Chương III
Cấu trúc đại số

I- Phép toán hai ngôi:

1.1. Định nghĩa phép toán hai ngôi

Cho X là một tập hợp. Ta gọi *một phép toán* trên X là một ánh xạ

$$T : X \times X \to X$$

từ tích Decartes $X \times X$ vào X.

Như vậy phép toán T đặt mỗi cặp phần tử (x, y) của tập $X \times X$ với một phần tử duy nhất T(x, y) của X. Phần tử T(x, y) gọi là *kết quả* của phép toán T. Thay cho cách viết T(x,y) ta sẽ viết là xTy và thay cho kí hiệu T ta còn viết các ký hiệu khác như +, . , * , o, ...

x + y được đọc là *x cộng y* và kết quả đó gọi là *tổng* của x và y.

x.y (hay xy) được đọc là *x nhân y* và kết quả đó gọi là *tích* của x và y.

Ví dụ 1: Với phép toán ở vế phải là "phép toán" mà ta đã quen biết thì

a) $T_1(x, y) = x + y$ là phép toán trên **N***, **N**, **Z, Q, R.**

b) $T_2(x, y) = x.y$ là phép toán trên **N***, **N**, **Z, Q, R.**

c) $T_3(x, y) = x^y$ là phép toán trên **N***.

Ví dụ 2: Kí hiệu X^X là tập các ánh xạ từ X vào chính nó. Khi đó phép hợp thành của hai ánh xạ f, g $\in X^X$.

$$T_4(f, g) = gof$$

là phép toán trên X^X.

Ví dụ 3: a) Phép trừ là phép toán trên **Z** nhưng không là phép toán trên **N**.

b) Phép chia là phép toán trên **Q*** nhưng không là phép toán trên **Q**, không là phép toán trên **Z***.

1.2. Phép toán cảm sinh.

Một bộ phận A của X gọi là ổn định (đối với phép toán * trong X) nếu và chỉ nếu với mọi x, y $\in$ A đều có x * y $\in$ A.

Nếu phép toán * ổn định trên A thì:

$$T : A \times A \to A,\ T(x, y) = x * y$$

cũng là một ánh xạ, do đó cũng là một phép toán trên A.

Phép toán này trên tập A được gọi là *phép toán cảm sinh* bởi phép toán * trên X.

Ví dụ 4: a) Phép cộng trên N ổn định trên tập con **Z**, các số nguyên chẵn. Do đó phép cộng trên **N** cảm sinh bởi phép cộng trên **Z**.

b) Phép trừ trên **Z** không ổn định trên tập con **N**. Do đó phép trừ trên **Z** không cảm sinh một phép toán trên **N**.

Ví dụ 5: Trên **R** xét phép toán

$$aob = a + b - ab.$$

Phép toán o ổn định trên tập S = [0, 1].

Thật vậy, aob = a + b - ab = a(1 - b) + b. Với mọi a, b $\in$ S:

$$0 \leq a(1 - b) + b \leq (1 - b) + b = 1.$$

Vậy aob $\in$ S với mọi a, b $\in$ S.

1.3. Các tính chất đặc biệt của phép toán

a. Tính chất kết hợp

Cho * là một phép toán trên tập X. Phép toán * gọi là có tính chất *kết hợp* nếu mọi x, y, z $\in$ X ta có:

$$(x * y) * z = z * (y * z).$$

Ví dụ 6: a) Phép +, . trên **N**, **Z**, **Q**, **R** là kết hợp.

b) Phép - trên **Z** không kết hợp. Chẳng hạn

$$(1- 2) - 3 \neq 1 - (2 - 3).$$

c) Phép luỹ thừa trên **N*** không kết hợp. Chẳng hạn

$$\neq$$

d) Phép hợp thành các ánh xạ trên X^X là kết hợp.

b. Tính chất giao hoán

Cho * là một phép toán trên tập X. Phép toán * gọi là có tính chất *giao hoán* nếu mọi x, y $\in$ X ta có

$$x * y = y * x.$$

Ví dụ 7: a) Phép +, . trên **N**, **Z**, **Q**, **R** là giao hoán.

b) Phép - trên **Z** không giao hoán. Chẳng hạn 1 - 2 $\neq$ 2- 1

c) Nếu X có nhiều hơn một phần tử thì phép toán hợp thành o trên X^X không giao hoán. Thật vậy, giả sử a, b $\in$ X, a $\neq$ b.

Gọi f và g $\in X^X$ là các ánh xạ xác định bởi

$$f(x) = a \text{ với mọi } x \in X$$

$$g(x) = b \text{ với mọi } x \in X.$$

Khi đó $gof(a) = b$, $fog(a) = a$. Vậy $gof \neq fog$.

c) Tính giản ước được: Cho X là một tập hợp, *là một phép toán trên X. Phần tử a bất kỳ thuộc X.

- Ta nói rằng a là chính quy (hoặc giản ước được) trái đối với * khi và chỉ khi $\forall(x, y) \in X^2$, nếu $a * x = a * y$ thì $x = y$.

- Ta nói rằng a là chính quy (hoặc giản ước được) phải đối với * khi và chỉ $\forall(x, y) \in X^2$: nếu $x * a = y * a$ thì $x = y$.

- Ta nói rằng a là chính quy (hoặc giản ước được) khi và chỉ khi a là chính quy trái và phải đối với *

1.4. Các phần tử đặc biệt của phép toán

a. Phần tử trung hoà

Cho * là một phép toán trên tập X. Phần tử $e' \in X$ ($e'' \in X$) gọi là *phần tử trung hoà bên trái (phải)* của phép toán * nếu với mọi $x \in X$

$$e' * x = x \quad (x * e'' = x).$$

Phần tử e gọi là *phần tử trung hoà* của phép toán * nếu e vừa là phần tử trung hoà bên trái vừa là phần tử trung hoà bên phải, tức là với mọi $x \in X$

$$e * x = x * e = x.$$

Định lí 1. *Cho * là một phép toán trên X. Khi đó nếu e' là phần tử trung hoà bên trái và e" là phần tử trung hoà bên phải của * thì e' = e".*

Chứng minh. Do e' là phần tử trung hoà bên trái nên

$$e' * e'' = e''$$

Do e" là phần tử trung hoà bên phải nên

$$e' * e'' = e'.$$

Từ hai đẳng thức trên suy ra $e' = e''$.

Hệ quả. *Phần tử trung hoà của một phép toán *, nếu có, là duy nhất.*

Ví dụ 8. a) 0 là phần tử trung hoà của phép cộng trên **N**, **Z**, **Q**, **R**.

b) 1 là phần tử trung hoà của phép nhân trên N*, **N**, **Z**, **Q**, **R**.

c) 0 là phần tử trung hoà bên phải của phép trừ trên **Z** nhưng không phải là phần tử trung hoà bên trái.

d) ánh xạ đồng nhất I_X là phần tử trung hoà của phép toán o trên X^X.

b. Phần tử đối xứng

Cho * là một phép toán trên X có phần tử trung hoà là e. Phần tử x' ∈ X (x" ∈ X) gọi là *phần tử đối xứng bên trái (phải)* của phần tử x ∈ X nếu:

$$x' * x = e \quad (x * x'' = e).$$

Phần tử x' gọi là *phần tử đối xứng* của x nếu x' vừa là phần tử đối xứng bên phải vừa là phần tử đối xứng bên trái của x, tức là

$$x' * x = x * x' = e.$$

Nếu x có phần tử đối xứng thì x gọi là phần tử khả đối xứng.

Định lí 2. *Nếu phép toán * trên X kết hợp, x' là phần tử đối xứng bên trái của x, x" là phần tử đối xứng bên phải của x thì x' = x".*

Chứng minh. Theo giả thiết ta có

$$\begin{aligned} x' &= x' * e \\ &= x' * (x * x'') \\ &= (x' * x) * x'' \\ &= e * x'' \\ &= x'' \end{aligned}$$

Vậy x' = x".

Hệ quả. *Nếu phép toán kết hợp thì phần tử đối xứng của một phần tử nếu có là duy nhất.*

Ví dụ 9. a) Trên **Z, Q, R** với phép cộng, mọi phần tử x có phần tử đối xứng là -x.

b) Trên **Q***, **R*** với phép nhân, mọi phần tử x có phần tử đối xứng là x^{-1}.

c) Trên X^X với phép toán o, phần tử f khả đối xứng khi và chỉ khi f song ánh. Phần tử đối xứng của f là ánh xạ ngược f^{-1} của f.

d) Nếu e là phần tử trung hoà của phép toán * trên X thì e khả đối xứng và phần tử đối xứng của e là chính nó.

**** Chú ý:***

Nếu phép toán trên X là phép công (+) thì phần tử trung hoà thường gọi là *phần tử không,* kí hiệu là 0_x hoặc 0; phần tử đối xứng của x gọi là *phần tử đối* của x, kí hiệu là - x.

Nếu phép toán trên X là phép nhân (.) thì phần tử trung hoà thường gọi là *phần tử đơn vị*, kí hiệu là 1_x hoặc 1; phần tử khả đối xứng gọi là *phần tử khả nghịch*, phần tử đối xứng của x gọi là *phần tử nghịch đảo* của x, kí hiệu là x^{-1}. Cũng như với phép nhân số thông thường dấu (.) thương được bỏ đi.

