simeq G / K$ trong đó $(xH)(KH) \mapsto xK$. ***(đpcm)***

1.7.12. Hệ quả: Mọi nhóm cyclic vô hạn đều đẳng cấu với nhóm cộng các số nguyên $\mathbb{Z}$. Mọi nhóm cyclic hữu hạn cấp n đều đẳng cấu với nhóm cộng $\mathbb{Z}_n$ các số nguyên *mod* n.

Chứng minh: Giả sử G là nhóm cyclic sinh bởi x. Xét ánh xạ $f:\mathbb{Z}\to G$ định bởi $f(m)=x^m$. Dễ thấy f là một đồng cấu từ nhóm cộng các số nguyên $\mathbb{Z}$ và G. Khi đó Kerf là một nhóm con của $\mathbb{Z}$ nên Kerf có dạng $Kerf=n\mathbb{Z}$ với $n\in\mathbb{N}$.

Nếu n = 0 thì $Kerf=\{0\}$ nên f là đơn cấu và do đó cũng là đẳng cấu. Trong trường hợp này G vô hạn và $G\simeq\mathbb{Z}$.

Nếu n > 0 thì theo định lý 1.7.9 $\mathbb{Z}/n\mathbb{Z}\simeq G$. Vì nhóm thương $\mathbb{Z}/n\mathbb{Z}$ chính là nhóm $\mathbb{Z}_n$ nên trong trường hợp này G hữu hạn cấp n và $G\simeq\mathbb{Z}_n$.

1.7.13. Ví dụ

Ví dụ 1: Đồng cấu $f:\mathbb{R}\to\mathbb{C}^*$ định bởi $f(x)=cos2\pi x+isin2\pi x$ có $Kerf=\mathbb{Z}$ và $Im\,f=U$ trong đó $U=\{z\in\mathbb{C}^*\,||z|=1\}$. Do đó theo định lý 1.7.9 $\mathbb{R}/\mathbb{Z}\simeq U$.

Ví dụ 2: Toàn cấu $f:GL(n,\mathbb{R})\to\mathbb{R}^*$ định bởi $f(A)=det(A)$ có $Kerf=\{A\in GL(n,\mathbb{R})\,|\,det(A)=1\}=SL(n,\mathbb{R})$ nên $GL(n,\mathbb{R})/SL(n,\mathbb{R})\simeq\mathbb{R}^*$.

BÀI TẬP CHƯƠNG 1

1. Lập các bảng toán cho các tập hợp gồm 2 phần tử, 3 phần tử để được những nhóm.

2. Cho X là một nửa nhóm khác rỗng. Với mỗi $a\in X$ ký hiệu

$aX=\{ax\,|\,x\in X\}$ và $Xa=\{xa\,|\,x\in X\}$

Chứng minh X là một nhóm khi và chỉ khi với mọi $a\in X$ ta có $aX=Xa=X$.

3. Cho X là một nhóm với đơn vị e. Chứng minh rằng nếu với mọi $a\in X$, $a^2=e$ thì X là Abel.

4. Cho một họ khác rỗng những nhóm $(X_i)_{i\in I}$ mà các phép toán ký hiệu bằng dấu nhân. Chứng minh rằng tập hợp tích Đêcác $\prod_{i\in I}X_i$ với phép toán xác định như sau:

$(x_i)_{i\in I}.(y_i)_{i\in I}=(x_iy_i)_{i\in I}$ là một nhóm (gọi là tích của các nhóm X_i).

5. Chứng minh rằng mọi nửa nhóm khác rỗng hữu hạn X là một nhóm nếu và chỉ nếu luật giản ước thực hiện được đối với mọi phần tử của X.

6. Cho A và B là hai bộ phận của một nhóm X. Ta định nghĩa:

$$AB = \{ab \mid a \in A, b \in B\}$$

$A^{-1} = \{a^{-1} \mid a \in A\}$. Chứng minh các đẳng thức sau đây:

a. $(AB)C = A(BC)$;

b. $\left(A^{-1}\right)^{-1} = A$;

c. $(AB)^{-1} = B^{-1}A^{-1}$;

d. Nếu A là một nhóm con của nhóm X thì $A^{-1} = A$.

7. Cho A là một bộ phận khác rỗng của một nhóm X. Chứng minh A là nhóm con của X khi và chỉ khi $AA^{-1} = A$.

8. Cho A là một nhóm con của một nhóm X, $a \in X$. Chứng minh rằng aA là một nhóm con của X khi và chỉ khi $a \in A$.

9. Trong một nhóm X chứng minh rằng nhóm con sinh ra bởi tập ϕ là nhóm con $\{e\}$, e là đơn vị của X.

10. Cho X là một nhóm với phần tử đơn vị e, một phần tử $a \in X$ có cấp là n. Chứng minh rằng $a^k = e$ khi và chỉ khi k chia hết cho n.

11. Cho a, b là hai phần tử tùy ý của một nhóm. Chứng minh ab và ba có cùng cấp.

12. Giả sử X là một nhóm, ta gọi bộ phận $C(X) = \{a \in X \mid ax = xa, \forall x \in X\}$ là tâm của X. Chứng minh rằng C(X) là một nhóm con giao hoán và mọi nhóm con của C(X) là một nhóm con chuẩn tắc của X.

13. Giả sử X là một nhóm, x và y là hai phần tử của X. Ta gọi là hoán tử của x và y phần tử $xyx^{-1}y^{-1}$. Chứng minh rằng nhóm con A sinh bởi tập hợp các hoán tử của tất cả các phần tử x, y của X là một nhóm con chuẩn tắc của X và nhóm thương X/A là Abel. Nhóm con A được gọi là *nhóm con hoán tử* của X và ký hiệu $[x;x]$.

14. Chứng minh rằng muốn cho nhóm thương X/H của một nhóm X là Abel cần và đủ là nhóm con chuẩn tắc H chứa nhóm con các hoán tử của X.

15. Chứng minh rằng mọi nhóm cấp bé hơn hay bằng 5 đều là Abel.

16. Hãy tìm các nhóm thương của:

a. Nhóm cộng các số nguyên là bội của 3 trên nhóm cộng các số nguyên là bội của 15.

b. Nhóm cộng các số nguyên là bội của 4 trên nhóm cộng các số nguyên là bội của 24.

17. Cho X là một nhóm giao hoán, chứng minh rằng ánh xạ: $\varphi : X \to X$ xác định bởi $a \mapsto a^k$ (với k là một số nguyên cho trước) là một đồng cấu. Xác định $Ker\varphi$.

18. Cho X là một nhóm. Ánh xạ: $\varphi : X \to X$ xác định bởi $a \mapsto a^{-1}$ là một tự đẳng cấu của nhóm X khi và chỉ khi X là một nhóm Abel.

19. Chứng minh rằng mọi nhóm thương của một nhóm cyclic là một nhóm cyclic, ảnh đồng cấu của một nhóm cyclic là một nhóm cyclic.

Chương 2: VÀNH VÀ TRƯỜNG

2.1. Khái niệm về vành

2.1.1. Định nghĩa: *Vành* là một tập hợp R cùng với 2 phép toán cộng và nhân thỏa các 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:

$$x(y+z) = xy + xz$$
$$(y+z)x = yx + zx$$

Phần tử trung hòa của phép cộng được gọi là *phần tử không*, ký hiệu là 0; phần tử đối xứng của phần tử $x \in R$ là *phần tử đối* của x, ký hiệu là $-x$. Nếu phép nhân giao hoán thì ta nói vành R *giao hoán*; nếu phép nhân có phần tử đơn vị thì vành R được gọi là *vành có đơn vị*. Phần tử đơn vị được ký hiệu là e hay 1.

2.1.2. Nhận xét: Cho R là vành có đơn vị e. Phần tử $x \in R$ được gọi là khả nghịch nếu x khả đối xứng với phép nhân, nghĩa là tồn tại $y \in R$ sao cho $xy = yx = e$. Ký hiệu: $R^* = \{ x \in R \mid x$ khả nghịch$\}$. Khi đó R^* là một nhóm đối với phép nhân, gọi là *nhóm các phần tử khả nghịch* của R.

2.1.3. Ví dụ

Ví dụ 1: Tập hợp các số nguyên $\mathbb{Z}$ với phép cộng và phép nhân thông thường là vành giao hoán, có đơn vị, gọi là *vành các số nguyên*. Tương tự ta cũng có vành các số hữu tỷ $\mathbb{Q}$, vành các số thực $\mathbb{R}$, vành các số phức $\mathbb{C}$.

Ví dụ 2: Trên nhóm cộng $\mathbb{Z}_n$ các số nguyên modulo n, ta định nghĩa phép toán nhân như sau: với mọi $\bar{x},\bar{y} \in \mathbb{Z}_n$, $\bar{x}\bar{y} = \overline{xy}$. Khi đó $\mathbb{Z}_n$ trở thành vành giao hoán có đơn vị $\bar{1}$.

Ví dụ 3: Tập $M(n,\mathbb{R})$ các ma trận vuông cấp n với hệ số thực cùng với phép cộng và nhân ma trận thông thường là vành có đơn vị. Vành này không giao hoán nếu $n \geq 2$.

Ví dụ 4: Cho (G, +) là một nhóm Abel. Tập hợp $End(G)$ các tự đồng cấu của nhóm G là vành có đơn vị với phép cộng định bởi:

$$(f+g)(x)=f(x)+g(x),\forall f,g\in End(G),\forall x\in G,$$

và phép nhân là phép hợp nối ánh xạ. Vành này không giao hoán nếu $|G|\geq 2$.

Ví dụ 5: Giả sử $R_1,R_2,...,R_n$ là các vành. Khi đó tích Descartes

$\prod_{i=1}^{n}R_i=\{(x_1,x_2,...,x_n)\,|\,x_1\in R_1,x_2\in R_2,...,x_n\in R_n\}$ cùng với phép cộng $(x_i)+(y_i)=(x_i+y_i)$ và phép nhân $(x_i)(y_i)=(x_iy_i)$, là một vành, gọi là *vành tích trực tiếp* của $R_1,R_2,...,R_n$. Hiển nhiên nếu mọi vành R_i đều giao hoán (tương ứng, có đơn vị) thì vành tích trực tiếp cũng giao hoán (tương ứng, có đơn vị).

Từ định nghĩa 2.1.1 ta có mệnh đề sau:

2.1.4. Mệnh đề: Cho R là một vành. Khi đó với mọi $x,y,z\in R$ và $n\in\mathbb{Z}$, ta có: **i)** $x(y-z)=xy-xz$ và $(y-z)x=yx-zx$.

ii) $0x=x0=0$.

iii) $x(-y)=(-x)y=-(xy)$ và $(-x)(-y)=xy$.

iv) $(nx)y=x(ny)=n(xy)$. Đặc biệt, nếu R có đơn vị e thì $nx=(ne)x=x(ne)$.

Chứng minh: **i)** Do tính phân phối của phép nhân đối với phép cộng ta có: $xy=x[(y-z)+z]=x(y-z)+xz\Rightarrow x(y-z)=xy-xz$. Đẳng thức còn lại được chứng minh tương tự.

(ii) Do (i) ta có $0x=(y-y)x=yx-yx=0$. Tương tự $x0=0$.

(iii) Từ (i) và (ii) ta có $x(-y)=x(0-y)=x0-xy=-xy$. Tương tự $(-x)y=-(xy)$. Hơn nữa, $(-x)(-y)=-(-xy)=xy$.

(iv) Ta chứng minh $(nx)y=n(xy)$. Với n = 0 đẳng thức hiển nhiên đúng.

Xét n > 0 ta có $(nx)y=(x+x+...+x)y=xy+xy+...+xy=n(xy)$.

Với n < 0, đặt $m=-n>0$ ta có:

$(nx)y=[m(-x)]y=m[(-x)y]=m(-xy)=(-m)(xy)=n(xy)$.

Vậy: $(nx)y=n(xy)\ \ \forall n\in\mathbb{Z}$. Tương tự: $x(ny)=n(xy)$.

Nếu R có đơn vị thì $nx = n(ex) = (ne)x$. Tương tự: $nx = x(ne)$. ***(đpcm)***

2.2. Vành con, Ideal và vành thương

2.2.1. Định nghĩa: Cho R là một vành.

(i) Tập con A khác rỗng của R được gọi là một *vành con* của R nếu A ổn định đối với hai phép toán trong vành R và A cùng với hai phép toán cảm sinh là một vành.

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

2.2.2. Định lý (Đặc trưng của vành con): Cho A là một tập con khác rỗng của vành R. Các mệnh đề sau tương đương:

i) A là một vành con của vành R;

ii) Với mọi $x, y \in A, x + y \in A, xy \in A, -x \in A$;

iii) Với mọi $x, y \in A, x - y \in A, xy \in A$.

Chứng minh: $(i) \Rightarrow (ii)$: Vì A là một vành con của R nên A ổn định đối với phép cộng và phép nhân, nghĩa là $x + y \in A$ và $xy \in A$. Mặt khác, do

(A, +) là một nhóm con của (R, +) nên $-x \in A$.

$(ii) \Rightarrow (iii)$: $\forall x, y \in A$ ta có $\forall x, (-y) \in A$ nên $x - y = x + (-y) \in A$.

$(iii) \Rightarrow (i)$: Từ giả thiết (iii) ta có (A, +) là nhóm con của (R, +). Mặt khác, các phép toán cảm sinh cũng có tính chất kết hợp và phân phối nên A là một vành, nghĩa là A là một vành con của R. ***(đpcm)***

2.2.3. Định lý (Đặc trưng của Ideal): Cho I là một tập con khác rỗng của vành R. Các mệnh đề sau tương đương:

i) I là một Ideal của R;

ii) Với mọi $x, y \in I$ và $r \in R, x + y \in I, -x \in I, rx \in I$ và $xr \in I$;

iii) Với mọi $x, y \in I$ và $r \in R, x - y \in I, xr \in I$ và $rx \in I$.

Chứng minh: Dựa vào định lý 2.2.2 và định nghĩa 2.2.1 suy ra đpcm.

2.2.4. Nhận xét:

i) Các tập con $\{0\}$ và R đều là các ideal của R, gọi là các *Ideal tầm thường*.

ii) Nếu vành R giao hoán thì các khái niệm Ideal trái, Ideal phải và Ideal là trùng nhau.

iii) Giả sử R là vành có đơn vị và I là một Ideal trái hay phải của R. Khi đó $I = R \Leftrightarrow I$ chứa ít nhất một phần tử khả nghịch $\Leftrightarrow I$ chứa phần tử đơn vị.

iv) Với I, J là hai Ideal của R, đặt $I + J = \{x + y \mid x \in I, y \in J\}$; $IJ = \left\{ \sum_{i=1}^{n} x_i y_i \mid x_i \in I, y_i \in J, n \in \mathbb{N}^* \right\}$. Khi đó $I + J$ và IJ cũng là các Ideal của R, gọi là *tổng* và *tích* của các Ideal I và J.

2.2.5. Ví dụ

Ví dụ 1: I là Ideal của $\mathbb{Z}$ khi và chỉ khi I có dạng $n\mathbb{Z}$ với $n \in \mathbb{Z}$.

Ví dụ 2: $M(n,\mathbb{Z})$ là vành con của $M(n,\mathbb{Q})$ nhưng không là Ideal.

Ví dụ 3: $M(n,2\mathbb{Z})$ là Ideal của $M(n,\mathbb{Z})$.

Từ định nghĩa 2.2.1 ta thấy giao của một họ khác ϕ các vành con (tương ứng Ideal) của một vành R cũng là một vành con (tương ứng Ideal) của vành R.

Giả sử S là một tập con của vành R. Khi đó S chứa trong ít nhất một vành con (tương ứng Ideal) của R, chẳng hạn $S \subset R$. Giao của tất cả các vành con (tương ứng Ideal) của R có chứa S là một vành con (tương ứng Ideal) của R có chứa S. Ta có định nghĩa sau:

2.2.6. Định nghĩa: Cho S là một tập con khác rỗng của vành R. Ta định nghĩa: **(i)** Giao của tất cả các vành con của R có chứa S là vành con *sinh bởi S*.

(ii) Giao của tất cả các Ideal của R có chứa S là *Ideal sinh bởi S*, ký hiệu là $\langle S \rangle$.

Từ định nghĩa ta thấy vành con (tương ứng Ideal) của R sinh bởi tập hợp S chính là vành con (tương ứng Ideal) nhỏ nhất của R có chứa S. Đặc biệt $\{0\}$ là vành con và cũng là Ideal sinh bởi tập rỗng. Mệnh đề sau đây mô tả vành con và Ideal sinh bởi các tập hợp khác rỗng.

2.2.7. Mệnh đề: Cho S là một tập con khác rỗng của vành R. Khi đó:

i) Vành con của R sinh bởi S là tập hợp $\left\{ \sum_{huu\ han} s_1 s_2 ... s_n \mid s_i \in S \ \ hay \ -s_i \in S, n \in \mathbb{N}^* \right\}$.

ii) Nếu R có đơn vị thì Ideal sinh bởi S là tập hợp $\langle S\rangle = \left\{ \sum_{i=1}^{n} x_i s_i y_i \mid x_i, y_i \in R, s_i \in S, n \in \mathbb{N}^* \right\}$.

iii) Nếu R giao hoán có đơn vị thì $\langle S\rangle = \left\{ \sum_{i=1}^{n} x_i s_i \mid x_i \in R, s_i \in S, n \in \mathbb{N}^* \right\}$.

2.2.8. Định nghĩa: Cho S là một tập con của vành R và $I = \langle S\rangle$. Ta nói *I được sinh ra bởi S* và S là *tập sinh* của I. Nếu S hữu hạn thì ta nói I *hữu hạn sinh*. Đặc biệt, nếu $S = \{a\}$ thì ta viết $I = \langle a\rangle$, gọi là *Ideal chính sinh bởi a*.

2.2.9. Nhận xét:

Nếu vành R giao hoán, có đơn vị thì Ideal chính sinh bởi a là: $\langle a\rangle = \{xa \mid x \in R\}$. Ta còn ký hiệu tập hợp trên là *Ra*.

Xét vành (R, +, .) và I là một Ideal tùy ý của R. Vì phép cộng giao hoán nên nhóm con (I, +) chuẩn tắc trong (R, +) và ta có thể lập được nhóm thương (R/I, +). Định lý sau đây cho thấy ta có thể trang bị cho (R, +) một phép toán nhân để nó trở thành một vành.

2.2.10. Định lý: Giả sử I là một ideal của vành (R, +, .). Trên nhóm thương (R/I, +) ta định nghĩa phép toán nhân như sau: $(x+I)(y+I) = xy + I$. Khi đó (R/I, +, .) là một vành, gọi là *vành thương* của R trên Ideal I.

Chứng minh: Trước hết ta chứng minh phép toán nhân được xác định. Thật vậy, giả sử $x + I = x' + I$ và $y + I = y' + I$, nghĩa là $x - x' \in I$ và $y - y' \in I$ hay $x = x' + a$ và $y = y' + b$ với $a, b \in I$ nào đó. Khi đó $xy = (x' + a)(y' + b) = x'y' + x'b + ay' + ab$. Chú ý rằng $x'b, ay'$ và ab đều thuộc I vì I là Ideal của vành R. Do đó $xy - x'y' \in I$ hay $xy + I = x'y' + I$. Như vậy phép nhân trên R/I được xác định.

Do phép nhân trên R có tính kết hợp và phân phối đối với phép cộng nên dễ thấy phép nhân trên R/I được định nghĩa như trên cũng có tính chất kết hợp và phân phối đối với phép cộng. Điều này chứng tỏ (R/I, +, .) là một vành.

2.2.11. Nhận xét:

i) Nếu vành R giao hoán thì vành thương R/I cũng giao hoán. Chiều ngược lại không đúng.

ii) Nếu vành R có đơn vị e thì vành thương R/I có đơn vị là $e+I$. Chiều ngược lại không đúng.

2.2.12. Ví dụ: Vành thương của vành các số nguyên $\mathbb{Z}$ trên Ideal $n\mathbb{Z}$ chính là vành $\mathbb{Z}_n$ các số nguyên modulo n, trong đó ngoài phép cộng đã biết, ta có phép toán nhân định bởi $(x+n\mathbb{Z})(y+n\mathbb{Z})=xy+n\mathbb{Z}$.

2.3. Đồng cấu

2.3.1. Định nghĩa: Một ánh xạ f từ vành R vào vành R' được gọi là một *đồng cấu vành* nếu f bảo toàn các phép toán, nghĩa là với mọi $x,y\in R$, $f(x+y)=f(x)+f(y)$, $f(xy)=f(x)f(y)$.

Một đồng cấu từ R vào R được gọi là một *tự đồng cấu* của R. Một đồng cấu đồng thời là đơn ánh, toàn ánh, song ánh được gọi lần lượt là *đơn cấu, toàn cấu, đẳng cấu*. Một tự đồng cấu song ánh được gọi là một *tự đẳng cấu*. Nếu tồn tại một đẳng cấu từ R vào R' thì ta nói R đẳng cấu với R', ký hiệu là $R\simeq R'$.

2.3.2. Ví dụ

Ví dụ 1: Ánh xạ đồng nhất $id_{\mathbb{R}}$ của vành R là một tự đẳng cấu, gọi là tự đẳng cấu đồng nhất của R.

Ví dụ 2: Giả sử A là một vành con của vành R. Khi đó ánh xạ bao hàm $i_A : A\to R$ định bởi $i_A(x)=x$ là một đơn cấu, gọi là *đơn cấu chính tắc*.

Ví dụ 3: Giả sử I là một Ideal của vành R. Khi đó ánh xạ $\pi : R\to R/I$ định bởi $\pi(x)=x+I$ là một toàn cấu, gọi là *toàn cấu chính tắc*.

Ví dụ 4: Giả sử R,R' là hai vành. Khi đó ánh xạ $f : R\to R'$ định bởi $f(x)=0_{R'}$ ($0_{R'}$ là phần tử không của vành R') là một đồng cấu, gọi là *đồng cấu tầm thường*.

Ví dụ 5: Cho R là một vành có đơn vị và $a\in R$ khả nghịch. Khi đó ánh xạ $f : R\to R$ định bởi $f(x)=axa^{-1}$ là một tự đẳng cấu của R.

Thật vậy, dễ thấy f là một song ánh, hơn nữa f là đồng cấu vì

$$f(x+y)=a(x+y)a^{-1}=axa^{-1}+aya^{-1}=f(x)+f(y)$$

$$f(xy)=a(xy)a^{-1}=\left(axa^{-1}\right)\left(aya^{-1}\right)=f(x)f(y)$$

Vậy f là đẳng cấu.

Ví dụ 6: Xét ánh xạ $f:\mathbb{Z}_6\to\mathbb{Z}_6$ định bởi $f(\bar{x})=4\bar{x}$. Khi đó f là đồng cấu vành vì

$$f(\bar{x}+\bar{y})=f(\overline{x+y})=4(\overline{x+y})=4\bar{x}+4\bar{y}=f(\bar{x})+f(\bar{y})$$

$$f(\bar{x}\,\bar{y})=f(\overline{xy})=4\overline{xy}=4\bar{x}\,\bar{y}+12\bar{x}\,\bar{y}=16\bar{x}\,\bar{y}=(4\bar{x})(4\bar{y})=f(\bar{x})f(\bar{y}).$$

Từ định nghĩa 2.3.1 lý luận tương tự như đối với đồng cấu nhóm ta thấy đồng cấu vành có các tính chất sau:

2.3.3. Mệnh đề: Nếu $f:R\to R'$ là một đồng cấu vành thì $f(0_R)=0_{R'}$ và $f(-x)=-f(x)$ với mọi $x\in R$.

2.3.4. Mệnh đề: Tích của hai đồng cấu vành là một 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.

2.3.5. Mệnh đề: Ánh xạ ngược của một đẳng cấu vành cũng là đẳng cấu vành.

2.3.6. Chú ý: Do các mệnh đề 2.3.4 và 2.3.5 ta thấy quan hệ đẳng cấu $\simeq$ giữa các vành là một quan hệ tương đương, nghĩa là thỏa 3 tính chất: phản xạ, đối xứng và bắc cầu.

2.3.7. Định lý: Cho đồng cấu vành $f:R\to R'$ và A là một vành con của vành R, A' là một vành con của vành R'. Khi đó:

i) $f(A)$ là một vành con của vành R'.

ii) $f^{-1}(A')$ là một vành con của vành R. Hơn nữa, nếu A' là một Ideal của R' thì $f^{-1}(A')$ cũng là Ideal của R.

Đặc biệt, $Im\,f=f(R)$ là vành con của R' và $Kerf=f^{-1}(0_{R'})$ là Ideal của R. Ta gọi $Im\,f$ là ảnh của f và Kerf là hạt nhân của f.

Chứng minh: **(i)** Vì $(A,+)\le(R,+)$ nên $f(A)$ là nhóm con của nhóm cộng R'. Mặt khác, $\forall x',y'\in f(A)$, $\exists x,y\in A$ sao cho $f(x)=x'$, $f(y)=y'$ nên $x'y'=f(x)f(y)=f(xy)\in f(A)$. Điều này chứng tỏ $f(A)$ là vành con của R'.

(ii) Vì $(A',+)\le(R',+)$ nên $f^{-1}(A')$ là nhóm con của nhóm cộng R. Mặt khác, $\forall x,y\in f^{-1}(A')$, $f(x), f(y)\in A'$ nên $f(xy)=f(x)f(y)\in A'$, nghĩa là $xy\in f^{-1}(A')$. Điều này chứng tỏ $f^{-1}(A')$ là vành con của R. Giả sử A' là một Ideal của R'. Khi đó theo chứng minh trên $f^{-1}(A')$ là vành con của R; Hơn nữa $\forall r\in R$ và $x\in f^{-1}(A')$ ta có $f(rx)=f(r)f(x)\in A'$ (do $f(x)\in A'$ và A' là Ideal của R'), nghĩa là $rx\in f^{-1}(A')$; tương tự $xr\in f^{-1}(A')$. Điều này chứng tỏ $f^{-1}(A')$ là Ideal của R.

Cuối cùng nhận xét rằng R là vành con của R và $\{0_{R'}\}$ là Ideal của R' nên theo kết quả trên ta có khẳng định sau cùng trong định lý. ***(đpcm)***

Lưu ý: Theo lý thuyết ánh xạ, hiển nhiên một đồng cấu vành $f: R\to R'$ là toàn cấu khi và chỉ khi $Im\, f = R'$. Mặt khác, do mọi đồng cấu vành đều thỏa tính chất của đồng cấu nhóm cộng, ta có định lý sau:

2.3.8. Định lý: Đồng cấu vành $f: R\to R'$ là đơn cấu khi và chỉ khi $Kerf=\{0_R\}$.

Tương tự như trong lý thuyết nhóm ta cũng có các định lý đẳng cấu vành như sau:

2.3.9. Định lý đẳng cấu 1: Cho đồng cấu vành $f: R\to R'$. Khi đó ánh xạ $\overline{f}: R/Kerf\to R'$ định bởi $\overline{f}(x+Kerf)=f(x)$ là đơn cấu vành. Đặc biệt $R/Kerf\simeq Im\, f$.

Chứng minh: Theo định lý 2.3.7 Kerf là Ideal của R nên ta lập được vành thương $R/Kerf$ và theo định lý về nhóm của chương 1 ta có $\overline{f}$ là đơn cấu nhóm cộng. Ta chỉ cần kiểm chứng $\overline{f}$ bảo toàn phép nhân. Thật vậy, đặt $I=Kerf$, khi đó $\forall x,y\in R$, ta có

$\overline{f}\big((x+I)(y+I)\big)=\overline{f}(xy+I)=f(xy)$

$=f(x)f(y)=\overline{f}(x+I)\overline{f}(y+I)$. Điều này chứng tỏ $\overline{f}$ là đơn cấu vành.

2.3.10. Định lý đẳng cấu 2: Cho *R* là một vành và I là một Ideal, A là một vành con của *R*. Khi đó I + A là vành con của *R*; I là Ideal của I + A; $I \cap A$ là Ideal của A và $A / I \cap A \simeq (I + A) / I$ qua đẳng cấu vành $x + I \cap A \mapsto x + I$.

Chứng minh: Đối với phép cộng, I và A đều là các nhóm con của nhóm R. Mặt khác, $\forall x,x' \in I$ và $a,a' \in A$ ta có:

$(x + a)(x' + a') = (xx' + xa' + ax') + aa' \in I + A$ nên $I + A$ là vành con của *R*. Khẳng định I là Ideal của $I + A$ và $I \cap A$ là Ideal của A được suy ra từ giả thiết I là một Ideal của R. Ta đã biết ánh xạ $f : A / I \cap A \to (I + A) / I$ định bởi $f(x + I \cap A) = x + I$ là đẳng cấu nhóm cộng. Mặt khác, f cũng bảo toàn phép toán nhân vì $\forall x,y \in A$ ta có:

$f((x + I \cap A)(y + I \cap A))$

$= f(xy + I \cap A) = xy + I = (x + I)(y + I) = f(x + I \cap A) f(y + I \cap A)$. Điều này chứng tỏ f là đẳng cấu vành.

2.3.11. Định lý đẳng cấu 3: Cho *R* là một vành và *I* là một Ideal của *R*. Khi đó: **i)** Λ là một vành con của vành thương *R/I* khi và chỉ khi Λ có dạng *A/I* với *A* là một vành con của *R* và *A* chứa *I*.

ii) Λ là một Ideal của vành thương *R/I* khi và chỉ khi Λ có dạng *A/I* với *A* là một Ideal của *R* và *A* chứa *I*. Hơn nữa, ta có: $(R / I) / (A / I) \simeq R / A$ qua đẳng cấu $(x + I) + (A / I) \mapsto x + A$.