II. Nửa nhóm

2.1. Định nghĩa nửa nhóm.

Cho X là một tập và * là một phép toán trên X. Tập X cùng với phép toán * được kí hiệu là (X, *) hoặc X.

(X, *) gọi là *một nửa nhóm* nếu phép toán * có tính chất kết hợp

(X, *) gọi là *một vị nhóm* nếu phép toán * kết hợp và có phần tử trung hoà.

Nửa nhóm (vị nhóm) (X, *) gọi là *nửa nhóm (vị nhóm)* giao hoán nếu phép toán * là giao hoán.

Ví dụ 11. a) (**N***, +) là một nửa nhóm giao hoán, nhưng không là vị nhóm; (**N**, +) là một vị nhóm.

b) (**N***, .), (**N**, .), (**Z**, .) là các vị nhóm giao hoán.

c) (X^X, o) là vị nhóm. Nếu X có nhiều hơn một phần tử thì vị nhóm này không giao hoán.

Ví dụ 12. Cho X là một tập hợp. Trên X xét phép toán

$$x * y = x \text{ với mọi } x, y \in X$$

• (X, *) là một nửa nhóm. Thật vậy, mọi x, y, z ∈ X, ta có:

(x * y) * z = x * z = x; x * (y * z) = x * y = x nên (x*y) * z = x * (y * z). Vậy phép toán * kết hợp.

• Nếu X có hơn một phần tử thì nửa nhóm (X, *) không giao hoán. Thật vậy, giả sử x, y ∈ X, x ≠ y, ta có x * y = x, y * x = y, tức là x * y ≠ y * x.

• Mọi y ∈ X đều là phần tử trung hoà bên phải. Thật vậy, mọi x ∈ X ta có x * y = x nên y là phần tử trung hoà bên phải.

• Nếu X có hơn một phần tử thì trong X không có phần tử trung hoà bên trái. Thật vậy, với mọi y ∈ X, chọn x ∈ X, x ≠ y. Khi đó y * x = y ≠ x nên y không là phần tử trung hoà bên phải.

2.2. Tích các phần tử trong nửa nhóm.

Định lý 3: Giả sử $x_1, x_2..., x_n$ là n ($n \geq 3$) phần tử (phân biệt hoặc không) của một nửa nhóm X, thế thì:

$$x_1x_2... x_n = (x_1... x_i)(x_{i+1}... x_J)... (x_{m+1}... x_n)$$

Chứng minh:

Vì X là nửa nhóm nên mệnh đề đúng với n = 3. Giả sử mệnh đề đúng cho k nhân tử, ta chứng minh mệnh đề đúng với k + 1.

Thật vậy: $(x_1... x_i)(x_{i+1}... x_J)... (x_{m+1}... x_{k+1})$

$= [(x_1... x_i)...(x_{e+1}... x_m)] (x_{m+1}... x_{k+1})$

$= (x_1...x_m) [(x_{m+1}... x_{k+1})]$

$= (x_1.... x_m)[(x_{m+1}... x_k)x_{k+1}]$

$= [(x_1... x_m)(x_{m+1}... x_k)] x_{k+1}$

$= (x_1... x_k)x_{k+1} = x_1x_2... x_{k+1}$

Định lí 4. *Cho $x_1, x_2,..., x_n$ là các phần tử của một nửa nhóm giao hoán X. Khi đó.*

$$x_1x_2... x_n = x_{\sigma(1)} x_{\sigma(2)}... x_{\sigma(n)}$$

trong đó σ là một hoán vị bất kỳ của các số 1, 2,...,n.

Chứng minh. Hiển nhiên kết quả đúng với $n \leq 3$. Giả sử kết quả đúng với $n - 1 \geq 3$, ta sẽ chứng minh kết quả đúng với n. Với hoán vị σ bất kì, đặt $\sigma(n) = k$ ta có

$a_1a_2...a_n = (a_1... a_{k-1})\, a_k(a_{k+1}...a_n)$ (theo định lí 1).

$= (a_1...a_{k-1})\, (a_{k+1}...a_n)\, a_k$

$= (a_1...a_{k-1}a_{k+1}...a_n)\, a_k$

$= (a_{\sigma(1)}\, a_{\sigma(2)}...\, a_{\sigma(n-1)})\, a_{\sigma(n)}$ (do giả thiết quy nạp).

$= a_{\sigma(1)}\, a_{\sigma(2)}...\, a_{\sigma(n-1)}\, a_{\sigma(n)}$

Nhận xét : 1) Theo định lí 4, với mọi $a, b \in X$, X là nửa nhóm giao hoán và $n \in \mathbf{N}^*$ ta có

$$(ab)^n = a^nb^n$$

2) Nếu X là nửa nhóm cộng giao hoán thì quy tắc trong 1) trở thành $n(a + b) = na + nb$.

2.3. Tính chất của phần tử khả nghịch.

Định lí 5. *Cho X là một vị nhóm với phần tử đơn vị 1_X. Khi đó*

1) $1_X\ 1_X = 1_X$

2) $x \in X$ khả nghịch thì x^{-1} khả nghịch và $(x^{-1})^{-1} = x$.

3) $x, y \in X$ khả nghịch thì xy khả nghịch và $(xy)^{-1} = y^{-1}x^{-1}$.

Chứng minh.

1) Vì $1_X 1_X = 1_X$.

2) Vì $xx^{-1} = x^{-1}x = 1_X$

3) Vì $(y^{-1}x^{-1})(xy) = y^{-1}1_Xy = y^{-1}y = 1_X$.

$(xy)\ (y^{-1}x^{-1}) = x\ 1_Xx^{-1} = xx^{-1} = 1_X$.

Nhận xét 3. Nếu (X, +) là một vị nhóm với phần tử không 0_X thì các quy tắc trong định lí 5 trở thành

1) $-\ 0_X = 0_X$

2) $-\ (-x) = x$ nếu x có phần tử đối.

3) $-\ (x+y) = -y - x$ nếu x, y có phần tử đối.

ở đây ta sử dụng kí hiệu $x + (-y) = x-y$, đọc là x trừ y, nếu y có phần tử đối.

2.4. Luật giản ước

Phần tử a của nửa nhóm nhân X gọi là *thoả mãn luật giản ước* nếu mọi $x, y \in X$, ta có:

$$ax = ay \text{ suy ra } x = y$$

$$xa = ya \text{ suy ra } x = y$$

Định lí 6. *Nếu a là phần tử khả nghịch của một vị nhóm X thì a thoả mãn luật giản ước.*

Chứng minh. Với mọi $x, y \in X$ ta có

$$ax = ay \Rightarrow a^{-1}(ax) = a^{-1}(ay)$$

$$\Rightarrow (a^{-1}a)x = (a^{-1}a)y$$

$$\Rightarrow 1_Xx = 1_Xy$$

$$\Rightarrow x = y$$

Tương tự ta cũng có

$$xa = ya \Rightarrow x = y$$

2.5. Nửa nhóm con

a. ***Định nghĩa: -*** Giả sử (X, *) là một nửa nhóm tuỳ ý, A là tập con của X. Khi đó A được gọi là nửa nhóm con của X nếu A ổn định trên X.

- A là một nửa nhóm con của vị nhóm X chứa phần tử trung hoà của X thì A được gọi là vị nhóm con của X.

b. ***Tiêu chuẩn nửa nhóm con***: Tập con A của nửa nhóm (X, **)** được gọi là nửa nhóm con của X khi và chỉ khi với mọi x, y ∈ A thì x*y ∈ A

Ví dụ 13. Trong tập **Z** xét C là tập con các số chẵn và L là tập con các số lẻ. Khi đó C là vị nhóm con của vị nhóm (**Z**, +), L là vị nhóm con của vị nhóm (**Z**, .).

Ví dụ 14. Xét tập **R** với phép toán.

$$aob = a + b - ab$$

và tập con S = [0, 1]. Với mọi a, b, c, ∈ **R** ta có

$$\begin{aligned}(aob)oc &= (a + b - ab)oc \\ &= a + b - ab + c - c(a + b - ab) \\ &= a + b + c - ab - ac - bc + abc\end{aligned}$$

Tương tự ta tính được ao(boc) và có (aob)oc = ao(boc).

Vì phép toán o kết hợp nên (**R**, o) là một nửa nhóm.

Mọi a, b ∈ **R**, ta có aob = a+ b - ab = b + a - ba = boa nên phép toán o giao hoán.

Mọi a ∈ **R**, ta có ao0 = a + 0 - a0 = a, 0oa = a.

Do đó 0 là phần tử trung hoà của phép toán o.

Vậy (**R**, o) là một vị nhóm giao hoán. Theo ví dụ 5, S là nửa nhóm con của (**R**, o). Do 0 ∈ S nên S là vị nhóm con của (**R**, o).

Ví dụ 15. Nếu X là nửa nhóm thì X là một nửa nhóm con của X. Nếu X là một vị nhóm thì X và $\{1_X\}$ là vị nhóm con của X.