Chứng minh: Vì mọi vành con của vành R đều là nhóm con của nhóm cộng R nên theo định lý của chương 1, mọi vành con của Λ của R/I đều có dạng A/I với A là nhóm con của nhóm cộng R và A chứa I. Mặt khác, dễ kiểm chứng rằng Λ là vành (tương ứng Ideal) của R/I khi và chỉ khi Λ là vành con (tương ứng Ideal) của R. Như vậy, khi $\Lambda = A / I$ là Ideal của vành thương R/I, ta lập được các vành thương (R/I)/(A/I) và R/A. Theo định lý của chương 1, ánh xạ (R/I)/(A/I) vào R/A được xác định bởi $(x + I) + (A / I) \mapsto x + A$ là đẳng cấu nhóm cộng. Mặt khác, lý luận tương tự như trong các chứng minh 2.3.9 và 2.3.10 ta thấy ánh xạ trên cũng bảo toàn phép nhân và do đó cũng là đẳng cấu vành. ***(đpcm)***

2.3.12. Ví dụ: Xét đồng cấu vành $f:\mathbb{Z}_6\to\mathbb{Z}_6$ định bởi $f\left(\bar{x}\right)=4\bar{x}$ (xem ví dụ 6), ta có:

$Im\ f=4\mathbb{Z}_6=2\mathbb{Z}_6=\left\{2\bar{x}\,|\,\bar{x}\in\mathbb{Z}_6\right\}$;

$Kerf=\left\{\bar{x}\in\mathbb{Z}_6\,|\,4\bar{x}=\bar{0}\right\}=\left\{\bar{x}\in\mathbb{Z}_6\,|\,4x\equiv 0\ (mod\ 6)\right\}=\left\{\bar{x}\in\mathbb{Z}_6\,|\,x\equiv 0\ (mod\ 3)\right\}=3\mathbb{Z}_6$

Theo định lý đẳng cấu 2.3.9 ta có $\mathbb{Z}_6/3\mathbb{Z}_6\simeq 2\mathbb{Z}_6$.

2.3.13. Bổ đề: Cho *R* là một vành giao hoán có đơn vị và *I, J* là hai Ideal của *R* sao cho $I+J=R$. Khi đó $I\cap J=IJ$ và $R/I\cap J\simeq\left(R/I\right)\times\left(R/J\right)$ qua đẳng cấu $x+I\cap J\mapsto\left(x+I,x+J\right)$.

Bổ đề 2.3.13 được mở rộng thành định lý sau:

2.3.14. Định lý Dư số Trung Hoa: Cho *R* là một vành giao hoán có đơn vị và $I_1,I_2,...,I_n$ là các Ideal của *R* sao cho $I_i+I_j=R$ với mọi $i\neq j$. Khi đó: $R/I_1I_2...I_n\simeq\prod_{i=1}^{n}\left(R/I_i\right)$ qua đẳng cấu $x+I_1I_2...I_n\mapsto\left(x+I_i\right)$.

2.4. Miền nguyên và trường

2.4.1. Định nghĩa:

(i) Cho *R* là một vành giao hoán. Phần tử $x\in R\setminus\{0\}$ được gọi là *ước* của 0 nếu tồn tại $y\in R\setminus\{0\}$ sao cho $xy=0$.

(ii) Một vành giao hoán, có đơn vị, có nhiều hơn một phần tử và không có ước của 0 được gọi là *miền nguyên*.

(iii) Một vành giao hoán, có đơn vị, có nhiều hơn một phần tử trong đó mọi phần tử khác 0 đều khả nghịch được gọi là một *trường*.

2.4.2. Nhận xét:

i) Trong miền nguyên *R*, phép nhân có tính giản ước cho các phần tử khác 0 nghĩa là nếu $xy=xz$ và $x\neq 0$ thì $y=z$.

ii) Mọi trường *R* chỉ có hai Ideal là $\{0\}$ và *R*.

iii) (R, +, .) là một trường khi và chỉ khi các tính chất sau đây được thỏa:

- (R, +) là nhóm Abel;

- $R\setminus\{0\}$ là nhóm Abel;

- Phép nhân phân phối với phép cộng.

2.4.3. Ví dụ

Ví dụ 1: Tập các số nguyên $\mathbb{Z}$ với phép cộng và nhân thông thường là miền nguyên nhưng không là trường.

Ví dụ 2: Tập hợp các số hữu tỷ $\mathbb{Q}$ với phép cộng và nhân thông thường là trường. Ta gọi đó là *trường các số hữu tỷ* $\mathbb{Q}$. Tương tự, ta có *trường các số thực* $\mathbb{R}$ và *trường các số phức* $\mathbb{C}$.

Ví dụ 3: Vành $\mathbb{Z}_n$ các số nguyên modulo n là trường khi và chỉ khi n = p nguyên tố.

2.4.4. Định lý:

i) Mọi trường đều là miền nguyên.

ii) Mọi miền nguyên hữu hạn đều là trường.

Chứng minh: **(i)** Ta chỉ cần chứng minh mọi trường R đều không có ước của 0. Thật vậy, giả sử $xy=0$ và $x\neq 0$. Khi đó x khả nghịch nên tồn tại $x^{-1}\in R$ sao cho $x^{-1}x=e$. Do đó $y=ey=x^{-1}xy=x^{-1}0=0$. Điều này chứng tỏ R không có ước của 0 và do đó R là miền nguyên.

(ii) Giả sử R là một miền nguyên hữu hạn. Cho $a\in R\setminus\{0\}$ bất kỳ. Ta chứng minh a khả nghịch. Thật vậy, xét ánh xạ $f: R\setminus\{0\}\to R\setminus\{0\}$ định bởi $x\mapsto ax$. Vì trong miền nguyên R phép nhân có tính giản ước nên ta thấy ngay f là đơn ánh. Theo giả thiết $R\setminus\{0\}$ hữu hạn nên f phải là song ánh. Suy ra $\exists\, b\in R\setminus\{0\}$ sao cho $f(b)=e$, nghĩa là $ab=e$. Điều này chứng tỏ a khả nghịch, và do đó R là trường. ***(đpcm)***

2.4.5. Nhận xét: Giả thiết hữu hạn trong (ii) của định lý 2.4.4 không thể bỏ được. Chẳng hạn $\mathbb{Z}$ là miền nguyên vô hạn nhưng không phải là trường.

2.4.6. Định nghĩa: Cho *R* là một trường và *I* là một tập con khác rỗng của *R* ổn định đối với hai phép toán trong *R*. Ta nói *I* là một *trường con* của *R* nếu *I* với hai phép toán cảm sinh từ *R* cũng là một trường.

2.4.7. Ví dụ: Trường các số hữu tỷ $\mathbb{Q}$ là trường con của trường các số thực $\mathbb{R}$. Tương tự $\mathbb{R}$ là trường con của $\mathbb{C}$.

Từ định nghĩa 2.4.6 ta suy ra ngay các tính chất đặc trưng của các trường con như sau:

2.4.8. Định lý (Đặc trưng của trường con): Cho *R* là một trường và *I* là tập con của *R* có chứa ít nhất hai phần tử. Các mệnh đề sau tương đương:

i) *I* là một trường con của *R*;

ii) Với mọi $x,y \in I$, $x+y \in I$, $xy \in I$, $-x \in I$ và hơn nữa, nếu $x \neq 0$ thì $x^{-1} \in I$;

iii) Với mọi $x,y \in I$, $x-y \in I$ và hơn nữa, nếu $x \neq 0$ thì $x^{-1}y \in I$.

Xét *R* là một trường với phần tử đơn vị e. Trong nhóm cộng *R*, phần tử đơn vị e hoặc có cấp hữu hạn hoặc có cấp vô hạn. Giả sử e có cấp hữu hạn là n. Khi đó n phải là số nguyên tố, vì nếu không thì có $1<m,k<n$ sao cho $n=mk$ dẫn đến $0=ne=(mk)e=(me)(ke)$, suy ra $me=0$ hoặc $ke=0$, mâu thuẫn với tính chất của cấp n. Vậy nếu e có cấp hữu hạn thì cấp đó phải là số nguyên tố. Trường hợp e có cấp vô hạn, ta nói *R* là *trường có đặc số* (hoặc *đặc trưng*) 0, ký hiệu là $charR=0$ $charR=0$. Trường hợp e có cấp hữu hạn *p*, ta nói trường *R* có *đặc số* (hoặc *đặc trưng*) *p,* ký hiệu là $charR=p$.

2.4.9. Ví dụ:

Ví dụ 1: Các trường số $\mathbb{Q},\mathbb{R},\mathbb{C}$ đều có đặc số 0.

Ví dụ 2: Với p nguyên tố, trường $\mathbb{Z}_p$ các số nguyên modulo p có đặc số p.

Các định lý sau nêu lên tính chất của đặc số của các trường:

2.4.10: Định lý: Cho *R* là một trường. Các mệnh đề sau tương đương:

i) $charR=0$;

ii) Với mọi $x \in R\setminus\{0\}$ và $n \in \mathbb{Z}$, nếu $nx=0$ thì $n=0$;

iii) *R* chứa một trường con đẳng cấu (vành) với $\mathbb{Q}$.

Chứng minh: $(i)\Rightarrow(ii)$: Giả sử $charR=0$. Xét $x \in R\setminus\{0\}$ và $n \in \mathbb{Z}$ thỏa $nx=0$. Khi đó $0=nx=(ne)x$ và $x \neq 0$ nên $ne=0$. Suy ra: n = 0 (do $charR=0$).

$(ii) \Rightarrow (iii)$: Với giả thiết (ii), xét ánh xạ $f : \mathbb{Q} \to R$ định bởi $f\left(mn^{-1}\right) = (me)(ne)^{-1}$. Ta thấy f được xác định và là đơn ánh vì

$mn^{-1} = m'(n')^{-1} \Leftrightarrow mn' - m'n = 0 \Leftrightarrow (mn' - m'n)e = 0$ (do (ii))

$\Leftrightarrow (me)(n'e) - (m'e)(ne) = 0 \Leftrightarrow (me)(ne)^{-1} - (m'e)(n'e)^{-1} = 0$

$\Leftrightarrow f\left(mn^{-1}\right) = f\left(m'(n')^{-1}\right)$. Hơn nữa, f bảo toàn các phép toán vì

$f\left(mn^{-1} + m'(n')^{-1}\right) = f\left((mn' + m'n)(nn')^{-1}\right) = \left[(mn' + m'n)e\right](nn'e)^{-1}$

$= \left[(me)(n'e) + (m'e)(ne)\right](ne)^{-1}(n'e)^{-1} = (me)(ne)^{-1} + (m'e)(n'e)^{-1}$

$= f\left(mn^{-1}\right) + f\left(m'(n')^{-1}\right)$.

Và tương tự $f\left(\left(mn^{-1}\right)\left(m'(n')^{-1}\right)\right) = f\left(mn^{-1}\right) f\left(m'(n')^{-1}\right)$. Vậy f là đơn cấu vành. Suy ra Imf là trường con của R đẳng cấu với $\mathbb{Q}$.

$(iii) \Rightarrow (i)$: Vì $char\mathbb{Q} = 0$ nên trường con của R đẳng cấu với $\mathbb{Q}$ cũng có đặc số 0. Do đó R cũng có đặc số 0.

2.4.11. Định lý: Cho *R* là một trường và *p* là một số nguyên tố. Các mệnh đề sau tương đương:

i) $charR = p$;

ii) Với mọi $x \in R \setminus \{0\}$ và $n \in \mathbb{Z}$, $nx = 0$ khi và chỉ khi $p \mid n$;

iii) *R* chứa một trường con đẳng cấu (vành) với $\mathbb{Z}_p$.

Chứng minh: $(i) \Rightarrow (ii)$: Giả sử $charR = p$. Xét $x \in R \setminus \{0\}$ và $n \in \mathbb{Z}$ thỏa $nx = 0$. Khi đó $0 = nx = (ne)x$ và $x \neq 0$ nên $ne = 0$. Từ đây do $charR = p = |e|$ nên $p \mid n$. Đảo lại, nếu $p \mid n$ thì $nx = (ne)x = 0x = 0$.

$(ii) \Rightarrow (iii)$: Với giả thiết (ii), xét ánh xạ $f : \mathbb{Z} \to R$ định bởi $f(n) = ne$. Dễ thấy f là đồng cấu vành và $Kerf = p\mathbb{Z}$. Do đó theo định lý 2.3.9 ta có $\mathbb{Z}_p = \mathbb{Z} / p\mathbb{Z} \simeq Im f$. Chú ý rằng $\mathbb{Z}_p$ là trường do p nguyên tố nên R chứa trường con Imf đẳng cấu với $\mathbb{Z}_p$.

$(iii) \Rightarrow (i)$: Vì $char\mathbb{Z}_p = p$ nên trường con của R đẳng cấu với $\mathbb{Z}_p$ cũng có đặc trưng p. Do đó $charR = p$.

2.4.12. Nhận xét: Cho R là một trường có đặc số p nguyên tố. Khi đó ánh xạ $\varphi : R \to R$ định bởi $\varphi(x) = x^p$ là một tự đơn cấu của R.

Chứng minh: $\forall x, y \in R$ ta có: $\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$, hơn nữa

$$\varphi(x+y) = (x+y)^p = x^p + \sum_{k=1}^{p-1} C_p^k x^{p-k} y^k + y^p = x^p + y^p = \varphi(x) + \varphi(y)$$

do $C_p^k = \dfrac{p!}{k!(p-k)!}$ là bội số của p (p nguyên tố) $\forall 1 \le k \le p-1$. Điều này chứng tỏ φ là đồng cấu. Mặt khác do $Ker\varphi = 0$ nên φ là đơn cấu. (đpcm)

Xét R là một miền nguyên. Khi đó phép nhân trong R có tính giản ước cho các phần tử khác 0. Tuy nhiên điều đó chưa đủ để khẳng định mọi phần tử khác 0 đều khả nghich trong R. Ta sẽ xây dựng trường $\overline{R}$ nhỏ nhất có chứa R, trong đó mọi phần tử khác 0 của R đều khả nghịch trong $\overline{R}$. Ta gọi $\overline{R}$ là trường các thương của miền nguyên R.

2.4.13. Định nghĩa: Cho R là một miền nguyên và $\overline{R}$ là một trường. Ta nói $\overline{R}$ là *trường các thương* của miền nguyên R nếu tồn tại một đơn cấu (vành) $f : R \to \overline{R}$ sao cho mọi phần tử của $\overline{R}$ đều có dạng $f(a) f(b)^{-1}$ với $a, b \in R, b \neq 0$.

2.4.14. Định lý: Cho R là một miền nguyên. Khi đó trường các thương $\overline{R}$ của R luôn luôn tồn tại và duy nhất (sai khác một đẳng cấu).

2.4.15. Nhận xét: Vì ánh xạ $f : R \to \overline{R}$ định bởi $f(a) = \dfrac{a}{e}$ là đơn cấu vành nên ta có thể đồng nhất $a \in R$ với $\dfrac{a}{e} \in \overline{R}$. Do đó có thể xem $\overline{R}$ như là một trường chứa miền nguyên R và mọi phần tử thuộc $\overline{R}$ đều có dạng $\dfrac{a}{b} = \dfrac{a}{\varepsilon}\left(\dfrac{b}{\varepsilon}\right)^{-1} = ab^{-1}$ với $a, b \in R, b \neq 0$. Rõ ràng mọi trường chứa miền nguyên R đều phải chứa các phần tử có dạng ab^{-1} như thế nên $\overline{R}$ là trường nhỏ nhất chứa R.

2.4.16. Ví dụ: Trường các số hữu tỷ $\mathbb{Q}$ chính là trường các thương của miền nguyên $\mathbb{Z}$ vì $\mathbb{Q} = \left\{ \frac{a}{b} \mid a,b \in \mathbb{Z} \right\} = \left\{ ab^{-1} \mid a,b \in \mathbb{Z} \right\}$.

2.5. Vành đa thức một ẩn

2.5.1. Định nghĩa: Giả sử R là một vành giao hoán, có đơn vị 1. Gọi A là tập hợp tất cả các dãy $(a_0,a_1,...,a_n,...)$, trong đó các $a_i \in R, \forall i \in \mathbb{N}$ và bằng 0 tất cả trừ một số hữu hạn. Như vậy A là một bộ phận của lũy thừa Descartes $R^{\mathbb{N}}$.

Ta định nghĩa phép cộng và nhân trong A như sau: Giả sử $f = (a_0,a_1,...,a_n,...)$ và $g = (b_0,b_1,...,b_n,...)$ là các phần tử tùy ý của A. Khi đó

$$f + g = (a_0 + b_0, a_1 + b_1, ..., a_n + b_n, ...)$$

$$fg = (c_0,c_1,...,c_n,...), \text{ trong đó } c_k = \sum_{i+j=k} a_i b_j,\ k = 0,1,2,...$$

Dễ dàng kiểm tra lại rằng A cùng với hai phép toán đó lập nên một vành giao hoán, có đơn vị là $(1,0,0,...)$, phần tử không của vành này là $(0,0,0,...)$. Ta sẽ ký hiệu phần tử đơn vị của A là 1 và phần tử không của A là 0.

Đặt $x = (0,1,0,0,...)$. Dễ thấy rằng $x^2 = (0,0,1,0,...)$

$$x^3 = (0,0,0,1,0,...)$$

$$x^n = (0,0,...,0,1,0,...)$$

Ta quy ước $x^0 = (1,0,0,...)$ và mỗi phần tử $a \in R$ có thể đồng nhất với dãy $(a,0,0,...)$ nhờ đơn cấu vành

$$R \to A$$
$$a \mapsto (a,0,0,...)$$

Như vậy $ax^n = (0,0,...,0,a,0,...),\ \forall a \in R$.

Do đó $f = (a_0,a_1,...,a_n,0,0,...) = a_0 + a_1x + ... + a_nx^n$ và thường được viết là $f(x) = a_nx^n + ... + a_1x + a_0$

Cách biểu thị như vậy là duy nhất đối với mỗi phần tử $f \in A$. Nói cách khác:

$a_n x^n + ... + a_1 x + a_0 = b_n x^n + ... + b_1 x + b_0$ khi và chỉ khi $a_n = b_n, ..., a_1 = b_1, a_0 = b_0$.

Vành A nói trên được gọi là *vành đa thức của ẩn x* (hay *biến x*) với các hệ số trong *R*, và được ký hiệu là $R[x]$. Mỗi phần tử của $R[x]$ được gọi là *một đa thức của ẩn x* trên *R*. Đa thức dạng $ax^n \ (a \in R)$ được gọi là một *đơn thức*.

Giả sử $f(x) = a_n x^n + ... + a_1 x + a_0$ với $a_n \neq 0$. Khi đó ta nói đa thức $f(x)$ có *bậc* là n và ký hiệu $deg\ f = n$ hay $deg\ f(x) = n$. Phần tử a_i được gọi là *hệ số thứ i* của $f(x)$, phần tử a_n được gọi là *hệ số cao nhất*, còn phần tử a_0 được gọi là *hệ số tự do*. Bậc của đa thức 0 được quy ước là $-\infty$.

Dễ dàng thấy rằng: *i)* $deg(f(x) + g(x)) \leq max\{deg\ f(x), deg\ g(x)\}$

$$ii)\ deg(f(x)g(x)) \leq deg\ f(x) + deg\ g(x)$$

với $f(x)$ và $g(x)$ là hai đa thức bất kỳ trên *R*.

2.5.2. Định lý: Nếu D là một miền nguyên thì D[x] cũng là một miền nguyên.

2.5.3. Định lý (Phép chia Euclide): Giả sử K là một trường và $f(x), g(x) \in K[x], g(x) \neq 0$. Khi đó tồn 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 $g(x)$.

2.5.4. Ví dụ: Trong thực hành, để thực hiện phép chia đa thức $f(x)$ cho đa thức $g(x)$ ta sắp đặt như việc chia số nguyên. Chẳng hạn trong $\mathbb{Z}_{11}[x]$, để tìm thương và dư trong phép chia đa thức: $f(x) = -\bar{1}x^3 - \bar{7}x^2 + \bar{3}x - \bar{5}$ cho $g(x) = -\bar{2}x^2 + \bar{2}x - \bar{1}$ ta viết

$$\begin{array}{r|l} -\bar{1}x^3 - \bar{7}x^2 + \bar{3}x - \bar{5} & -\bar{2}x^2 + \bar{2}x - \bar{1} \\ \cline{2-2} -\bar{1}x^3 + \bar{1}x^2 - \bar{6}x & \bar{6}x + \bar{4} \\ -\bar{8}x^2 + \bar{9}x - \bar{5} & \\ -\bar{8}x^2 + \bar{8}x - \bar{4} & \\ \bar{1}x - \bar{1} & \end{array}$$

Vậy $-\bar{1}x^3 - \bar{7}x^2 + \bar{3}x - \bar{5} = \left(-\bar{2}x^2 + \bar{2}x - \bar{1}\right)\left(\bar{6}x + \bar{4}\right) + \bar{1}x - \bar{1}$

2.5.5. Định nghĩa: Cho các đa thức $f(x), g(x) \in K[x]$, ở đây K là một trường và $g(x) \neq 0$. Nếu tồn tại $q(x) \in K[x]$ sao cho $f(x) = q(x)g(x)$ thì ta nói $f(x)$ *chia hết cho* $g(x)$ (hay $g(x)$ là *ước* của $f(x)$) trong $K[x]$. Một đa thức $d(x) \in K[x]$ là ước 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 $d(x)$ 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 $g(x)$, viết tắt là UCLN, ký hiệu là $d(x) = (f(x), g(x))$. Để đảm bảo tính duy nhất của UCLN, ta quy ước rằng hệ số cao nhất của UCLN bao giờ cũng lấy bằng 1.

2.5.6. Thuật chia Euclide: 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:

$$f(x) = g(x)q(x) + r(x), \qquad deg\, r(x) < deg\, g(x)$$

$$g(x) = r(x)q_1(x) + r_1(x), \qquad deg\, r_1(x) < deg\, r(x)$$

…….

$$r_{k-2}(x) = r_{k-1}(x)q_k(x) + r_k(x), \qquad deg\, r_k(x) < deg\, r_{k-1}(x)$$

$$r_{k-1}(x) = r_k(x)q_{k+1}(x).$$

Đa thức dư cuối cùng khác 0 trong dãy phép chia nói trên chính là $r_k(x)$ và

$$UCLN = \frac{r_k(x)}{he\,so\,cao\,nhat\,cua\ r_k(x)}.$$

Từ thuật toán Euclide ta thấy rằng nếu $d(x) = (f(x), g(x))$ thì ta có thể tìm được hai đa thức $u(x), v(x) \in K[x]$ sao cho $f(x)u(x) + g(x)v(x) = d(x)$.

2.5.7. Ví dụ: Trong $\mathbb{R}[x]$ cho các đa thức $f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9$ và $g(x) = 2x^3 - x^2 - 5x + 4$. Tìm $d(x) = (f(x), g(x))$ và tìm các đa thức $u(x), v(x) \in \mathbb{R}[x]$ sao cho $f(x)u(x) + g(x)v(x) = d(x)$.

Giải: Để tìm UCLN của f(x) và g(x), ta thực hiện dãy các phép chia liên tiếp

$$\begin{array}{l|l} 4x^4-2x^3-16x^2+5x+9 & 2x^3-x^2-5x+4 \\ \hline 4x^4-2x^3-10x^2+8x & 2x \\ \qquad\qquad -6x^2-3x+9 & \end{array}$$

$f(x)=g(x)q(x)+r(x),\ \ r(x)=-6x^2-3x+9, q(x)=2x.$

Nhân g(x) với 3 rồi chia cho r(x):

$$\begin{array}{l|l} 6x^3-3x^2-15x+12 & -6x^2-3x+9 \\ \hline 6x^3+3x^2-9x & -x+1 \\ \qquad -6x^2-6x+12 & \\ \qquad -6x^2-3x+9 & \\ \qquad\qquad -3x+3 & \end{array}$$

$3g(x)=r(x)q_1(x)+r_1(x),\ \ q_1(x)=-x+1,\ \ r_1(x)=-3x+3$

Lấy r(x) chia cho $r_1(x)$ ta có:

$$\begin{array}{l|l} -6x^2-3x+9 & -3x+3 \\ \hline -6x^2+6x & 2x+3 \\ -9x+9 & \\ -9x+9 & \\ 0 & \end{array}$$

$r(x)=(2x+3)r_1(x).$

Do đó ta có $r_1(x)=-3x+3$ là dư cuối cùng khác 0. Theo quy ước, ta sẽ lấy $d(x)=(f(x),g(x))=x-1.$

Theo quá trình trên ta có: $r_1(x)=3g(x)-r(x)q_1(x)$

$$=3g(x)-q_1(x)(f(x)-g(x)q(x))$$

$$=(3+q(x)q_1(x))g(x)-q_1(x)f(x).$$

Suy ra $$d(x)=\frac{-x+1}{3}f(x)+\frac{2x^2-2x-3}{3}g(x).$$

2.5.8. Đa thức bất khả quy trên miền nguyên

Nếu D là miền nguyên thì D[x] cũng là miền nguyên (định lý 2.5.2). Đa thức $f(x) \in D[x]$ khác không, không khả nghịch gọi là *bất khả quy* trong D[x] (hay còn gọi là bất khả quy trên D) nếu nó không có ước thực sự trong D[x], tức là nếu $f(x) = g(x)h(x)$, $(g(x), h(x) \in D[x])$ thì g(x) hay h(x) phải là phần tử khả nghịch của D.

Nói riêng, nếu K là một trường thì các phần tử khả nghịch trong K[x] chính là các phần tử khác không của K. Đa thức $f(x) \in K[x]$, khác không, không khả nghịch là bất khả quy trên K khi và chỉ khi nếu $f(x) = g(x)h(x)$, $(g(x), h(x) \in K[x])$ thì g(x) hay h(x) là phần tử khác không của K. Số các đa thức bất khả quy trên một trường là vô hạn. Cụ thể ta có định lý sau:

2.5.9. Định lý: Có vô số đa thức với hệ số cao nhất là 1 bất khả quy trên trường K.

2.6. Nghiệm của đa thức

2.6.1. Định nghĩa: Giả sử $c \in R$ và $f(x) = a_n x^n + ... + a_1 x + a_0 \in R[x]$. Phần tử $f(c) = a_n c^n + ... + a_1 c + a_0$ được gọi là *giá trị* của f(x) tại *c*. Nếu $f(c) = 0$ thì *c* được gọi là *nghiệm* của f(x). Tìm nghiệm của f(x) trong *R* là giải phương trình đại số $a_n x^n + ... + a_1 x + a_0 = 0$ trong *R*.

2.6.2. Định lý Bezout: Phần tử *c* của trường K là nghiệm của đa thức $f(x) \in K[x]$ khi và chỉ khi $f(x)$ chia hết cho $x - c$.

2.6.3. Sơ đồ Horner: Cho $f(x) = a_n x^n + ... + a_1 x + a_0 \in K[x]$ và $c \in K$. Ta dùng sơ đồ Horner dưới đây để tìm $q(x) = b_{n-1} x^{n-1} + ... + b_1 x + b_0$ và $r = f(c)$ trong thuật chia Euclide $f(x) = (x - c)q(x) + r$.

	a_n	a_{n-1}	...	a_1	a_0
c	$b_{n-1} = a_n$	$b_{n-2} = a_{n-1} + cb_{n-1}$	...	$b_0 = a_1 + cb_1$	$r = a_0 + cb_0$

2.6.4. Ví dụ:

Ví dụ 1: Trong $\mathbb{Q}[x]$ cho $f(x) = 3x^5 + 4x^4 - 2x^3 + 5x^2 - x + 6$ và $c = 4 \in \mathbb{Q}$. Ta có sơ đồ Horner như sau:

	3	4	- 2	5	- 1	6
4	3	16	62	253	1011	4050

Vậy $f(x)=(x-4)q(x)+r$ với $q(x)=3x^4+16x^3+62x^2+253x+1011$ và $r=f(4)=4050$.

Ví dụ 2: Trong $\mathbb{Z}_7[x]$ cho $f(x)=\bar{2}x^5-x^3+\bar{3}x^2-\bar{2}$ và $c=-\bar{3}\in\mathbb{Z}_7$. Ta có sơ đồ Horner như sau:

	$\bar{2}$	$\bar{0}$	$-\bar{1}$	$\bar{3}$	$\bar{0}$	$-\bar{2}$
$-\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{3}$	$\bar{1}$	$-\bar{3}$	$\bar{0}$

Vậy $f(x)=(x+\bar{3})q(x)$ với $q(x)=\bar{2}x^4+x^3+\bar{3}x^2+x-\bar{3}$, $r=0$. Đa thức $f(x)$ chia hết cho $x+\bar{3}$ nên $c=-\bar{3}$ là một nghiệm của $f(x)$.

2.6.5. Định lý: Cho đa thức $f(x)$ trên trường K, $deg\, f(x)=n\geq 0$. Khi đó $f(x)$ có nhiều nhất n nghiệm trên K.

2.6.6. Hệ quả: Nếu hai đa thức trên trường K có cùng bậc n và lấy những giá trị bằng nhau tại $n+1$ phần tử khác nhau của K thì chúng bằng nhau.

2.6.7. Nhận xét: Hệ quả 2.6.6 vẫn còn đúng cho các đa thức trên miền nguyên R. Nếu R không phải là miền nguyên thì hệ quả trên không đúng.

2.6.8. Định nghĩa: Cho đa thức $f(x)$ trên trường K.

(i) Nếu $f(x)=a_0\in K$, đặt $f'(x)=0$. Nếu $f(x)=\sum_{k=0}^{n}a_kx^k$ với $n\geq 1$, đặt $f'(x)=\sum_{k=1}^{n}ka_kx^{k-1}$. Ta gọi $f'(x)$ là đạo hàm của $f(x)$.

(ii) Đặt $f^{(0)}(x)=f(x)$, $f^{(1)}(x)=f'(x)$, $f^{(2)}(x)=\left(f^{(1)}(x)\right)'$,..., $f^{(k)}(x)=\left(f^{(k-1)}(x)\right)'$, $\forall k\in\mathbb{N}^*$. Ta nói $f^{(m)}(x)$ là đạo hàm cấp m của $f(x)$, $\forall m\in\mathbb{N}$.

2.6.9. Khai triển Taylor: Cho đa thức $f(x)$ trên trường K và $deg\, f(x)=n$. Khi đó với mỗi $c\in K$ đa thức $f(x)$ có thể khai triển duy nhất dưới dạng $f(x)=\sum_{k=0}^{n}c_k(x-c)^k$.