2.6 Đồng cấu nửa nhóm

Cho hai nửa nhóm (X, *) và (Y, o) . Một ánh xạ

$$f : X \rightarrow Y$$

gọi là một *đồng cấu nửa nhóm* nếu

$$f(x * y) = f(x)of(y) \quad \text{với mọi } x, y \in X.$$

Nếu X và Y đều là vị nhóm thì đồng cấu nửa nhóm gọi là *đồng cấu vị nhóm.*

Khi ánh xạ f là đơn ánh, toàn ánh, song ánh thì đồng cấu f tương ứng được gọi là *đơn cấu, toàn cấu, đẳng cấu.*

Ví dụ 16. Cho f : ($\mathbf{N}$, +) → ($\mathbf{N}$, .) $f(n) = 2^n$

Ta có $f(m+n) = 2^{m+n} = 2^m.2^n = f(m).f(n)$ với mọi m, n ∈ $\mathbf{N}$, nên f là đồng cấu. Dễ thấy f là đơn ánh nên f là đơn cấu từ ($\mathbf{N}$, +) vào ($\mathbf{N}$, .). Chú ý rằng f cũng là đơn cấu vị nhóm.

Ví dụ 17. a) Cho X là một nửa nhóm (vị nhóm). Khi đó ánh xạ đồng nhất

$I_X : X \to X, I_X(x) = x$ với mọi $x \in X$

là đẳng cấu nửa nhóm (vị nhóm).

b) Cho A là một nửa nhóm con của X. Khi đó ánh xạ

$j_A : A \to X, j_A(x) = x$ với mọi $x \in A$

là đơn cấu nửa nhóm, gọi là phép nhúng chính tắc A vào X.

c) Cho X là một nửa nhóm, Y là một vị nhóm. Khi đó ánh xạ

$f: X \to Y, f(x) = 1_Y$ với mọi $x \in X$

là đồng cấu nửa nhóm. Đặc biệt, nếu X là vị nhóm thì ánh xạ

$f : X \to X, f(x) = 1_X$ với mọi $x \in X$ là đồng cấu vị nhóm.

Định lí *7. Cho f : (X, *) → (Y, o) là một đồng cấu nửa nhóm. Khi đó*

1) A là nửa nhóm con của X thì f(A) là nửa nhóm con của Y.

2) B là nửa nhóm con của Y thì $f^{-1}(B)$ là nửa nhóm con của X.

Chứng minh.

1) Lấy tuỳ ý $y_1, y_2 \in f(A)$. Khi đó tồn tại $x_1, x_2 \in A$ sao cho $f(x_1) = y_1$, $f(x_2) = y_2$. Từ đó

$$y_1 o y_2 = f(x_1) \, o \, f(x_2) = f(x_1 * x_2)$$

Vì $x_1 * x_2 \in A$ nên $y_1 o\, y_2 \in f(A)$. Vậy f(A) là nửa nhóm con của Y.

2) Lấy tuỳ ý $x_1, x_2 \in f^{-1}(B)$. Khi đó $f(x_1), f(x_2) \in B$. Do B là nửa nhóm nên $f(x_1)$ o $f(x_2) = f(x_1 * x_2) \in B$. Suy ra $x_1 * x_2 \in f^{-1}(B)$.

Vậy $f^{-1}(B)$ là nửa nhóm con của X.

Ví dụ 18. Theo ví dụ 16 ta có $f(\mathbf{N}) = \{2^n \mid n \in \mathbf{N}\}$ là nửa nhóm con của nhóm ($\mathbf{N}$, .).

2.7. Nửa nhóm sắp thứ tự

a. Định nghĩa

Cho (X, *) là một nửa nhóm giao hoán và $\leq$ là một quan hệ thứ tự toàn phần trên X. Nếu mọi $x, y, z \in X$

$$x \leq y \Rightarrow x * z \leq y * z \qquad (1)$$

thì (X, *, $\leq$) gọi là *một nửa nhóm sắp thứ tự.*

Nếu $x \leq y$ và $x \neq y$ thì ta viết $x < y$. Nếu điều kiện (1) thay đổi điều kiện

$$x < y \Rightarrow x * z < y * z$$

thì nửa nhóm gọi là *nửa nhóm sắp thứ tự nghiêm ngặt.*

Trên **N** hoặc **Z** ta có quan hệ thứ tự thông thường:

$m \leq n$ nếu tồn tại $k \in$ **N** sao cho $m + k = n$.

Ta có $\leq$ là quan hệ thứ tự toàn phần trên **N** và trên **Z.**

Ví dụ 19. a) (**N, +,** $\leq$), ($\mathbf{N}^*$, ., $\leq$) là nửa nhóm sắp thứ tự nghiêm ngặt; (**N**, ., $\leq$) là nửa nhóm sắp thứ tự (không nghiêm ngặt).

b) (**Z**, +, $\leq$) là nửa nhóm sắp thứ tự nghiêm ngặt; (**Z**, ., $\leq$) không là nửa nhóm sắp thứ tự.

c) Mọi nửa nhóm con của một nửa nhóm sắp thứ tự là nửa nhóm sắp thứ tự.

b. Đồng cấu đơn điệu.

Cho (X, $\leq$) và (Y, $\leq$) là hai tập được sắp thứ tự. Một ánh xạ $f : X \rightarrow Y$ gọi là *đơn điệu* nếu mọi $x, y \in X$.

$$x \leq y \Rightarrow f(x) \leq f(y) \qquad (2)$$

Điều kiện (2) được thay bởi

$$x < y \Rightarrow f(x) < f(y)$$

thì f được gọi là *đơn điệu nghiêm ngặt.*

Một đồng cấu gọi là *đồng cấu đơn điệu* hay *đơn điệu nghiêm ngặt* nếu ánh xạ f có tính chất đó.

Ví dụ 20. $f : (\mathbf{N}, +) \rightarrow (\mathbf{N}, +)$, $f(n) = 2n$ với mọi $n \in$ **N** là đồng cấu đơn điệu nghiêm ngặt.

c. Nửa nhóm sắp thứ tự Acsimet

Cho nửa nhóm sắp thứ tự nghiêm ngặt (X, *, $\leq$). Phần tử $a \in X$ gọi là *phần tử dương* nếu $x < a * x$ với mọi $x \in X$.

Nửa nhóm sắp thứ tự nghiêm ngặt (X, *, $\leq$) gọi là *sắp thứ tự Archimedes* nếu mọi a, b $\in$ X, b là phần tử dương, đều tồn tại n $\in$ **N** sao cho

$$a < b * b * \ldots * b \text{ (n lần)}$$

Nếu X là nửa nhóm cộng thì điều kiện trên được viết lại là a < nb.

Ví dụ 21. a) Trong (**N**, +) và (**Z**, +) phần tử dương là mọi a $\in$ **N***. Trong (**N**, .) phần tử dương là a $\neq$ 0, a $\neq$ 1.

b) (**N**, +), (**Z**, +), (**N**,.) là nửa nhóm sắp thứ tự Archimedes.

Bài tập

1.1. Xét các tính chất và phần tử đặc biệt của các phép toán:

a) m * n = m + 2n trên **N**;

b) m * n = m.2^n trên **N**.

c) m * n = m + n^2 trên **Z**.

1.2. Trên **N*** đặt:

a) a * b = ƯCLN (a, b),

b) a □ b = BCNN [a, b].

* và □ có là phép toán trên $\mathbf{N}^*$ không? Nếu là phép toán hãy xét các tính chất và các phần tử đặc biệt.

1.3. Cho * là phép toán xác định trên R bởi: x*y = x + y - xy

a. Kiểm tra * có tính chất giao hoán, kết hợp, có phần tử trung hoà

b. Giải phương trình sau (với ẩn x $\in$ R)

1. 2 * x = 5
2. x * x = 1

1.4. Cho * là một phép toán trên X. Chứng minh rằng tập con

S = {x $\in$ X | (x*y) * z = x * (y * z) với mọi y, z $\in$ X}

ổn định với phép toán trên X và (S, *) là một nửa nhóm.

1.5. Chứng minh rằng các tập và các phép toán tương ứng sau đây là những nửa nhóm giao hoán

a) **R**, x * y = x + y + xy.

b) **N**, x $\oplus$ y = x + y + 2.

1.6. Trên **R*** xét phép toán $a * b = |a| b$. Chứng tỏ (**R***, *) là một nửa nhóm không gian hoán.

1.7. Phép toán * trên X gọi là luỹ đẳng nếu $x * x = x$ với mọi x.

Cho (X, *) là một nửa nhóm giao hoán luỹ đẳng. Trên X đặt

$$x \leq y \text{ nếu } x * y = y$$

Chứng minh $\leq$ là một quan hệ thứ tự trên X.

1.8. Kí hiệu **p**(X) là tập tất cả các tập con của X.

a) Chứng tỏ (**p**(x), $\cup$) là một vị nhóm giao hoán. Tìm các phần tử khả đối xứng của vị nhóm này.

b) Chứng tỏ (**p**(x), $\cap$) là một vị nhóm giao hoán. Tìm các phần tử khả đối xứng của vị nhóm này.

1.9. Trên tập S = [0, 1] đặt $a * b = \min\{a+b, 1\}$. Chứng tỏ (S,*) là một vị nhóm giao hoán. Tìm các phần tử khả đối xứng của vị nhóm này.

1.10. Cho X là một nửa nhóm và a, b $\in$ X là hai phần tử thoả mãn ab = ba. Chứng minh rằng $(ab)^n = a^n b^n$ với mọi n $\in$ **N***.

1.11. Trong nửa nhóm X^X các ánh xạ từ tập X vào tập X với phép toán hợp thành của ánh xạ, chứng minh rằng

a) f thoả mãn luật giản ước trái (tức $fog = foh \Rightarrow g = h$) $\Leftrightarrow$ f là đơn ánh.

b) f thoả mãn luật giản ước phải (tức $gof = hof \Rightarrow g = h$) $\Leftrightarrow$ f là toàn ánh.

c) f thoả mãn luật giản ước $\Leftrightarrow$ f là song ánh.

III - Nhóm

3.1. Định nghĩa nhóm

Tập hợp X được gọi là nhóm nếu trên X trang bị một phép toán hai ngôi thoả mãn các điều kiện sau:

i. Tính kết hợp: Mọi x, y, z $\in$ X: $(xy)z = x(yz)$

ii. Tồn tại phần tử trung lập: Với mọi x $\in$ X $\quad 1_X x = x 1_X = x$

iii. Mọi x $\in$ X tồn tại $x^{-1} \in X$ (gọi là phần tử nghịch đảo của x) sao cho

$$x^{-1}x = xx^{-1} = 1_X$$

Nhận xét 1. Trong một nhóm nhân có phép chia (:) được định nghĩa như sau: $x : y = xy^{-1}$

Trong một nhóm cộng có phép trừ (-) được định nghĩa như sau: $x - y = x + (-y)$.

2) Thông thường, phép cộng được sử dụng khi nhóm là giao hoán, còn phép nhân được sử dụng cho cả nhóm giao hoán và không giao hoán. Để đơn giản kí hiệu, các kết quả lý thuyết về sau ta thường chỉ xét với nhóm nhân. Tương tự như trong chương I, dễ dàng chuyển các kết quả này do nhóm cộng hay nhóm với phép toán tuỳ ý.

3) Theo định nghĩa thì một nửa nhóm có thể là tập rỗng, còn nhóm bao giờ cũng chứa ít nhất một phần tử, đó là phần tử trung hoà.

Ví dụ 1. a) ($\mathbf{Z}$, +), ($\mathbf{Q}$, +), ($\mathbf{R}$, +) là nhóm Abel. Phần tử không là 0, phần tử đối của x là -x.

b) ($\mathbf{Q}^*$, .). ($\mathbf{R}^*$, .) là nhóm Abel. Phần tử đơn vị là 1, phần tử nghịch đảo của x là .

c) Tập S_X các song ánh từ X lên chính nó với phép hợp thành ánh xạ (tích ánh xạ) là một nhóm. Phần tử đơn vị của S_X là I_X, phần tử nghịch đảo của f là f^{-1} (ánh xạ ngược của f). Nếu X có nhiều hơn hai phần tử thì S_X không giao hoán. Nếu X = {1,2, ..., n} thì S_X được kí hiệu là S_n và gọi là *nhóm các phép thế bậc n*.

Ví dụ 2. Với mỗi k ∈ $\mathbf{N}^*$ cố định ta định nghĩa quan hệ S trên $\mathbf{Z}$

x S y nếu x - y ⋮ k.

Dễ dàng kiểm tra S là quan hệ tương đương trên $\mathbf{Z}$. Kí hiệu tập thương của $\mathbf{Z}$ theo quan hệ S là $\mathbf{Z}_k$. Ta có

$\mathbf{Z}_k$ = {}.

trong đó = {x ∈ $\mathbf{Z}$| x - j ⋮ k}, gọi là lớp đồng dư với j theo môđun k.

Trên $\mathbf{Z}_k$ ta được định nghĩa phép cộng và nhân như sau

, r là số dư trong phép chia m + n cho k.

, s là số dư trong phép chia m.n cho k.

Dễ dàng kiểm tra rằng: ($\mathbf{Z}_k$, +) là một nhóm Abel, phần tử không là , phần tử đối của là ; ($\mathbf{Z}_k$, .) là một nhóm giao hoán với phần tử đơn vị là .

Ta kí hiệu = $\mathbf{Z}_k$ \ {}.

Có thể chứng minh rằng nếu k > 1 thì (, .) là nhóm khi và chỉ khi k là số nguyên tố. Chẳng hạn (, .) không là nhóm vì phần tử không có phần tử nghịch đảo (≠ với mọi j = 1, 2, 3).

Với mọi , ∈ $\mathbf{Z}_k$ ta còn có () = + .

3.2. Tính chất của các phần tử trong nhóm

Nếu a là phần tử của một nhóm X thì ta định nghĩa

$$a^0 = 1$$

$$a^n = aa...a \text{ (n lần) nếu } n > 0$$

$$a^n = (a^{-1})^{|n|} \qquad \text{nếu } n < 0$$

Theo nhận xét 1 và 2 chương I, suy ra:

1) Với mọi phần tử a của một nhóm X và p, q $\in$ **Z** ta có

$$a^p.a^q = a^{p+q}$$

$$a^{pq} = (a^p)^q$$

2) Với mọi phần tử a, b của một nhóm X và m $\in$ **Z** ta có

$$(a.b)^m = a^m b^m.$$

Theo định lí 5 chương I suy ra:

3) Với mọi phần tử a, b của một nhóm X ta có

$$(a^{-1})^{-1} = a,\ (ab)^{-1} = b^{-1}a^{-1}.$$

Theo định lí 6 chương I suy ra:

4) Mọi phần tử của một nhóm X đều thoả mãn luật giản ước, tức là mọi a, b, c $\in$ X: ab = ac $\Rightarrow$ b = c; ba = ca $\Rightarrow$ b = c.

3.3. Nhóm con

a. Định nghĩa nhóm con

Cho X là nhóm và tập con A của X ổn định với phép toán trên X. Nếu A cùng với phép toán cảm sinh là một nhóm thì A gọi là *nhóm con* của X.

Một cách tương đương, nhóm con của thể định nghĩa như sau:

Tập con A của nhóm X gọi là một nhóm con của X nếu thoả mãn ba điều kiện sau đây

1/ Mọi x, y $\in$ A đều có xy $\in$ A;

2/ $1_X \in$ A;

3/ Mọi x $\in$ A đầu có $x^{-1} \in$ A.

Thật vậy, nếu A thoả mãn ba điều kiện trên thì với phép toán cảm sinh A là một nhóm, do đó A là nhóm con của X. Ngược lại nếu A là nhóm con của X thì do A ổn định với phép toán trên X nếu có 1^0/. Gọi 1_A là phần tử đơn vị của nhóm A thì $1_A.1_X = 1_A.1_A$, vì 1_A thoả mãn luật giản ước nên $1_X = 1_A \in$ A, tức là có 2^0/. Với mọi X $\in$ A kí hiệu là nghịch đảo của x trong A. Khi đó $x.x^{-1} = x.$ (= 1_X), vì x thoả mãn luật giản ước nên $x^{-1} = x_A \in$ A, tức là cũng có 3^0/.

Nhận xét 2. 1) Nếu A là nhóm con của nhóm X thì đơn vị của A cũng chính là đơn vị của X; nghịch đảo của $x \in A$ trong A cũng chính là nghịch đảo của x trong X.

2) Nếu A là nhóm con của một vị nhóm X (tức là với phép toán cảm sinh A là một nhóm) thì điều nói trên có thể không đúng. Chẳng hạn: (**Z** , .) là một vị nhóm, $A = \{0\} \subset$ **Z** hiển nhiên là một nhóm con của (**Z** , .). Đơn vị của A là 0 khác đơn vị của (**Z** , .) là 1, nghịch đảo của 0 trong A là 0 còn 0 không khả nghịch trong (**Z** , .).

Ví dụ 3. a) Tập con các số nguyên chẵn là nhóm con của nhóm(**Z** , +).

b) là nhóm con của nhóm ($\mathbf{Q}^*$, .)

c) {-1, 1} là nhóm con của nhóm ($\mathbf{R}^*$, .)

d) Với mọi X, các tập $\{1_X\}$ và X là nhóm con của X. Các nhóm con này gọi là các *nhóm con tầm thường* của X.

b. Các tiêu chuẩn của nhóm con

Định lí 1. *Tập con A của nhóm X là một nhóm con của X khi và chỉ khi thoả mãn các điều kiện sau*

1) $A \neq \emptyset$

2) $x, y \in A \Rightarrow xy \in A$

3) $x \in A \Rightarrow x^{-1} \in A$

Chứng minh. Hiển nhiên 2°/ ⇒ 1) nên từ 1°/, 2°/, 3°/ suy ra 1), 2), 3).

Ngược lại, nếu có 1), 2), 3) thì do 1) tồn tại $x \in A$, do 2) tồn tại $x^{-1} \in A$ từ đó do 3) $1_X = x.x^{-1} \in A$, tức là có 2°/. Vậy từ 1), 2), 3) suy ra 1° /, 2° /, 3°/.

Định lí 2. *Tập con A của nhóm X là một nhóm con của X khi và chỉ khi thoả mãn các điều kiện sau*

1) $A \neq \emptyset$

2) $x, y \in A \Rightarrow xy^{-1} \in A$.