Thật vậy, thực hiện phép chia $f(x)$ cho $x-c$ ta có $f(x)=(x-c)g(x)+c_0$, trong đó $c_0 \in K$ và $g(x) \in K[x]$, $(deg\, g(x)=n-1)$ xác định duy nhất. Lại tiếp tục thực hiện phép chia g(x) cho $x-c$ ta có duy nhất $c_1 \in K$ và $g_1(x) \in K[x]$ sao cho $g(x)=(x-c)g_1(x)+c_1,\ deg\, g_1(x)=n-2$.

Khi đó ta có $f(x)=(x-c)^2 g_1(x)+c_1(x-c)+c_0$.

Lặp lại quá trình trên, cuối cùng ta được:

$$f(x)=c_n(x-c)^n+c_{n-1}(x-c)^{n-1}+...+c_1(x-c)+c_0$$

Nhờ sơ đồ Horner ta dễ dàng thu được các hệ số $c_0,...,c_n$ như bảng sau:

	a_n	a_{n-1}	…	a_1	a_0
c	a_n	*	…	*	$[c_0]$
c	a_n	*	…	$[c_1]$	
⋮	⋮	⋮	⋮		
c	a_n	$[c_{n-1}]$ $[c_{n-1}]$			
c	$[c_n=a_n]$				

2.6.10. Ví dụ: Trong vành $\mathbb{Q}[x]$, để phân tích đa thức $f(x)=x^4-x^3+1$ theo các lũy thừa của $x-3$ ta lập sơ đồ Horner

	1	–1	0	0	1
3	1	2	6	18	[55]
3	1	5	21	[81]	
3	1	8	[45]		
3	1	[11]			
3	[1]				

Từ đó $f(x)=(x-3)^4+11(x-3)^3+45(x-3)^2+81(x-3)+55$

2.6.11. Nhận xét: Trong trường hợp K là trường có đặc số 0 thì các hệ số c_k trong khai triển Taylor có thể tính theo các đạo hàm của đa thức $f(x)$ như sau: $c_k = \frac{f^{(k)}(c)}{k!}$, nghĩa là $f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(c)}{k!}(x-c)^k$.

2.6.12. Định nghĩa: Giả sử k là một số tự nhiên khác không, R là miền nguyên. Phần tử $c \in R$ được gọi là nghiệm bội k của đa thức $f(x) \in R[x]$ nếu $f(x)$ chia hết cho $(x-c)^k$ nhưng không chia hết cho $(x-c)^{k+1}$, nghĩa là $f(x)$ có thể phân tích thành $f(x) = (x-c)^k g(x)$ với $g(x) \in R[x]$ và $g(c) \neq 0$.

2.6.13. Ví dụ: Trong $\mathbb{Z}_7[x]$, cho $f(x) = \bar{2}x^4 - \bar{3}x^3 + \bar{2}x - \bar{3}$ và $c = -\bar{2} \in \mathbb{Z}_7$. Để kiểm tra xem c có là nghiệm của $f(x)$ hay không, nếu có thì là nghiệm bội bao nhiêu, ta sẽ dùng sơ đồ Horner một số lần liên tiếp như sau:

	$\bar{2}$	$-\bar{3}$	$\bar{0}$	$\bar{2}$	$-\bar{3}$
$-\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{0}$	$\bar{2}$	$[\bar{0}]$
$-\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{1}$	$[\bar{0}]$	
$-\bar{2}$	$\bar{2}$	$-\bar{1}$	$[\bar{3}]$		

Căn cứ vào sơ đồ Horner ta thấy $c = -\bar{2}$ là một nghiệm kép của $f(x)$.

2.6.14. Công thức Viet: Cho đa thức $f(x) \in K[x]$, $f(x) = a_n x^n + ... + a_1 x + a_0$, $a_n \neq 0$. Giả sử $f(x)$ có n nghiệm (kể cả số bội) là $\alpha_1, \alpha_2, ..., \alpha_n \in K$. Khi đó ta có $f(x) = a_n(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$. Khai triển vế phải và so sánh các hệ số của các lũy thừa giống nhau ta sẽ được công thức sau gọi là *công thức Viet*, chúng biểu thị các hệ số của đa thức theo các nghiệm của nó:

$$\frac{a_{n-1}}{a_n} = -(\alpha_1 + \alpha_2 + ... + \alpha_n) = -\sum_{i=1}^{n} \alpha_i$$

$$\frac{a_{n-2}}{a_n} = \sum_{1 \le i < j \le n} \alpha_i \alpha_j$$

$$\vdots \qquad \vdots$$

$$\frac{a_{n-k}}{a_n} = (-1)^k \sum_{1 \le i_1 < i_2 < \ldots < i_k \le n} \alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_k}$$

$$\vdots \qquad \vdots$$

$$\frac{a_0}{a_n} = (-1)^n \alpha_1 \alpha_2 \ldots \alpha_n$$

Ta thấy rằng các vế phải của công thức Viet không thay đổi nếu ta thực hiện phép hoán vị bất kỳ trên các nghiệm $\alpha_1, \alpha_2, \ldots, \alpha_n$. Đó là những đa thức đối xứng.

2.6.16. Ví dụ:

Ví dụ 1: Nếu x_1 và x_2 là các nghiệm của một phương trình bậc hai $ax^2 + bx + c = 0,\ a \neq 0$ thì ta có: $x_1 + x_2 = -\frac{b}{a}$ và $x_1.x_2 = \frac{c}{a}$.

Ví dụ 2: Nếu x_1, x_2 và x_3 là các nghiệm của một phương trình bậc ba $ax^3 + bx^2 + cx + d = 0,\ a \neq 0$ thì ta có: $x_1 + x_2 + x_3 = -\frac{b}{a}$,

$x_1.x_2 + x_2.x_3 + x_3.x_1 = \frac{c}{a}$ và $x_1.x_2.x_3 = -\frac{d}{a}$.

BÀI TẬP CHƯƠNG 2

1. Chứng minh tập hợp các số có dạng $a + b\sqrt{2}$ (với $a,b \in \mathbb{Z}$) với phép cộng và phép nhân các số lập thành một vành giao hoán, có đơn vị.

2. Chứng minh rằng nếu một miền nguyên X mà có đặc số $m \neq 0$ thì m phải là một số nguyên tố.

3. Tìm các ước của không trong vành $\mathbb{Z}/6\mathbb{Z}$.

4. Chứng minh tập hợp $X = \mathbb{Z} \times \mathbb{Z}$ cùng với hai phép toán:

$(a_1,b_1) + (a_2,b_2) = (a_1 + a_2, b_1 + b_2)$ và $(a_1,b_1)(a_2,b_2) = (a_1a_2, b_1b_2)$

là một vành giao hoán, có đơn vị. Tìm tất cả các ước của không của vành này.

5. Giả sử X là một vành có tính chất sau đây: $x^2 = x\ \forall x \in X$. Chứng minh rằng:

a. $x=-x\ \ \forall x\in X$;

b. X là vành giao hoán;

c. Nếu X là vành không có ước của 0, có nhiều hơn một phần tử thì X là miền nguyên.

6. Cho X là một vành tùy ý, A và B là hai Ideal của X. Chứng minh rằng bộ phận $A+B=\{a+b\,|\,a\in A,b\in B\}$ là một Ideal của X.

7. Cho X là một vành tùy ý, n là một số nguyên cho trước. Chứng minh bộ phận $A=\{x\in X\,|\,nx=0\}$ là một Ideal của X.

8. Cho m và n là hai số nguyên dương. Chứng minh rằng $m\mathbb{Z}+n\mathbb{Z}=\mathbb{Z}$ khi và chỉ khi m và n nguyên tố cùng nhau.

9. Giả sử $f:X\to X$ là một tự đồng cấu của vành X. Chứng minh rằng tập hợp $A=\{x\in X\,|\,f(x)=x\}$ là một vành con của X.

10. Chứng minh rằng trường các số hữu tỷ không có trường con nào khác ngoài bản thân nó.

11. Chứng minh rằng bộ phận $A=\{a+b\sqrt{2}\,|\,a,b\in\mathbb{Q}\}$ là một trường con của trường số thực $\mathbb{R}$.

12. Tìm tập các tự đẳng cấu của trường $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\,|\,a,b\in\mathbb{Q}\}$.

13. Giả sử p là một số nguyên tố. Chứng minh rằng tập hợp các số hữu tỷ có dạng $\frac{m}{n}$, trong đó n nguyên tố với p, là một miền nguyên. Tìm trường các thương của miền nguyên này.

14. Cho X là một miền nguyên. Chứng minh rằng X là một trường khi và chỉ khi X chỉ có hai Ideal tầm thường là $\{0\}$ và X.

15. Trong vành đa thức $\mathbb{Z}_5[x]$ hãy thực hiện các phép nhân:

a. $(\bar{2}x^2+\bar{4}x+\bar{1}).(\bar{3}x^2+\bar{1}x+\bar{2})$

b. $(-\bar{2}x^2+\bar{4}x+\bar{3})^2$

16. Trong vành $\mathbb{Z}_6[x]$ thực hiện phép nhân: $\left(\bar{2}x^3+\bar{4}x^2+\bar{1}x\right).\left(\bar{3}x^2+\bar{3}x+\bar{2}\right)$.

17. Trong vành $\mathbb{Z}_5[x]$ hãy thực hiện phép chia $f(x)=-\bar{1}x^3+\bar{2}x^2+\bar{2}x+\bar{1}$ cho $g(x)=-\bar{2}x^2+\bar{2}x-\bar{1}$.

18. Phân tích đa thức sau thành các nhân tử:

$$f(x,y)=6x^4-11x^3y-18x^2y^2-11xy^3+6y^4$$

19. Giả sử $f(x)=x^5+x^3+x^2+x+1$ và $g(x)=x^3+2x^2+x+1$. Tìm ước chung lớn nhất của f(x) và g(x) trong $\mathbb{Q}[x]$.

20. Tìm ước chung lớn nhất của f(x) và g(x) trong $\mathbb{Z}_3[x]$ với $f(x)=\bar{1}x^5+\bar{1}x^3+\bar{1}x^2+\bar{1}x+\bar{1}$ và $g(x)=\bar{1}x^3+\bar{2}x^2+\bar{1}x+\bar{1}$.

21. Dừng thuật chia Euclide tìm UCLN của hai đa thức trong $\mathbb{Q}[x]$

a. $f(x)=x^6+3x^4-4x^3-3x^2+8x-5$ và $g(x)=x^5+x^2-x+1$.

b. $f(x)=x^5+x^4-x^3-3x^2-3x-1$ và $g(x)=x^4-2x^3-x^2-2x+1$.

c. $f(x)=x^4-4x^3+1$ và $g(x)=x^3-3x^2+1$.

22. Dùng thuật toán Euclide tìm các đa thức p(x) và q(x) sao cho:
f(x)p(x) + g(x)q(x) = d(x), trong đó d(x) là ước chung lớn nhất của f(x) và g(x) với:

a. $f(x)=x^4+2x^3-x^2-4x-2$ và $g(x)=x^4+x^3-x^2-2x-2$.

b. $f(x)=4x^4-3x^3-16x^2+5x+9$ và $g(x)=2x^3-x^2-5x+4$.

Chương 3: LÝ THUYẾT CHIA HẾT VÀ ĐỒNG DƯ

3.1. Phép chia hết và có dư trên vành số nguyên

3.1.1. Phép chia hết:

Xét $a,b\in\mathbb{Z}$ và $b\neq 0$. Ta nói b chia hết a (là ước của a) hay a chia hết cho b (là bội của b) khi tồn tại $q\in\mathbb{Z}$ sao cho: $a=bq$. Ký hiệu: $b\,|\,a\Leftrightarrow\exists q\in\mathbb{Z}$ sao cho $a=bq\Leftrightarrow a\vdots b$

Ví dụ: i) $3\,|\,6$ vì $\exists\,2\in\mathbb{Z}$ mà $6=3.2$

ii) $(n\neq 0)$ $0\vdots n$ vì $\exists\,0\in\mathbb{Z}$ mà $0=n.0$: 0 là bội của mọi số nguyên $n\neq 0$

iii) $1\,|\,n$ vì $\exists\,n\in\mathbb{Z}$ mà $n=1.n$: 1 là ước của mọi số nguyên n

3.1.2. Tính chất của phép chia hết:

i) $b\,|\,a\Leftrightarrow\pm b\,|\,\pm a$

ii) $\forall a\neq 0,\ a\,|\,a$

iii) $\forall a,\ \pm 1\,|\,a$

iv) $\forall a\neq 0,\ a\,|\,0$

v) $(a\,|\,b$ và $b\,|\,a)\Leftrightarrow a=\pm b$

vi) $(a\,|\,b$ và $b\,|\,c)\Rightarrow a\,|\,c$

vii) $(c\,|\,a$ và $c\,|\,b)\Rightarrow c\,|\,(ax+by)$

viii) $(a\,|\,x$ và $b\,|\,y)\Rightarrow ab\,|\,xy$

3.1.3. Phép chia có dư: Nếu $a,b\in\mathbb{Z}$ và $b\neq 0$ thì tồn tại duy nhất cặp số nguyên (q,r) sao cho: $\begin{cases}a=bq+r\\0\le r<|b|\end{cases}$, với q là thương, r là dư. Khi $r=0$ ta có phép chia hết.

Ví dụ:

a	b	q	r
11	4	2	3
-18	5	-4	2
10	-7	-1	3
21	3	7	0

3.2. Ước chung lớn nhất (UCLN)

3.2.1. Một số định nghĩa: Cho n số nguyên $a_1,a_2,...,a_n \in \mathbb{Z}$.

*** Ước chung:** Số nguyên $d \in \mathbb{Z}$ được gọi là ước chung (UC) của các $a_i \left(i=\overline{1,n}\right)$ khi d là ước của mỗi a_i.

Ví dụ: ± 1 ± 2 ± 3 là các ước chung của $\pm 24, \pm 54, \pm 60$

*** Ước chung lớn nhất:** Ước chung d của các $a_i \left(i=\overline{1,n}\right)$ được gọi là ước chung lớn nhất (UCLN) nếu d là bội của mọi ước chung khác của các a_i. Ký hiệu: $d=\left(a_1,a_2,...,a_n\right)$.

Ví dụ: $\left(18,24,-30\right)=\pm 6$

$\left(13,34,8\right)=\pm 1$

Ghi chú: Nếu d là UCLN của các a_i thì $-d$ cũng là UCLN của các a_i, giữa chúng sẽ có một giá trị dương. Người ta quy ước UCLN là một số dương. Vậy: $\left(18,24,-30\right)=6$ và $\left(13,34,8\right)=1$.

Nhận xét: $\left(a,b\right)=\left(b,a\right)$: giao hoán

$\left(\left(a,b\right),c\right)=\left(a,\left(b,c\right)\right)=\left(a,b,c\right)$: kết hợp

*** Số nguyên tố cùng nhau:** Nếu UCLN của các a_i bằng 1 thì các a_i được gọi là nguyên tố cùng nhau. Ta có $\left(a_1,a_2,...,a_n\right)=1 \Leftrightarrow a_1,a_2,...,a_n$ là nguyên tố cùng nhau.