Chứng minh. Hiển nhiên 2°/ ⇒ 1). Với mọi $x, y \in A$ theo 3°/ $x, y^{-1} \in A$, theo *2*°/ $xy^{-1} \in A$, do đó có 2). Vậy từ 1 ° /, 2° /, 3° / suy ra 1), 2).

Ngược lại, nếu có 1), 2), 3) thì theo 1) tồn tại $x \in A$, theo 2) $1_X = x.x^{-1} \in A$, tức là 2°/. Với mọi $x \in A$ theo 2) $x^{-1} = 1_X x^{-1} \in A$, tức là có 3°/. Với mọi $x, y \in A$ ta có $x, y^{-1} \in A$, từ đó theo 2) $xy = x(y^{-1})^{-1} \in A$, tức là có 1°/. Vậy từ 1), 2) suy ra 1 ° /, 2° /, 3°/.

3.4. Đồng cấu nhóm

a. Định nghĩa.

Cho X và Y là hai nhóm, để đơn giản kí hiệu ta đều xét phép toán trên chúng là phép nhân, chú ý rằng phép toán trên X và Y nói chung là khác nhau.

Một ánh xạ $f : X \to Y$ gọi là *một đồng cấu nhóm* nếu mọi x, y $\in$ X đều có $f(x.y) = f(x).f(y)$.

b. Các tính chất.

Định lí 3. *Cho $f : X \to Y$ là một đồng cấu nhóm. Khi đó*

1) $f(1_X) = 1_Y$

2) Với mọi $x \in X$, $f(x^{-1}) = [f(x)]^{-1}$.

Chứng minh. a) Vì $1_X.1_X = 1_X$ nên $f(1_X).f(1_X) = f(1_X)$. Theo luật giản ước ta có $f(1_X) = 1_Y$.

b) Mọi $x \in X$, $xx^{-1} = 1_X$ nên $f(x)\ f(x^{-1}) = f(1_X) = 1_Y$.

Do phần tử khả nghịch của f(x) là duy nhất nên $f(x^{-1}) = [f(x)]^{-1}$

Khi ánh xạ $f: X \to Y$ là đơn ánh, toàn ánh, song ánh thì đồng cấu f được gọi là tương ứng là *đơn cấu, toàn cầu, đẳng cấu*.

Đồng cấu f từ nhóm X vào chính nó được gọi là *tự đẳng cấu*.

Ví dụ 3. a) **Z** là nhóm cộng các số nguyên, X là một nhóm nhân bất kì và $a \in X$ là một phần tử cố định. ánh xạ f: $\mathbf{Z} \to X$, $f(m) = a^m$ là một đồng cấu nhóm.

b) ánh xạ $f : (\mathbf{R}, +) \to (\mathbf{R}^*_+, .)$, $f(x) = 2^x$ là một đẳng cấu nhóm.

c) Cho X và Y là hai nhóm. ánh xạ $x \mapsto 1_Y$ với mọi $x \in X$ là một đồng cấu nhóm từ X vào Y. Đồng cấu này gọi là đồng cấu tầm thường từ X vào Y.

d) Cho X là một nhóm. ánh xạ đồng nhất $I_X : X \to Y$ là đẳng cấu nhóm.

e) Cho A là một nhóm con của nhóm X. ánh xạ $j_A : A \to X$, $j_A(x) = x$ là đơn cấu nhóm, gọi là phép nhúng chính tắc A vào X.

Định lí 4. *Cho $f : X \to Y$, $g : Y \to Z$ là các đồng cấu nhóm. Khi đó $h : X \to Z$, $h = gof$ là đồng cấu nhóm.*

Chứng minh. Với mọi x, y $\in$ X ta có

$h(x.y) = g(f(x.y)) = g(f(x).f(y))$

$= g(f(x)).\ g(f(x)) = h(x).h(y)$, do đó h là đồng cấu.

Định lí 5. *Nếu $f : X \to Y$ là một đẳng cấu thì ánh xạ ngược $f^{-1}: Y \to X$ cũng là đẳng cấu.*

Chứng minh. Vì f là song ánh nên ánh xạ ngược f^{-1} tồn tại và cũng là một song ánh. Với mọi x', y' ∈ Y tồn tại duy nhất x, y ∈ X để f(x) = x', f(y) = y' . Từ đó.

$$\begin{aligned} f^{-1}(x'y') &= f^{-1}(f(x)\, f(y)) \\ &= f^{-1}(f(xy)) \\ &= I_X(xy) \\ &= xy \\ &= f^{-1}(x')\, f^{-1}(y'). \end{aligned}$$

Vậy f^{-1}là đồng cấu và do đó là đẳng cấu.

Định lí 6. *Cho f: X → Y là một đồng cấu nhóm. Khi đó*

1) A là nhóm con của X thì f(A) là nhóm con của Y.

2) B là nhóm con của Y thì $f^{-1}(B)$ là nhóm con của X.

Chứng minh. 1) Lấy tuỳ ý $y_1, y_2 \in f(A)$. Khi đó tồn tại $x_1, x_2 \in A$ sao cho $f(x_1) = y_1$, $f(x_2) = y_2$. Từ đó

$$y_1y_2^{-1} = f(x_1)\,(f(x_2))^{-1} = f(x_1)\, f() = f(x_1).$$

Do $x_1 \in A$ nên $y_1 \in f(A)$. Mặt khác $1_Y = f(1_X) \in f(A)$ nên f(A) là nhóm con của Y.

2) Lấy tuỳ ý $x_1, x_2 \in f^{-1}(B)$. Khi đó $f(x_1), f(x_2) \in B$.

Do B là nửa nhóm nên $f(x_1).\,(f(x_2))^{-1} = f(x_1).f() = f(x_1.) \in B$. Từ đó suy ra $x_1 \in f^{-1}(B)$. Hiển nhiên $1_X \in f^{-1}(B)$ nên $f^{-1}(B)$ là nhóm con của X.

Cho f: X → Y là một đồng cấu nhóm. Theo định lí 12, f(X) là một nhóm con của Y, ta gọi nhóm con này là *ảnh* của f, kí hiệu là Imf; $f^{-1}(\{1_Y\}) = f^{-1}(1_Y)$ là một nhóm con của X, ta gọi nhóm con này là *hạt nhân* của f, kí hiệu là Ker f.

3.5. Nhóm sắp thứ tự

Cho (X,.) là một nhóm Abel và ≤ là một quan hệ thứ tự toàn phần trên X. Nếu (X,., ≤) là một nửa nhóm sắp thứ tự thì (X,., ≤) gọi là *một nhóm sắp thứ tự*, tức là mọi x, y, z ∈ X, x ≤ y đều có xz ≤ yz. Trong nhóm sắp thứ tự dễ thấy x < y kéo theo xz < yz. Do đó mọi nhóm sắp thứ tự đều là sắp thứ tự nghiêm ngặt.

Trong nhóm sắp thứ tự x < ax ⇔ 1_X < a, do đó phần tử a của nhóm sắp thứ tự X gọi là *dương* nếu 1_X < a.

Nhận xét 4. 1) Nếu (X, ., $\leq$) là nhóm sắp thứ tự thì mọi nhóm con của X cũng là nhóm sắp thứ tự.

2) Trong nhóm sắp thứ tự ta có

$a \leq b,\ c \leq d \Rightarrow ac \leq bd$

$a < b,\ c < d \Rightarrow ac < bd$

Định lí 7. *Cho (X, ., $\leq$) là một nhóm sắp thứ tự, P là tập các phần tử dương của nó khi đó*

1) $a, b \in P \Rightarrow ab \in P$;

2) Mọi $a \in X$ thì hoặc $a \in P$, hoặc $a^{-1} \in P$ hoặc $a = 1_X$;

3) $a, b \in X$, $a < b \Leftrightarrow ba^{-1} \in P$;

4) $1_X < a \Leftrightarrow a^{-1} < 1_X$.

Chứng minh.

1) Mọi $a, b \in P$, $1_X < a$, $1_X < b \Rightarrow b < ab$, $1_X < b \Rightarrow 1_X < ab$. Vậy $ab \in P$.

2) Hiển nhiên $1_X \notin P$. Nếu a và a^{-1} đồng thời thuộc P thì theo 1) $1_X = aa^{-1} \in P$, ta gặp mâu thuẫn. Nếu cả a và a^{-1} đều không thuộc P và $a \neq 1_X$ thì $a < 1_X$, $a^{-1} < 1_X$, $1_X < a \Rightarrow a = 1_X$, ta cũng gặp mâu thuẫn.

3) $a, b \in X$, $a < b \Leftrightarrow aa^{-1} < ba^{-1} \Leftrightarrow 1_X < ba^{-1} \Leftrightarrow ba^{-1} \in P$.

4) $1_X < a \Leftrightarrow 1_X a^{-1} < aa^{-1} \Leftrightarrow a^{-1} < 1_X$.

Định lí 8. *Cho (X,.) là một nhóm Abel, P là một tập con của X thoả mãn các điều kiện:*

1) $a, b \in P \Rightarrow ab \in P$;

2) Mỗi $a \in X$ thì hoặc $a \in P$, hoặc $a^{-1} \in P$ hoặc $a = 1_X$. Khi đó đặt $a \leq b$ nếu $a = b$ hoặc $ba^{-1} \in P$ thì $\leq$ là một quan hệ thứ tự trên X và (X,.) là một nhóm sắp thứ tự.

Chứng minh. Với mọi $a \in X$, $a \leq a$ nên $\leq$ có tính chất phản xạ. Nếu $a \leq b$, $b \leq a$ và $a \neq b$ thì $ba^{-1} \in P$, $ab^{-1} \in P \Rightarrow 1_X = (ba^{-1})(ab^{-1}) \in P$ ta gặp mâu thuẫn, do đó $a \leq b$, $b \leq a$ thì $a = b$, tức $\leq$ có tính phản xứng. Nếu $a \leq b$, $b \leq c$ và $a = b$ hoặc $b = c$ thì hiển nhiên $a \leq c$; nếu $a \neq b$ và $b \neq c$ thì $ba^{-1} \in P$ và $cb^{-1} \in P \Rightarrow ca^{-1} = (cb^{-1})(ba^{-1}) \in P \Rightarrow a \leq c$ vậy $\leq$ có tính chất bắc cầu.

Với mọi $a, b \in X$, nếu $ba^{-1} \in P$ thì $a < b$; nếu $(ba^{-1})^{-1} \in P$ thì $ab^{-1} \in P$ nên $b < a$; nếu $ba^{-1} = 1_X$ thì $a = b$. Do đó $\leq$ là quan hệ thứ tự toàn phần trên X.

Cuối cùng nếu $a, b, x \in X$, $a < b$ thì $ax < bx$ vì $(bx)(ax)^{-1} = ba^{-1} \in P$.

Vậy (X,.,$\leq$) là nhóm sắp thứ tự.

Nhận xét 5. Theo định lí 16, có thể định nghĩa: Nhóm Abel X gọi là sắp thứ tự nếu tồn tại một tập con P ≠ ⊘, gọi là tập dương, thoả mãn hai tính chất 1) và 2) của định lí 16.

Ví dụ 4. Tập con **N*** của nhóm (**Z**, +) có các tính chất 1) và 2). Do đó với mọi m, n ∈ **Z** ta định nghĩa m ≤ n nếu m = n hoặc n-m ∈ **N*** thì **Z** trở thành một nhóm sắp thứ tự. Thứ tự đó chính là thứ tự thông thương trên **Z**.

3.6. Đối xứng hoá

Trong toán học cao cấp ta phải giải quyết bài toán tổng quát sau:

Hãy mở rộng vị nhóm X để được một nhóm G sao cho X ⊂ G và tập G là "tiết kiệm" nhất.

Phương pháp giải quyết bài toán trên ta gọi là *phương pháp đối xứng hoá.*

a- Định nghĩa và ví dụ:

Cho * là phép toán hai ngôi xác định trong tập G. Phần tử a ∈ G gọi là chính quy phải (hoặc trái) nếu từ b*a = c*a (hoặc a*b = a*c) suy ra b = c; với mọi b, c ∈ G.

Nếu a đồng thời là chính quy phải và chính quy trái thì ta nói a là phần tử chính quy.

Ví dụ:

1) Trong tập số tự nhiên N, cùng với phép nhân, mỗi phần tử khác 0 đều là chính quy, 0 không phải là phần tử chính quy.

2) Trong tập số tự nhiên **N** cùng với phép cộng thông thường mỗi phần tử đều là chính quy.

3) Cho A = {0, 1, 2, 3} và * là phép toán trong A xác định:

a * b = a; với mọi a, b ∈ A.

Khi đó mọi phần tử trong A đều không phải là phần tử chính quy.

Nhận xét: Trong một nhóm, đẳng thức ab = ac (ba = ca) kéo theo b= c. Điều này do sự tồn tại của đối xứng a^{-1} của a. Nhưng trong một vị nhóm, mọi phần tử có đối xứng đều chính quy. Nhưng ngược lại không đúng (xét vị nhóm nhân **N** các số tự nhiên). Điều kiện chính quy chỉ là điều kiện cần để có đối xứng.

b. Định lý

Bây giờ ta xét vấn đề sau "nhúng" một vị nhóm giao hoán X vào một vị nhóm rộng hơn sao cho mọi phần tử chính quy của X có đối xứng trong .

Bổ đề: *Giả sử X là 1 nửa nhóm giao hoán có phần tử trung lập e và X* là bộ phận của X gồm các phần tử chính quy của X. Thế thì:*

1/ e $\in X^*$

2/ X^* là ổn định.

Chứng minh.

1) Vì ex = x, với mọi x $\in$ A nên từ ea = eb ta có a = b.

2) Giả sử a, b $\in$ X*. Từ abx = aby $\Rightarrow$ bx = by vì a là chính quy. Nhưng b cũng chính quy nên bx = by kéo theo x = y. Vậy ab là chính quy, tức là ab $\in$ X*.

Dưới đây ta trình bày phương pháp nhúng một vị nhóm vào một nhóm.

Giả sử (X, *) là một vị nhóm Aben, X* là tập hợp tất cả các phần tử chính quy của X. Trên tích Đề các X $\times$ X* ta định nghĩa quan hệ hai ngôi **R** như sau:

(a, b) ; (a', b') $\in$ X $\times$ X* ;

(a, b) R (a', b') $\Leftrightarrow$ a* b' = b * a'

Dễ dàng chỉ ra rằng R là quan hệ tương đương trên X $\times$ X*.

Đặt: = X $\times$ X* $/_R$ với hai phần tử x = () và y = ta định nghĩa: x o y = ().

ở đây () là lớp các phần tử tương đương với (a, b).

Định lý 9. *Giả sử (X, *) là 1 vị nhóm giao hoán mà mọi phần tử đều chính quy. Khi đó (, *) là nhóm giao hoán trong đó:*

i) = ($_X$, $_X$) là phần tử trung lập với e_X là phần tử trung hoà trong X.

ii) x' = () là phần tử đối xứng của x = () trong nhóm

iii) ánh xạ f : X $\rightarrow$

a () là đơn cấu từ vị nhóm X vào nhóm

(ta gọi là phép nhúng nhóm X vào).

Hệ quả. Nếu tất cả các phần tử của X đều là chính quy thì tất cả các phần tử của đều có đối xứng, đo đó là một nhóm.

c - ứng dụng

Ví dụ 1: Mở rộng tập N* để được Q^*_+.

Ta thấy (**N***, .) là vị nhóm Aben mà mọi phần tử đều chính quy. áp dụng quy trình ở định lý trên ta nhận được nhóm (*, .) . Kí hiệu * = Q^*_+. Mỗi phần tử của Q^*_+ gọi là một số hữu tỉ dương. Phép toán trong Q^*_+ được xây dựng trên đều gọi là phép nhân các số hữu tỉ dương. Kí hiệu: . (hoặc $\times$).

Mỗi phần tử của Q^*_+ được biểu diễn dưới dạng (). Như vậy tích của và sẽ là . Mỗi số nguyên dương N nhận được đồng nhất với số hữu tỉ

Ví dụ 2. Mở rộng tập **N** để được tập **Z**

Ta thấy rằng (N, +) là vị nhóm giao hoán mà mọi phần tử đều là chính quy. Theo định lí 9 thì là nhóm giao hoán, ta kí hiệu là **Z**. Mỗi phần tử **Z** gọi là số nguyên. Phép toán o trong Z, xây dựng như trên gọi là phép cộng các số nguyên. Kí hiệu: + (phép cộng các số tự nhiên). Mỗi phần tử của Z được biểu diễn dưới dạng hoặc (n, n + k) với n, k $\in$ N.

Đặt: k = và -k = (n, n + k).

Như vậy: Z = {... -3, -2, -1, 0, 1, 2, 3...}.

Bài tập

1. Chứng minh rằng **Z** với phép toán $m \oplus n = m + n - 1$ là một nhóm Abel.

2. Chứng minh rằng **R** \ với phép toán $x*y = x + y - 2xy$ là một nhóm Abel.

3. Chứng minh X = **R*** $\times$ **R** với phép toán (a, b) * (c,d) = (ac, bc + d) là một nhóm không giao hoán.

4. Chứng minh rằng G là một nhóm khi và chỉ khi

a) G là một nửa nhóm;

b) Với mọi a, b $\in$ G các phương trình ax = b, xa = b có nghiệm trong G.

5. Cho G là một nhóm Abel. Với mọi $n \geq 2$ kí hiệu

$$G_n = \{x \in G \mid x^n = 1_G\}.$$

Chứng minh rằng

a) G_n là nhóm con của G.

b) Nếu (m, n) = 1 thì $G_n \cap G_m = \{1_G\}$.

6. a) Chứng minh rằng một nửa nhóm G khác rỗng, hữu hạn là nhóm khi và chỉ khi mọi phần tử của nó đều thoả mãn luật giản ước.

b) Chứng minh rằng mọi tập con khác rỗng, hữu hạn, ổn định của nhóm G là một nhóm con của nhóm G.

7. Cho G là một nhóm có tính chất: $x^2 = 1_G$ với mọi x $\in$ G.

Chứng minh G là nhóm Abel.

8. Cho X là một nhóm. Tập con C(X) = {z $\in$ X | zx = xz với mọi x $\in$ X} gọi là *tâm* của nhóm X.

Chứng minh rằng C(X) là nhóm con của X.