Ví dụ: $\left(2,5,12,15\right)=1$ nên chúng là nguyên tố cùng nhau.

*** Số nguyên tố sánh đôi:** Nếu UCLN của 2 số bất kỳ trong các số $a_1,a_2,...,a_n$ là nguyên tố cùng nhau thì các a_i được gọi là nguyên tố sánh đôi.

Ví dụ: 4, 21, 19, 11 là nguyên tố sánh đôi.

Nhận xét: Nếu $a_1,a_2,...,a_n$ là nguyên tố sánh đôi thì $a_1,a_2,...,a_n$ là nguyên tố cùng nhau.

3.2.2. Sự tồn tại UCLN: Nếu các số nguyên $a_1,a_2,...,a_n$ không đồng thời bằng 0 thì tồn tại UCLN của chúng.

3.2.3. Các tính chất của UCLN:

i) Nếu $\left(a_1,a_2,...,a_n\right)=d$ thì tồn tại các số nguyên $x_1,x_2,...,x_n$ sao cho $a_1x_1+a_2x_2+...+a_nx_n=d$.

ii) Nếu m là số nguyên dương thì $(ma_1, ma_2, ..., ma_n) = m(a_1, a_2, ..., a_n)$.

iii) Nếu $d > 0$ là ước chung của $a_1, a_2, ..., a_n$ thì $\left(\frac{a_1}{d}, \frac{a_2}{d}, ..., \frac{a_n}{d}\right) = \frac{(a_1, a_2, ..., a_n)}{d}$.

iv) Nếu $d > 0$ là ước chung của $a_1, a_2, ..., a_n$ thì d là UCLN của $a_1, a_2, ..., a_n$ khi và chỉ khi $\left(\frac{a_1}{d}, \frac{a_2}{d}, ..., \frac{a_n}{d}\right) = 1$.

v) Nếu $b > 0$ là ước của a thì $(a, b) = b$.

vi) Nếu $c \mid ab$ và $(a, c) = 1$ thì $c \mid b$.

vii) Nếu $b \mid a$ và $c \mid a$ và $(b, c) = 1$ thì $bc \mid a$.

viii) Nếu $(a, b) = 1$ thì $(ac, b) = (c, b)$.

ix) Nếu $(a, b) = (a, c) = 1$ thì $(a, bc) = 1$.

3.2.4. Thuật toán Euclide tìm UCLN: Nếu a, b là 2 số nguyên dương và $a = bq + r$ với $0 \le r < |b|$ thì $(a, b) = (b, r)$.

Ví dụ: $(51, 45) = (45, 6) = (6, 3) = 3$

3.3. Bội chung nhỏ nhất

3.3.1. Một số định nghĩa: Xét các số nguyên $a_1, a_2, ..., a_n \in \mathbb{Z}$ đều khác 0.

*** Bội chung:** Số nguyên M được gọi là bội chung (BC) của các a_i khi nó là bội của mỗi $a_i \ (i = 1, 2, ..., n)$.

Ví dụ: ± 18 là bội chung của $\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18, ...$

± 24 là bội chung của $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24, ...$

*** Bội chung nhỏ nhất:** Bội chung M của các $a_i \ (i = 1, 2, ..., n)$ được gọi là bội chung nhỏ nhất (BCNN) nếu nó là ước của mọi bội chung khác của các a_i. Ký hiệu: $M = [a_1, a_2, ..., a_n]$.

Ví dụ: $[2, 3, 4] = \pm 12$ và $[7, 3, 5] = \pm 105$

Ghi chú: Tương tự như UCLN, BCNN được quy ước là một số nguyên dương. Do đó ta có: $[2,3,4]=12$ và $[7,3,5]=105$.

Nhận xét: $[a,b]=[b,a]$: giao hoán.

$$[a,[b,c]]=[[a,b],c]=[a,b,c]$$: kết hợp.

3.3.2. Sự tồn tại BCNN: Có BCNN của các số nguyên khác không $a_1,a_2,...,a_n$ cho trước.

3.3.3. Mối liên hệ giữa BCNN và UCLN: Với 2 số nguyên dương a và b ta có $[a,b]=\frac{ab}{(a,b)}$.

3.3.4. Các tính chất của BCNN: Xét các số nguyên khác không $a_1,a_2,...,a_n$

i) Nếu số nguyên $M>0$ là bội chung của $a_1,a_2,...,a_n$ thì $M=[a_1,a_2,...,a_n]\Leftrightarrow\left(\frac{M}{a_1},\frac{M}{a_2},...,\frac{M}{a_n}\right)=1$.

ii) Nếu $k>0$ là một số nguyên thì $[ka_1,ka_2,...,ka_n]=k[a_1,a_2,...,a_n]$.

iii) Nếu $d=(a_1,a_2,...,a_n)$ thì $\left[\frac{a_1}{d},\frac{a_2}{d},...,\frac{a_n}{d}\right]=\frac{[a_1,a_2,...,a_n]}{d}$

iv) Nếu $a_1,a_2,...,a_n$ là các số nguyên tố sánh đôi thì $[a_1,a_2,...,a_n]=a_1a_2...a_n$

3.4. Số nguyên tố và hợp số

3.4.1. Số nguyên tố và hợp số:

*** Số nguyên tố:** Một số nguyên p>1 được gọi là số nguyên tố nếu p không có ước số dương nào khác ngoài 1 và chính nó (không có ước dương thực sự).

Ví dụ: 2, 3, 5, 7,… là các số nguyên tố.

*** Hợp số:** Một số nguyên a>1 được gọi là hợp số nếu a có ước số dương khác 1 và khác chính nó (có ước dương thực sự).

Ví dụ: 4, 6, 8, 9,… là các hợp số.

3.4.2. Các kết quả về số nguyên tố: Ước số dương nhỏ nhất khác 1 của số nguyên lớn hơn 1 là một số nguyên tố.

Ví dụ: Các ước số dương >1 của 20 là: 2, 4, 5, 10,…

Các ước số dương >1 của 45 là: 3, 5, 9, 15,…

*** Định lý Euclide:** Tập hợp các số nguyên tố là vô hạn.

3.4.3. Bảng số nguyên tố - Sàng Erathosthene

*** Bổ đề:** Một hợp số a>1 có ít nhất một ước nguyên tố không vượt quá $\sqrt{a}$.

Người ta dựa vào bổ đề trên để lập ra bảng các số nguyên tố không vượt quá một số n>1, gọi là sàng Erathosthene như sau:

- Viết các dãy số từ 2 đến n.
- Tìm các số nguyên tố từ 2 đến $\sqrt{n}$.
- Xóa đi các bội thực sự của các số nguyên tố này.
- Các số còn lại là các số nguyên tố cần tìm.

*** Ví dụ:** Tìm các số nguyên tố không vượt quá 100.

	2	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

Nhận xét: Nếu một số nguyên a>1 không có ước nguyên tố nào vượt quá $\sqrt{a}$ thì a là số nguyên tố.

Ví dụ: $\sqrt{257} < 17$. Các số nguyên tố không vượt quá $\sqrt{257}$ là: 2, 3, 5, 7, 11, 13 đều không là ước của 257 nên 257 là số nguyên tố.

3.4.4. Định lý cơ bản của số học

Bổ đề 1: Nếu p là số nguyên tố, a là số nguyên dương thì:

- Hoặc p là ước của a.

- Hoặc p là nguyên tố cùng nhau với a.

Ví dụ: - $(5,15)=5$

- $(5,12)=1$

*** Bổ đề 2:** Nếu một tích các số nguyên dương chia hết cho số nguyên tố p thì phải có ít nhất một thừa số của tích đó chia hết cho p.

Nhận xét: Nếu tích các số nguyên tố $p_1, p_2, ..., p_n$ chia hết cho p thì p phải trùng với một trong các số nguyên tố của tích đó.

*** Định lý cơ bản của số học:** Mỗi số nguyên a>1 đều có thể phân tích được thành tích của các thừa số nguyên tố và sự phân tích đó là duy nhất nếu không kể đến thứ tự các thừa số.

Ví dụ: - $8=2.2.2=2^3$

- $18=2.3.3=2.3^2$

Nhận xét: Nếu số nguyên a>1 được phân tích thành thừa số nguyên tố có dạng $a=p_1^{\alpha_1}p_2^{\alpha_2}...p_n^{\alpha_n}$ thì số nguyên d>0 là ước của a khi và chỉ khi d được phân tích thành thừa số nguyên tố có dạng: $d=p_1^{\beta_1}p_2^{\beta_2}...p_n^{\beta_n}$ với $0\le\beta_i\le\alpha_i\ \left(i=\overline{1,n}\right)$.

Ví dụ: $180=2^2.3^2.5$

$90\,|\,180$ ta thấy $90=2.3^2.5$

$18\,|\,180$ ta thấy $18=2.3^2$

3.4.5. Một số vấn đề về số nguyên tố

*** Số nguyên tố thứ n:** Gọi p_n là số nguyên tố thứ n. Ta thấy: $p_1=2,\ p_2=3,\ p_3=5,\ldots$ Một cách tổng quát vẫn chưa tìm ra công thức tính p_n.

*** Số nguyên tố Fermat:** Nhà toán học Fermat đưa ra một công thức cho số nguyên tố như sau: $F_n=2^{2^n}+1\ \ (n=0,1,2,...)$.

Công thức này cho: $F_0=3,\ F_1=5,\ F_2=17,\ F_3=257$ là các số nguyên tố.

$F_5=2^{2^5}+1$ là hợp số vì là bội của 641.

*** Giả thiết Golbach – Euler:**

- Có phải chăng mọi số nguyên lẻ lớn hơn 5 đều được biểu diễn thành tổng của 3 số nguyên tố?

Ví dụ: $25=3+11+11=7+7+11$

- Có phải chăng mọi số chẵn lớn hơn 2 đều được biểu diễn thành tổng của 2 số nguyên tố?

Ví dụ: $34=5+29=3+31$

3.5. Phương trình Diophante

Một phương trình có nhiều ẩn số với tất cả các hệ số đều là số nguyên và phải tìm nghiệm nguyên của nó được gọi là phương trình Diophante.

Ví dụ: $7x+4y=100$

$$x^2+y^2=z^2$$

$$x^3-7y^2=1$$

3.5.1. Phương trình bậc nhất 2 ẩn

*** Dạng tổng quát:** Phương trình bậc nhất 2 ẩn có dạng tổng quát $ax+by=c\ (1)$ với $a,b\in\mathbb{Z}$ là các hệ số; $x,y\in\mathbb{Z}$ là các ẩn cần xác định giá trị

*** Nghiệm của phương trình:** Điều kiện cần và đủ để phương trình (1) có nghiệm nguyên là (a,b) là ước của c.

Ví dụ 1: Phương trình $2x-3y=5$ có nghiệm vì $(2,-3)=1|5$. Một nghiệm của phương trình này là $x=4$ và $y=1$.

Ví dụ 2: Phương trình $6x+4y=7$ vô nghiệm vì (6, 4) = 2 không là ước của 7.

*** Định lý:** Nếu phương trình $ax+by=c$ có một nghiệm nguyên (x_0,y_0) thì nó có vô số nghiệm nguyên (x,y) được tính bởi công thức: $\begin{cases} x=x_0+\dfrac{b}{d}t \\ y=y_0-\dfrac{a}{d}t \end{cases}$ hay $\begin{cases} x=x_0-\dfrac{b}{d}t \\ y=y_0+\dfrac{a}{d}t \end{cases}$ trong đó $\begin{cases} t\in\mathbb{Z} \\ d=(a,b) \end{cases}$.

Ví dụ: Phương trình $2x-3y=5$ có $d=(2,-3)=1|5$ nên có nghiệm, một nghiệm của phương trình là: $x_0=4, y_0=1$ nên nó có vô số nghiệm là: $\begin{cases}x=4-3t\\y=1-2t\end{cases} t\in\mathbb{Z}$

Với t = 0 thì $x=4, y=1$

Với t = 1 thì $x=1, y=-1$

Với t = 2 thì $x=-2, y=-3$

……..

*** Thực hành giải phương trình (1):** Để giải phương trình (1) người ta dựa vào các nhận xét sau đây:

i) Nếu $|a|$ hay $|b|$ bằng 1 thì việc tìm nghiệm nguyên của phương trình (1) coi như được giải quyết xong.

Ví dụ: Giải phương trình: $x-4y=2$

Phương trình này tương đương với $x=2+4y$.

Nghiệm của phương trình có dạng: $\begin{cases}x=2+4y\\y=t\end{cases} t\in\mathbb{Z}$

ii) Trong trường hợp $|a|$ và $|b|$ đều khác 0 và khác 1 thì bao giờ người ta cũng có thể chuyển việc tìm nghiệm nguyên của phương trình (1) về việc tìm nghiệm nguyên của phương trình bậc nhất hai ẩn mà ít nhất một hệ số của ẩn là ± 1.

Ví dụ: Giải phương trình: $47x-17y=5$

Phương trình tương đương với $17(2x-y)+13x=5 \Leftrightarrow \begin{cases}u=2x-y\\17u+13x=5\end{cases}$

$$\Leftrightarrow \begin{cases}u=2x-y\\13(u+x)+4u=5\end{cases} \Leftrightarrow \begin{cases}u=2x-y \qquad v=u+x\\13v+4u=5\end{cases}$$

$$\Leftrightarrow \begin{cases}u=2x-y \qquad v=u+x\\4(3v+u)+v=5\end{cases} \Leftrightarrow \begin{cases}u=2x-y \qquad v=u+x \quad t=3v+u\\4t+v=5\end{cases}$$

Phương trình sau cùng có hệ số của v bằng 1 nên ta có: $v=5-4t \quad t\in\mathbb{Z}$

Suy ra: $u = t - 3v = t - 3(5 - 4t) = -15 + 13t$

$x = v - u = (5 - 4t) - (-15 + 13t) = 20 - 17t$

$y = 2x - u = 2(20 - 17t) - (-15 + 13t) = 55 - 47t$

Vậy nghiệm của phương trình là: $\begin{cases} x = 20 - 17t \\ y = 55 - 47t \end{cases} \quad t \in \mathbb{Z}$

3.5.2. Phương trình bậc nhất nhiều ẩn: Một phương trình bậc nhất n ẩn, sau khi đã chia hai vế của phương trình cho UCLN của các hệ số, có nghiệm nguyên khi và chỉ khi hệ số của các ẩn là nguyên tố cùng nhau.

Ví dụ 1: Giải phương trình $2x - 5y - 6z = 4 \quad (1)$

Vì $(2,-5,-6) = 1$ nên phương trình có nghiệm.

Ta có $(2,-5) = 1$ nên biến đổi $(1) \Leftrightarrow 2x - 5y = 4 + 6z \Leftrightarrow \begin{cases} z = u \\ c = 4 + 6z = 4 + 6u \\ 2x - 5y = c \end{cases}$

Phương trình cuối có một nghiệm là $(3c, c)$ nên có nghiệm tổng quát là:

$\begin{cases} x = 3c + 5t = 3(4 + 6u) + 5t = 12 + 18u + 5t \\ y = c + 2t = 4 + 6u + 2t \end{cases}$

Vậy nghiệm của phương trình (1) là: $\begin{cases} x = 12 + 18u + 5t \\ y = 4 + 6u + 2t \\ z = u \end{cases}$ u và t là số nguyên.