9. Với mọi n $\in$ **N***, chứng minh (**Z**, +) $\cong$ (n**Z**,+).

10. Chứng minh rằng chỉ có một đồng cấu từ nhóm (**Q**, +) vào nhóm (**Z**, +) đó là đồng cấu tầm thường.

11. Chứng minh rằng không tồn tại một đẳng cấu từ (**R**, +) lên (**R***,.).

12. Chứng minh rằng ánh xạ $x \mapsto x^{-1}$ từ nhóm X vào chính nó là đẳng cấu nhóm khi và chỉ khi X là nhóm Abel.

13. Chứng minh rằng với phép toán m * n = m + n - 2 và thứ tự ≤ thông thường, (**Z**, *, ≤) là một nhóm sắp thứ tự

IV - Vành và trường

4.1. Vành

a. Định nghĩa và tính chất

Vành là một tập X cùng hai phép toán trên X, thường kí hiệu cộng và nhân thoả mãn các tính chất.

1) (X, +) là một nhóm Abel;

2) (X, .) là một nửa nhóm;

3) Phép nhân phân phối đối với phép cộng, tức là mọi x, y, z ∈ X ta có

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

Một cách tương đương, ta có thể định nghĩa (X, +, .) là một vành nếu nó thoả mãn các điều kiện sau:

(R_1) Mọi x, y, z ∈ X, (x + y) + z = x + (y + z).

(R_2) Mọi x, y ∈ X, x + y = y + x.

(R_3) Tồn tại 0_X ∈ X, mọi x ∈ X, x + 0_X = x.

(R_4) Mọi x ∈ X, tồn tại -x ∈ X, x +(-x) = 0_X.

(R_5) Mọi x, y, z ∈ X, (xy)z = x(yz).

(R_6) Mọi x, y, z ∈ X, x(y + z) = xy + xz, (y + z)x = yx + zx.

Nếu phép toán nhân của vành là giao hoán thì vành gọi là *vành giao hoán*. Nếu phép toán nhân có đơn vị thì vành gọi là *vành có đơn vị.*

Ví dụ 1. a) (**Z**, +, .), (**Q**, +, .), (**R**, +, .) là các vành giao hoán có đơn vị.

b) ($\mathbf{Z}_k$, +, .) là một vành giao hoán có đơn vị

c) Cho (X, +) là một nhóm Abel. Kí hiệu End(X) là tập các đồng cấu nhóm từ X vào X (gọi là các *tự đồng cấu*). Trên End(X) xác định phép + và . như sau

f + g được xác định bởi (f + g) (x) = f(x) + g(x) với mọi x ∈ X.

f.g được xác định bởi f.g(x) = f(g(x)) với mọi x ∈ X.

Dễ dàng kiểm tra (End(X), +, .) là một vành có đơn vị nhưng nói chung là không gian hoán. Ta gọi vành này là *vành các tự đồng cấu* của nhóm Abel X.

d) Cho (X, +) là một nhóm Abel. Trên X xác định phép toán nhân

$$x.y = 0_X \text{ với mọi } x, y \in X.$$

Dễ dàng kiểm tra (X, +, .) là một vành giao hoán, nói chung không có đơn vị. Ta gọi vành này là *vành không* của nhóm Abel.

Định lí 1. *Với mọi x, y, z của vành X ta có*

1) $x.0_X = 0_X.x = 0_X$

2) $(-x)y = x(-y) = -xy$

3) $(-x)(-y) = xy$

4) $x(y-z) = xy - xz;\quad (y - z)x = yx - zx.$

Chứng minh. 1) Ta có $x.0_X = x(0_X+ 0_X) = x0_X + x0_X$. Do đó $x.0_X = 0_X$. Tương tự cũng có $0_X.x = 0_X$.

2) Vì $xy + (-x)y = (x+(-x))y = 0_Xy = 0_X$ nên $(-x)y = -xy$.

Tương tự ta cũng có $x(-y) = -xy$.

3) Theo 2) ta có $(-x)(-y) = -x(-y) = -(-xy) = xy$.

4) Theo 2) ta có $x(y-z) = x(y +(-z)) = xy + x(-z) = xy - xz$.

Đẳng thức còn lại chứng minh tương tự.

Hệ quả. Với mọi $m \in \mathbf{Z}$ và mọi phần tử x, y của vành X ta có $m(xy) = (mx)y = x(my)$.

b. Vành con.

Cho X là một vành và tập con A của X ổn định đối với hai phép toán của vành X. Nếu với phép toán cảm sinh, (A, +, .) là một vành thì vành A gọi là *vành con* của X.

Ví dụ 2. a) Cho A là một vành. Khi đó $\{0_X\}$ và X là vành con của X. Các vành con này gọi là *vành con tầm thường* của X.

b)Vành **Z** các số nguyên là vành con của vành **Q** các số hữu tỉ.

c) Tập 2**Z** là vành con của vành **Z** các số nguyên.

Định lí 2. *Tập con A của một vành X là vành con của vành X khi và chỉ khi thoả mãn các điều kiện sau*

1) $A \neq \emptyset$

2) $x, y \in A \Rightarrow x + y \in A$ *và* $xy \in A$.

3) $x \in A \Rightarrow -x \in A$.

Chứng minh. Theo định lí **chương II**, (A,+) là nhóm Abel ⇔ $A \neq \emptyset$; x, y ∈ A thì $x + y \in A$, $-x \in A$; (A,.) là nửa nhóm ⇔ x, y ∈ A thì xy ∈ A. Nếu A ổn định với các phép toán thì trong A phép nhân phân phối với phép cộng. Như vậy A là vành con ⇔ A có các tính chất 1), 2), 3).

Định lí 3. *Tập con A của một vành X là vành con của vành X khi và chỉ khi thoả mãn các điều kiện sau*

1) $A \neq \emptyset$

2) $x, y \in A \Rightarrow x - y \in A$ *và* $xy \in A$.

Định lí 3 được chứng minh tương tự định lí 2 bằng cách áp dụng định lí 2, chương II.

Cho S là một tập con của vành X. Ta gọi vành con của X sinh bởi tập S là *vành con nhỏ nhất chứa S*, kí hiệu là [S]. Như vậy vành con [S] sinh bởi tập S có hai tính chất đặc trưng.

1) [S] là vành con;

2) Nếu A là vành con và $A \supset S$ thì $A \supset [S]$.

Định lí 4. *Với mọi tập con S của vành X đều tồn tại và duy nhất vành con [S] sinh bởi tập S.*

Chứng minh. Gọi **B** là họ tất cả các vành con của vành X chứa S. Vì x ∈ **B** nên **B** $\neq \emptyset$. Ta sẽ chứng minh

$$[S] = \bigcap_{B \in \mathbf{B}} B$$

tức là cần chứng minh $A = \bigcap_{B \in \mathbf{B}} B$ là vành con của X. Thật vậy, $0_X \in B$ với mọi B nên $0_X \in A$. Nếu x, y ∈ A thì x, y ∈ B với mọi B. Vì B là vành con nên $x- y \in B$ và $xy \in B$ với mọi B. Điều đó nghĩa là $x - y \in A$ và $xy \in A$. Theo định lí 3, A là vành con.

Ví dụ 3. Với mọi $k \in$ **N,** k**Z** là vành con của **Z** sinh bởi tập một phần tử {k}.

4.2. Đồng cấu vành

1. Định nghĩa và tính chất

Cho X và Y là hai vành. Một ánh xạ $f : X \to Y$ gọi là một *đồng cấu vành* nếu với mọi x, y ∈ ta có

$$f(x+y) = f(x) + f(y)$$
$$f(xy) = f(x)\, f(y)$$

Như vậy một đồng cấu vành $f : X \to Y$ là một đồng cấu từ nhóm cộng X vào nhóm cộng Y và là một đồng cấu từ nửa nhóm nhân X vào nửa nhóm nhân Y. Vì f là đồng cấu nhóm cộng nên

$$f(0_X) = 0_Y \ , \ f(-x) = -f(x)$$

Đồng cấu vành f được gọi tương ứng là *đơn cấu, toàn cấu, đồng cấu* nên ánh xạ f là đơn ánh, toàn ánh, song ánh.

Một đồng cấu từ vành X vào chính nó là một *tự đồng cầu.*

Ví dụ . a) Cho X là một vành có đơn vị 1_X. ánh xạ $f: \mathbf{Z} \to X$ xác định bởi $f(m) = m.1_X$ là một đồng cấu từ vành **Z** các số nguyên vào vành X. Thật vậy với mọi m, n ta có

$f(m+n) = (m+n)1_X = m1_X + n1_X = f(m) + f(n)$

$f(m.n) = (m.n)1_X = (m.1_X)(n.1_X) = f(m)f(n)$

b) Cho X là một vành. ánh xạ đồng nhất: $I_X : X \to X$ là đẳng cấu vành.

c) Cho A là một vành con của vành X. ánh xạ $j_A: A \to X$, $j_A(x) = x$ là đơn cấu vành, gọi là *phép nhúng chính tắc* A vào X.

d) Cho X và Y là hai vành. ánh xạ $f : X \to Y$, $f(x) = 0_Y$ với mọi $x \in Y$ là đồng cấu vành, gọi là *đồng cấu không*.