Ví dụ 2: Giải phương trình $6x + y + 3z = 15 \quad (2)$

Vì $(6,1,3) = 1$ nên phương trình có nghiệm.

Phương trình này có hệ số của ẩn y bằng 1 nên khi x và z lấy bất kỳ giá trị nào thì y cũng có giá trị nguyên. Vậy nghiệm của phương trình là: $\begin{cases} x = u \\ z = t \\ y = 15 - 6u - 3t \end{cases}$ u và t là số nguyên.

Ví dụ 3: Giải phương trình $6x + 15y + 10z = 3 \quad (3)$

Vì $(6,15,10) = 1$ nên phương trình có nghiệm.

Vì trong các hệ số của ẩn không có cặp nào là nguyên tố cùng nhau nên ta không thể biến đổi giống như ví dụ 1. Ta tìm cách đặt ẩn số phụ để đưa về phương trình có hệ số của một ẩn nào đó bằng 1 giống như ví dụ 2.

Ta có: (3) $\Leftrightarrow 6x+10(y+z)+5y=3$

$$\Leftrightarrow \begin{cases} y+z=u \\ 6x+10u+5y=3 \end{cases} \Leftrightarrow \begin{cases} y+z=u \\ x+10u+5(y+x)=3 \end{cases} \Leftrightarrow \begin{cases} y+z=u \\ x+y=v \\ x+10u+5v=3 \end{cases}$$

Phương trình cuối có hệ số của x bằng 1 nên theo ví dụ 2 ta tính được:

$$\begin{cases} x=3-10u-5v \\ y=v-x=v-(3-10u-5v)=-3+10u+6v \\ z=u-y=u-(-3+10u+6v)=3-9u-6v \end{cases}$$

Vậy: nghiệm tổng quát của phương trình là: $\begin{cases} x=3-10u-5v \\ y=-3+10u+6v \\ z=3-9u-6v \end{cases}$ u và v là số nguyên.

3.6. Lý thuyết đồng dư

3.6.1. Quan hệ đồng dư: Với $a,b,m>0$ là các số nguyên, *a* và *b* được gọi là *đồng dư theo modulo m* nếu *a* và *b* có cùng số dư khi chia chúng cho *m*, ký hiệu: $a\equiv b\,(mod\,m)$ và được gọi là *đồng dư thức*.

Nhận xét: - $a\equiv b\,(mod\,m)\Leftrightarrow b\equiv a\,(mod\,m)$

- *a* chia hết cho *m* khi và chỉ khi $a\equiv 0\,(mod\,m)$

Ví dụ: $16\equiv 11\,(mod\,5)\equiv 6\,(mod\,5)\equiv 1\,(mod\,5)$.....

$-7\equiv 2\,(mod\,3)\equiv 5\,(mod\,3)$.....

$12\equiv 0\,(mod\,2)\equiv 4\,(mod\,2)$.....

3.6.2. Hệ thặng dư đầy đủ: Quan hệ đồng dư theo modulo *m* trên tập số nguyên $\mathbb{Z}$ là một quan hệ tương đương, nó phân hoạch tập này thành m lớp như được ký hiệu sau:

- Lớp $\bar{0}$ gồm các số đồng dư với 0 theo modulo m.
- Lớp $\bar{1}$ gồm các số đồng dư với 1 theo modulo m.

- Lớp $\overline{2}$ gồm các số đồng dư với 2 theo modulo m.

- ……..

- Lớp $\overline{m-1}$ gồm các số đồng dư với $(m-1)$ theo modulo *m*.

Trong mỗi lớp trên người ta lấy ra một phần tử, gọi là phần tử đại diện. Tập hợp các phần tử đại diện đó được gọi là một hệ thặng dư đầy đủ theo modulo *m*. Hệ thặng dư đầy đủ không âm bé nhất modulo *m* thường được sử dụng là: 0 1 2 ..... $(m-1)$

Ví dụ: Hệ thặng dư đầy đủ không âm bé nhất modulo 10 là: 0 1 2 3 4 5 6 7 8 9

Định lý: Những mệnh đề sau đây là tương đương:

i) $a \equiv b \,(mod\, m)$

ii) $a = b + mt$ (t là một số nguyên)

iii) $(a-b) \equiv 0 \,(mod\, m)$

3.6.3. Tính chất: *m* là số nguyên dương

i) Nếu $a_i \equiv b_i \,(mod\, m)$ $(i = 1,2,...,n)$ thì

$$(a_1 + a_2 + ... + a_n) \equiv (b_1 + b_2 + ... + b_n) \,(mod\, m)$$ và

$$(a_1, a_2, ..., a_n) \equiv (b_1, b_2, ..., b_n) \,(mod\, m)$$

ii) $a \equiv b \,(mod\, m) \Leftrightarrow (a \pm c) \equiv (b \pm c) \,(mod\, m)$ (c là một số nguyên). Là hệ quả của tính chất (i).

iii) $a \equiv b \,(mod\, m) \Leftrightarrow a \equiv (b + km) \,(mod\, m) \Leftrightarrow (a + km) \equiv b \,(mod\, m)$ (k là một số nguyên).

iv) Nếu $a \equiv b \,(mod\, m)$ thì $a^n \equiv b^n \,(mod\, m)$ (n là số nguyên dương). Là hệ quả của tính chất (i).

v) Nếu $a \equiv b \,(mod\, m)$ thì $ac \equiv bc \,(mod\, m)$ (c là một số nguyên).

Nếu $(c, m) = 1$ thì $a \equiv b \,(mod\, m) \Leftrightarrow ac \equiv bc \,(mod\, m)$.

vi) Nếu $c > 0$ thì $a \equiv b \,(mod\, m) \Leftrightarrow ac \equiv bc \,(mod\, mc)$.

vii) Nếu $d>0$ là ước chung của a,b,m thì $a\equiv b\left(mod\, m\right)\Leftrightarrow \frac{a}{d}\equiv \frac{b}{d}\left(mod\frac{m}{d}\right)$. Là hệ quả của tính chất (vi).

viii) Nếu d là ước chung của a,b và $\left(d,m\right)=1$ thì $a\equiv b\left(mod\, m\right)\Leftrightarrow \frac{a}{d}\equiv \frac{b}{d}\left(mod\, m\right)$. Là hệ quả của tính chất (v).

ix) Nếu $a\equiv b\left(mod\, m_i\right)\ \left(i=1,2,...,n\right)$ và $m=\left[m_1,m_2,...,m_n\right]$ thì $a\equiv b\left(mod\, m\right)$.

x) Nếu $a\equiv b\left(mod\, m\right)$ và $d>0$ là ước của m thì $a\equiv b\left(mod\, d\right)$.

xi) Nếu $a\equiv b\left(mod\, m\right)$ và d là ước chung của a, m thì d là ước của b.

xii) Nếu $a\equiv b\left(mod\, m\right)$ thì $\left(a,m\right)=\left(b,m\right)$.

3.6.4. Hàm số Euler $\varphi(m)$: Với mỗi số m nguyên dương người ta gọi $\varphi(m)$ là số các số nguyên tố cùng nhau với m không vượt quá m.

Ví dụ: Các số nguyên dương không vượt quá 10 là: **1** 2 **3** 4 5 6 **7** 8 **9** 10. Vậy $\varphi(10)=4$.

Các số nguyên dương không vượt quá 7 là: **1 2 3 4 5 6** 7. Vậy $\varphi(7)=6$.

Nhận xét: Nếu p là số nguyên tố thì $\varphi(p)=p-1$.

Định lý: Nếu m_1 và m_2 là hai số nguyên dương và nguyên tố cùng nhau thì $\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$

*** Công thức tính hàm số Euler:**

i) Nếu $m=p^{\alpha}$ với p là một số nguyên tố và α là một số nguyên dương

thì: $\varphi(m)=\varphi\left(p^{\alpha}\right)=\left(1-\frac{1}{p}\right)p^{\alpha}$.

ii) Nếu $m>1$ và có dạng phân tích thành thừa số nguyên tố $m=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ thì:

$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right)$.

3.6.5. Hệ thặng dư thu gọn

*** Bổ đề:** Nếu $a, b, m > 0$ là các số nguyên và $(a,m) = 1$ thì khi *x* chạy qua hệ thặng dư đầy đủ modulo *m* thì $ax + b$ cũng chạy qua hệ thặng dư đầy đủ *m*.

*** Định nghĩa:** Xét một hệ thặng dư đầy đủ không âm modulo *m*: 0 1 2 3 … (*m*-2) (*m*-1) nếu trong đó có đúng $\varphi(m)$ phần tử nguyên tố cùng nhau với *m* thì các phần tử đó được gọi là hệ thặng dư thu gọn.

*** Bổ đề:** Nếu $a, m > 0$ là hai số nguyên thì khi *x* chạy qua hệ thặng dư thu gọn modulo *m* thì *ax* cũng chạy qua hệ thặng dư thu gọn modulo *m*.

3.6.6. Định lý Euler: Nếu *a* và *m>0* là hai số nguyên nguyên tố cùng nhau thì $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Ví dụ: Cho $a = 5 \;\; m = 6$. Ta có: $\varphi(m) = \varphi(6) = 2$

Suy ra $a^{\varphi(m)} \equiv 1 \pmod{m} \Leftrightarrow 5^2 = 25 \equiv 1 \pmod{6}$

3.6.7. Định lý Fermat: Nếu *a* là số nguyên và *p* là số nguyên tố thì: $a^{p-1} \equiv 1 \pmod{p}$ và $a^p \equiv a \pmod{p}$.

Ví dụ: $a = 4,\ p = 3 \Rightarrow 4^3 = 64 \equiv 4 \pmod{3} \equiv 1 \pmod{3}$.

3.7. Phương trình đồng dư bậc nhất một ẩn

3.7.1. Phương trình đồng dư: Phương trình đồng dư đại số bậc *n* có dạng: $a_0 x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n \equiv b \pmod{m}$ (1).

Trong đó: - $a_i \in \mathbb{Z}\ (i = \overline{0,n})$ là các hệ số nguyên.

- a_0 không là bội của *m*.
- $x \in \mathbb{Z}$ là ẩn số nguyên.

Ví dụ: $x^2 + x + 1 \equiv 1 \pmod{5}$; $9x \equiv 6 \pmod{15}$

3.7.2. Nghiệm của phương trình đồng dư: Nếu số nguyên x_0 là một nghiệm của phương trình đồng dư (1) thì mọi số nguyên *x* thuộc lớp $\overline{x}_0$ có dạng $x \equiv x_0 \pmod{m}$ cũng là nghiệm của (1). Người ta thường gọi lớp $\overline{x}_0$ là nghiệm của (1).

Ví dụ: Xét phương trình đồng dư: $x^2 \equiv 1 \pmod{5}$

Hệ thặng dư đầy đủ không âm bé nhất modulo 5 là: 0 1 2 3 4

Trong đó chỉ có $x_0 = 1$ và $x_0 = 4$ là thỏa phương trình đã cho

Vậy phương trình có 2 nghiệm: $x \equiv 1 \left(mod\, 5\right)$ và $x \equiv 4 \left(mod\, 5\right)$.

3.7.3. Phương trình đồng dư tương đương:

*** Định nghĩa:** Hai phương trình đồng dư được gọi là tương đương khi hai tập nghiệm của chúng bằng nhau.

Ví dụ: $x^2 \equiv 1 \left(mod\, 5\right) \Leftrightarrow x^2 + 2 \equiv 3 \left(mod\, 5\right)$.

*** Phép biến đổi tương đương:**

i) Nếu cộng hay trừ hai vế của phương trình với cùng một đa thức với hệ số nguyên thì ta được phương trình mới tương đương.

ii) Nếu thêm hay bớt ở hai vế của một phương trình đồng dư modulo *m* một bội của *m* thì ta được một phương trình mới tương đương.

iii) Nếu nhân các hệ số của phương trình đồng dư modulo *m* với cùng một số nguyên tố cùng nhau với *m* thì ta được phương trình mới tương đương.

Nếu chia các hệ số của phương trình đồng dư modulo *m* cho cùng một số là ước chung của các hệ số và nguyên tố cùng nhau với *m* thì ta được một phương trình mới tương đương.

iv) Nếu nhân các hệ số của phương trình đồng dư modulo *m* và *m* với cùng một số nguyên dương thì ta được một phương trình mới tương đương.

Nếu chia các hệ số của phương trình đồng dư modulo *m* và *m* với cùng một ước chung dương của chúng thì ta được một phương trình mới tương đương.

3.7.4. Phương trình đồng dư bậc nhất một ẩn:

*** Định nghĩa:** Phương trình đồng dư bậc nhất một ẩn có dạng: $ax \equiv b \left(mod\, m\right)$

*** Định lý về sự tồn tại nghiệm:** Phương trình $ax \equiv b \left(mod\, m\right)$ có nghiệm $\Leftrightarrow d = \left(a,m\right) | b$

Khi phương trình có nghiệm thì có đúng d nghiệm. Nếu x_0 là một giá trị thỏa phương trình thì d nghiệm đó được xác định bởi công thức: $\left[\begin{array}{l} x \equiv x_0 + 0.\dfrac{m}{d} \ (mod\, m) \\ x \equiv x_0 + 1.\dfrac{m}{d} \ (mod\, m) \\ ..... \\ x \equiv x_0 + (d-1)\dfrac{m}{d} \ (mod\, m) \end{array}\right.$

Ví dụ: Xét phương trình đồng dư $9x \equiv 6 \ (mod 15)$

Ta có: $d = (9,15) = 3 \mid 6$. Vậy phương trình có d = 3 nghiệm.

Hệ thặng dư đầy đủ không âm nhỏ nhất modulo 15 là:

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14

Một giá trị thỏa phương trình là $x_0 = 4$.

Phương trình có ba nghiệm là: $\left[\begin{array}{l} x \equiv 4 + 0.\dfrac{15}{3} \ (mod 15) \\ x \equiv 4 + 1.\dfrac{15}{3} \ (mod 15) \\ x \equiv 4 + 2.\dfrac{15}{3} \ (mod 15) \end{array}\right. \Leftrightarrow \left[\begin{array}{l} x \equiv 4 \ (mod 15) \\ x \equiv 9 \ (mod 15) \\ x \equiv 14 \ (mod 15) \end{array}\right.$.

*** Tìm một giá trị thỏa phương trình** $ax \equiv b \ (mod\, m)$

Khi phương trình có nghiệm thì $d = (a,m) \mid b$. Chia a,b,m cho d ta được phương trình tương đương: $\dfrac{a}{d}x \equiv \dfrac{b}{d} \left(mod \dfrac{m}{d} \right)$.

Vì $\dfrac{a}{d}$ và $\dfrac{m}{d}$ là nguyên tố cùng nhau nên có thể giả sử rằng phương trình đã cho thỏa $(a,m) = 1$. Vậy:

i) Nếu a là ước của b thì do $(a,m) = 1$, chia hai vế của phương trình cho a được một giá trị thỏa phương trình là: $x_0 = \dfrac{b}{a}$

Ví dụ: Một giá trị thỏa phương trình $4x \equiv 12 \pmod 7$ là: $x_0 = \frac{b}{a} = \frac{12}{4} = 3$

ii) Nếu a không là ước của b thì vì $(a,m) = 1 | b$ nên phương trình Diophante sau đây luôn có nghiệm: $ax \pm my = b \Leftrightarrow ax = b \pm my$ nghĩa là a và x đều là ước của $b \pm my$ nên một giá trị thỏa phương trình đồng dư là: $x_0 = \frac{b+ty}{a} \quad (t \in \mathbb{Z})$

Ví dụ: Một giá trị thỏa phương trình $3x \equiv 4 \pmod{11}$ là: $x_0 = \frac{b+ty}{a} = \frac{4+1.11}{3} = 5$

3.7.5. Mối quan hệ giữa phương trình đồng dư bậc nhất một ẩn và phương trình Diophante: Xét phương trình Diophante $ax + by = c$ (1) với giả thiết $b>0$.

i) Nếu (x_0, y_0) là một nghiệm của (1) thì: $ax_0 + by_0 = c \Rightarrow ax_0 = c - by_0$

$\Rightarrow ax_0 \equiv c \pmod b \Rightarrow x_0$ là nghiệm của phương trình đồng dư $ax \equiv c \pmod b$.

ii) Nếu x_0 là một nghiệm của phương trình đồng dư $ax \equiv c \pmod b$ thì: $ax_0 \equiv c \pmod b \Rightarrow \exists\, y_0$ sao cho $ax_0 = c - by_0 \Rightarrow \exists\, x_0, y_0$ sao cho $ax_0 + by_0 = c$

$\Rightarrow (x_0, y_0)$ là một nghiệm của (1).

3.8. Hệ phương trình đồng dư

3.8.1. Hệ phương trình đồng dư bậc nhất một ẩn: Ta chỉ xét hệ phương trình đồng dư bậc nhất một ẩn dạng như sau:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots\dots\dots\dots \\ x \equiv a_n \pmod{m_n} \end{cases} \quad (1)$$

*** Định lý 1:** Nếu hệ phương trình (1) có nghiệm thì đó là nghiệm duy nhất.

*** Định lý 2:** Xét hệ phương trình $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots\dots\dots\dots \\ x \equiv a_n \pmod{m_n} \end{cases}$. Nếu các modulo $m_1, m_2, \dots, m_n$ là nguyên tố sánh đôi thì hệ có nghiệm duy nhất x được xác định như sau:

- Tính $M = \left[m_1, m_2, ..., m_n\right] = m_1 m_2 ... m_n$

- Tính $M_i = \dfrac{M}{m_i}$ $\left(i = \overline{1,n}\right)$

- Giải các phương trình đồng dư: $M_i x \equiv a_i \left(mod\, m_i\right)$ $\left(i = \overline{1,n}\right)$ và tìm được các nghiệm $x \equiv N_i \left(mod\, m_i\right)$ $\left(i = \overline{1,n}\right)$

- Khi đó: $x \equiv M_1 N_1 + M_2 N_2 + ... + M_n N_n \left(mod\, M\right)$ là nghiệm của hệ.

Ví dụ: Giải hệ phương trình $\begin{cases} x \equiv 2 \left(mod\, 3\right) & (1) \\ x \equiv 3 \left(mod\, 5\right) & (2) \\ x \equiv 4 \left(mod\, 7\right) & (3) \end{cases}$

Vì các modulo nguyên tố sánh đôi nên áp dụng định lý trên:

- Tính $M = \left[3,5,7\right] = 3.5.7 = 105$

- Tính $\begin{cases} M_1 = \dfrac{M}{m_1} = \dfrac{105}{3} = 35 \\ M_2 = \dfrac{M}{m_2} = \dfrac{105}{5} = 21 \\ M_3 = \dfrac{M}{m_3} = \dfrac{105}{7} = 15 \end{cases}$

- Giải các phương trình đồng dư: $35x \equiv 2 \left(mod\, 3\right) \Leftrightarrow x \equiv 1 \left(mod\, 3\right)$

$21x \equiv 3 \left(mod\, 5\right) \Leftrightarrow x \equiv 3 \left(mod\, 5\right)$

$15x \equiv 4 \left(mod\, 7\right) \Leftrightarrow x \equiv 4 \left(mod\, 7\right)$

- Nghiệm của hệ: $x \equiv \left(35.1 + 21.3 + 15.4\right) \left(mod 105\right) \Leftrightarrow x \equiv 158 \left(mod 105\right)$ $\Leftrightarrow x \equiv 53 \left(mod 105\right)$.

3.8.2. Giải hệ phương trình đồng dư bằng phương pháp thế

*** Hệ 2 phương trình:** Giải hệ phương trình $\begin{cases} x \equiv 5 \left(mod\, 6\right) \\ x \equiv 8 \left(mod 15\right) \end{cases}$

$$\Leftrightarrow \begin{cases} x = 8 + 15t \quad (t \in \mathbb{Z}) \\ 8 + 15t \equiv 5 \pmod 6 \end{cases} \Leftrightarrow \begin{cases} x = 8 + 15t \quad (t \in \mathbb{Z}) \\ 15t \equiv -3 \pmod 6 \end{cases} \Leftrightarrow \begin{cases} x = 8 + 15t \quad (t \in \mathbb{Z}) \\ 3t + 12t \equiv -3 \pmod 6 \end{cases}$$

$$\Leftrightarrow \begin{cases} x = 8 + 15t \quad (t \in \mathbb{Z}) \\ 3t \equiv -3 \pmod 6 \end{cases} \text{ chia tất cả cho 3 } \Leftrightarrow \begin{cases} x = 8 + 15t \quad (t \in \mathbb{Z}) \\ t \equiv -1 \pmod 2 \end{cases}$$

$$\Leftrightarrow \begin{cases} x = 8 + 15t \quad (t \in \mathbb{Z}) \\ t = -1 + 2k \quad (k \in \mathbb{Z}) \end{cases} \Leftrightarrow x = 8 + 15(-1 + 2k) = -7 + 30k$$

$$\Leftrightarrow x \equiv -7 \pmod{30} \Leftrightarrow x \equiv 23 \pmod{30}$$

*** Hệ n>2 phương trình:** Trong trường hợp này người ta bắt đầu giải hệ 2 phương trình nào đó của hệ đã cho, rồi thay 2 phương trình này bằng nghiệm vừa tìm được. Khi đó ta được hệ có (n – 1) phương trình và lại tiếp tục giải như trước.

Ví dụ: Giải hệ phương trình $\begin{cases} x \equiv 4 \pmod 5 \ (1) \\ x \equiv 1 \pmod{12} \ (2) \\ x \equiv 7 \pmod{14} \ (3) \end{cases}$

Từ (1) $\Leftrightarrow x = 4 + 5k$. Thay vào (2) $\Leftrightarrow 4 + 5k \equiv 1 \pmod{12}$

$\Leftrightarrow 5k \equiv -3 \pmod{12} \Leftrightarrow 5k \equiv (-3 + 4.12) \pmod{12} \Leftrightarrow 5k \equiv 45 \pmod{12}$ (chia 2 vế cho 5, vì (5,12) = 1) $\Leftrightarrow k \equiv 9 \pmod{12} \Leftrightarrow k = 9 + 12m$

Thay vào (1) $\Leftrightarrow x = 4 + (9 + 12m).5 = 49 + 60m \Leftrightarrow x \equiv 49 \pmod{60}$

Ta xét hệ: $\begin{cases} x \equiv 49 \pmod{60} \ (*) \\ x \equiv 7 \pmod{14} \ (**) \end{cases}$. Từ $(**) \Leftrightarrow x = 7 + 14k$. Thay vào (*)

$\Leftrightarrow 7 + 14k \equiv 49 \pmod{60} \Leftrightarrow 7 + 14k \equiv 49 \pmod{60} \Leftrightarrow 14k \equiv 42 \pmod{60}$ (chia 2 vế cho 7, vì (7,60)=1) $\Leftrightarrow 2k \equiv 6 \pmod{60}$ (chia tất cả cho 2)

$\Leftrightarrow k \equiv 3 \pmod{30} \Leftrightarrow k = 3 + 30m$. Thay vào (**) ta được $x = 7 + (3 + 30m).14 = 49 + 420m \Leftrightarrow x \equiv 49 \pmod{420}$.

BÀI TẬP CHƯƠNG 3

1. Chứng minh rằng: $1997^{1999} - 1997^{1998}$ chia hết cho 4.

2. Chứng minh rằng trong hai số chẵn liên tiếp có một và chỉ một số chia hết cho 4.

3. Trong định lý về phép chia có dư $a = bq + r,\ 0 \le r < b$, cho biết a và q. Hãy tìm b và r trong các trường hợp sau:

a. $a = 133,\ q = 11$ **b.** $a = 350,\ q = 47$

4. Tìm các cặp số nguyên dương a và b thỏa mãn một trong các điều kiện sau:

a. $a + b = 432$ và $(a,b) = 36$. **b.** $ab = 8400$ và $(a,b) = 20$.

5. Chứng minh rằng $(a,b) = 1$ với $a = 21m + 4$ và $b = 14m + 3$.

6. Tìm BCNN $\left[2^n - 1,\ 2^n + 1\right]$ với $n \in \mathbb{N}$.

7. Tìm các cặp số tự nhiên a và b sao cho: $(a,b) = 15$ và $[a,b] = 2835$.

8. Tìm các cặp số tự nhiên a và b biết tổng bình phương của chúng bằng 468 và tổng ước chung lớn nhất và bội chung nhỏ nhất của chúng bằng 42.

9. Chứng minh rằng với m là một số nguyên lẻ, ta có:

a. $m^3 + 3m^2 - m - 3 \vdots 48$ **b.** $m^{12} - m^8 - m^4 + 1 \vdots 512$

10. Đặt $[a,b] = m$. Chứng minh rằng: $(a + b, m) = (a,b)$.

11. Chứng minh rằng với n là một số tự nhiên lớn hơn 1, các số dạng sau đây là những hợp số:

a. $n^4 + 4$. **b.** $n^4 + n^2 + 1$.

12. Tìm số nguyên tố p sao cho $p + 4$ và $p + 8$ cũng là những số nguyên tố.

13. Tìm số nguyên tố p sao cho $2p + 1$ là lập phương của một số tự nhiên.

14. Giải các phương trình Diophante sau:

a. $32x - 48y = 112$ **b.** $38x + 117y = 109$

c. $83x - 79y = 105$ **d.** $114x - 41y = 5$

15. Giải các hệ phương trình Diophante sau:

a. $\begin{cases} x + 2y + 4z = 7 \\ 2x - 5y - 7z = -7 \end{cases}$ **b.** $\begin{cases} 2x + 3y - 5z = 2 \\ 3x - 5y + 2z = 3 \end{cases}$ **c.** $\begin{cases} 5x - 5y + 3z = 6 \\ 3x - 2y + 3z = 5 \end{cases}$

16. Tìm các số nguyên mà khi chia chúng lần lượt cho 19 và 11 có dư tương ứng là 4 và 1.

17. Giải bài toán dân gian sau: "Mai em đi chợ phiên

Anh gửi một tiền

Mua cam cùng quýt

Không nhiều thì ít

Mua lấy một trăm

Cam ba đồng một

Quýt một đồng năm

Thanh yên tươi tốt

Năm đồng một trái"

Hỏi mỗi thứ mua được mấy trái?

Biết rằng một tiền bằng 60 đồng.

18. Tìm số dư trong các phép chia:

a. $1532^5 - 1$ chia cho 9. **b.** $51200^{2^{100}}$ chia cho 41.

19. Chứng minh rằng $\forall n \in \mathbb{N}^*$ ta có: $10^{6n} + 10^{3n} - 2 \equiv 0 \left(mod\ 111\right)$.

20. Hãy tìm nghiệm của đa thức $f\left(X\right) = \overline{4}X - \overline{2}$ trong vành $\mathbb{Z}_6$.

21. Tìm tất cả các số tự nhiên *m* biết rằng:

a. Dạng phân tích tiêu chuẩn $m = 3^\alpha 5^\beta 7^\gamma$ và $\varphi\left(m\right) = 3600$.

b. Dạng phân tích tiêu chuẩn $m = 2^\alpha 3^\beta p$ và $\varphi\left(m\right) = 180$.

c. Dạng phân tích tiêu chuẩn $m = 2^\alpha p$ và $\varphi\left(m\right) = 8$.

22. Chứng minh rằng: Nếu *a* nguyên tố với 7 thì $a^{12} - 1$ chia hết cho 7.

23. Chứng minh: $2^{70} + 3^{70} \vdots 13$.

24. Tìm số dư trong phép chia 6^{592} cho 11.

25. Chứng minh rằng với $n \geq 1$ ta có: $2^{3^{4n+1}} + 3 \vdots 11$.

26. Chứng minh rằng $\frac{2a + 11b}{19}$ là một số nguyên khi và chỉ khi $\frac{5a + 18b}{19}$ là một số nguyên, với $a,b \in \mathbb{Z}$.

27. Giải các phương trình đồng dư sau:

a. $3x \equiv 7 \pmod 8$ **b.** $7x \equiv 6 \pmod{13}$ **c.** $6x \equiv 27 \pmod{33}$

d. $10x \equiv 15 \pmod{65}$ **e.** $4x \equiv 1 \pmod 5$ **f.** $9x \equiv 42 \pmod{52}$

g. $137x \equiv 243 \pmod{481}$ **h.** $91x \equiv 84 \pmod{143}$

28. Giải các hệ phương trình đồng dư sau:

a. $\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{11} \end{cases}$ **b.** $\begin{cases} 5x \equiv 4 \pmod{11} \\ 11x \equiv 8 \pmod{13} \end{cases}$

c. $\begin{cases} 3x \equiv 5 \pmod 7 \\ 2x \equiv 3 \pmod 5 \\ 5x \equiv 1 \pmod 9 \end{cases}$ **d.** $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 4 \pmod 6 \\ x \equiv -5 \pmod{15} \end{cases}$ **e.** $\begin{cases} x \equiv 5 \pmod 6 \\ 7x \equiv 5 \pmod{12} \\ 17x \equiv 19 \pmod{30} \end{cases}$

TÀI LIỆU THAM KHẢO

[1] Nguyễn Viết Đông – Trần Ngọc Hội, *Đại số đại cương*, NXB ĐH Quốc gia TP HCM, 2005.

[2] Hoàng Xuân Sính, *Đại số đại cương*, NXB Giáo dục, 2007.

[3] Đậu Thế Cấp, *Cấu trúc đại số*, NXB Giáo dục, 2003.

[4] Bùi Huy Hiển, *Bài tập Đại số đại cương*, NXB Giáo dục, 2007.

[5] Nguyễn Tiến Quang, *Cơ sở lý thuyết trường và lý thuyết Galoa*, NXB ĐH Sư phạm, 2005.

[6] Trần Nam Dũng, *Số học*, Trường ĐH Khoa học tự nhiên TP HCM.

[7] Bùi Huy Hiển, *Bài tập đại số và số học tập 1*, NXB Giáo dục, 1985.

[8] Nguyễn Tiến Quang, *Bài tập Số học*, NXB ĐH Sư phạm, 2001.

[9] Jean – Marie Monier, *Đại số 1*, NXB Giáo dục.