Tương tự như đồng cấu nhóm, ta có

Định lí 5. 1) Cho $f: X \to Y$, $g: Y \to Z$ là các đồng cấu vành. Khi đó $gof : X \to Z$ là đồng cấu vành.

2) Cho $f: X \to Y$ là đẳng cấu vành, khi đó ánh xạ ngược $f^{-1} : Y \to X$ cũng là đẳng cấu vành.

4.3. Vành sắp thứ tự

1. Định nghĩa và tính chất:

Cho (X, +, .) là một vành giao hoán và $\leq$ là một quan hệ thứ tự toàn phần trên X. Khi đó (X, +, ., $\leq$) gọi là *một vành sắp thứ tự* nếu mọi $x, y, z \in X$ ta có

1) $x \leq y \to x + z \leq y + z$

2) $0 \leq x, 0 \leq y \Rightarrow 0 \leq xy$.

Vành được gọi là *sắp thứ tự nghiêm ngặt* nếu 2) được thay bởi

2') $0 < x, 0 < y \Rightarrow 0 < xy$.

ở đây như thông lệ $x < y$, nghĩa là $x \leq y$ và $x \neq y$.

Ví dụ 4. Vành **Z** các số nguyên với quan hệ thứ tự thông thường là vành sắp thứ tự nghiêm ngặt.

Trong một vành sắp thứ tự nghiêm ngặt X ta gọi phần tử $a \in X$ là *phần tử dương* nếu $0 < a$.

Kí hiệu P là các tập phần tử dương của vành sắp thứ tự X.

Định lí 6. *Trong một vành sắp thứ tự nghiêm ngặt X ta có*

1) $a, b \in P \Rightarrow a + b \in P$, a.b thuộc P;

2) Mọi $a \in X$ thì hoặc $a \in P$, hoặc $-a \in P$ hoặc $a = 0_X$;

3) $a, b \in X$, $a < b \Leftrightarrow b - a \in P$;

4) $0 < a \Leftrightarrow -a < 0$.

***Định lí** 7:* *Một vành giao hoán X được sắp thứ tự nghiêm ngặt khi và chỉ khi trong X tồn tại một tập P có các tính chất 1), 2) và 3) của định lí 10. Quan hệ thứ tự để biến X thành một vành sắp thứ tự là quan hệ.*

$$a \leq b \text{ nếu } a = b \text{ hoặc } b - a \in P.$$

4.4. Trường

a. Định nghĩa và tính chất

Ta gọi *trường* là một vành giao hoán, có đơn vị, có nhiều hơn một phần tử và mọi phần tử khác đều khả nghịch.

Cho X là một trường, kí hiệu 0 là *phần tử không,* 1 là *phần tử đơn vị*.

Trước hết ta nhận xét rằng $0 \neq 1$. Thật vậy, trong x tồn tại $x \neq 0$, do đó tồn tại x^{-1}. Từ đó $x.x^{-1} \neq 0.x^{-1} \Rightarrow 1 \neq 0$.

Phần tử $x \neq 0$ của một vành X gọi là *ước của không* nếu tồn tại $y \in X$, $y \neq 0$ sao cho $xy = 0$.

Ta nhận xét rằng: *Mọi trường X đều không có ước của không.* Thật vậy, mọi $x \in X$, $x \neq 0$, nếu có $y \in X$ sao cho $xy = 0$ thì $x^{-1}xy = x^{-1}0 \Rightarrow y = 0$. Do đó x không là ước của không.

Đặt $X^* = X \setminus \{0\}$. Theo các nhận xét trên X* ổn định với phép toán nhân, $1 \in X^*$. Nếu $x \in X^*$ thì tồn tại $x^{-1} \in X^*$. Do đó (X*, .) là một nhóm Abel.

Như vậy, một cách tương đương, có thể định nghĩa: *(X, +, .) là một trường nếu*:

1) X cùng phép toán cộng là một nhóm Abel;

2) $X^* = X \setminus \{0\}$ cùng với phép nhân là một nhóm Abel;

3) Phép nhân phân phối với phép cộng.

Ví dụ 5. a) Với phép cộng và nhân thông thường (**Q**,+,.), (**R**, +, .) là các trường.

b) ($\mathbf{Z}_p$,+,.) với p nguyên tố là trường.

b. Trường con

a) Định nghĩa. Cho X là một trường. Tập con A của X gọi là một *trường con* của X nếu A ổn định đối với hai phép toán trong X và A cùng với hai phép toán cảm sinh tạo thành một trường.

Ví dụ 6. **Q** là trường con của trường con của trường số thực **R**. Từ các định lí 1 và 2 chương II, ta có hai định lí sau

b) Tiêu chuẩn trường con:

Định lí 8. *Tập con A của trường X có nhiều hơn một phần tử là trường con của trường X khi và chỉ khi thoả mãn các điều kiện*

1) $x, y \in A \Rightarrow x + y \in A, xy \in A$.

2) $x \in A \Rightarrow -x \in A$

3) $x \in A, x \neq 0 \Rightarrow x^{-1} \in A$.

Định lí 9. *Tập con A của trường X có nhiều hơn một phần tử là trường con của trường X khi và chỉ khi thoả mãn các điều kiện*

1) $x, y \in A \Rightarrow x - y \in A$.

2) $x, y \in A, y \neq 0 \Rightarrow xy^{-1} \in A$.

Ví dụ 7. **Q** = {a + b | a, b ∈ **Q**} là trường con của trường số thực **R**.

Thật vậy với mọi x = a + bvà y = c + d thuộc **Q** ta có

$$x - y = (a - c) + (b - d) \in \mathbf{Q}$$

Nếu thêm y ≠ 0 thì

xy^{-1} =

= ∈ **Q**

Vậy theo định lí 9, **Q** là trường con của trường **R**.

c. Miền nguyên

Ta gọi một vành giao hoán, có đơn vị, nhiều hơn một phần tử, không có ước của không là một *miền nguyên*.

Theo nhận xét trong 1. thì mọi trường đều là miền nguyên. Vành số nguyên Z là ví dụ về một miền nguyên nhưng không phải là trường.

Trong miền nguyên mọi phần tử khác không đều thoả mãn luật giản ước đối với phép nhân. Thật vậy, với mọi a ≠ 0:

ab = ac ⇒ a(b - c) = 0 ⇒ b - c = 0 ⇒ b = c.

d. Trường sắp thứ tự.

Cho X là một trường và một quan hệ thứ tự toàn phần $\leq$ trên X. Khi đó X được gọi là một *trường sắp thứ tự* nếu nó là một vành sắp thứ tự. Dễ dàng thấy rằng *mọi miền nguyên sắp thứ tự đều là sắp thứ tự nghiêm ngặt*.

Cho X là một trường (hoặc vành) sắp thứ tự. Với mọi $x \in X$ ta gọi giá trị tuyệt đối của x là phần tử $|x| \in X$ được xác định bởi

$$|x| = \begin{cases} x \text{ nếu } 0 < x \\ 0 \text{ nếu } x = 0 \\ -x \text{ nếu } x < 0 \end{cases}$$

Với mọi $x, y \in X$ ta có các tính chất sau:

1) $0 \leq |x|, |x| = 0 \Leftrightarrow x = 0$

2) $|xy| = |x||y|$

3) $|x + y| \leq |x| + |y|$

4) $\big||a| - |b|\big| \leq |a - b|$.

Bài tập

1. Cho X là một vành và $x \in X$. Chứng minh rằng với mọi $n \in \mathbf{N}^*$

$$(-x)n = \begin{cases} x^n \text{ nếu n chẵn} \\ -x^n \text{ nếu n lẻ} \end{cases}$$

2. Trong một vành đơn vị X chứng minh rằng nếu x khả nghịch thì -x cũng khả nghịch và $(-x)^{-1} = -x^{-1}$.

3. Trên tập **Z** x **Z** định nghĩa các phép toán

$(m, n) + (p, q) = (m + p, n+ q)$

$(m, n).(p, q) = (mp + mq, np + nq)$.

Chứng minh rằng*, với các phép* toán trên **Z** x **Z** là một vành giao hoán, có đơn vị.

4. Cho X là một vành, S là một tập hợp. Kí hiệu X^S là tập các ánh xạ từ S đến X. Với mọi f, g, $\in X^S$ ta định nghĩa f + g và f.g xác định bởi

$(f + g)(s) = f(s) + g(s)$, $(f.g)(s) = f(s).g(s)$

với mọi $s \in S$. Chứng minh rằng với các phép toán trên X^S là một vành. Nếu vành X giao hoán hay có đơn vị thì vành X^S cũng có tính chất đó.

5. Các tập sau đây, tập nào là vành con của vành **R**:

a) {m + | m, n ∈ **Z**} ?

b) {m + | m, n ∈ **Z**} ?

c) {m + + | m, n, p ∈ **Z**} ?

6. Cho X là một vành. Ta gọi tâm của X là tập

C(X) = {a ∈ X | ax = xa với mọi x ∈ X}.

Chứng minh rằng C(X) là vành con giao hoán của X.

7. Tìm tất cả các tự đồng cấu của vành số nguyên **Z**.

8. Kí hiệu **Q**() = {a +b | a, b ∈ **Q**}, n = 7; 11.

Chứng minh rằng

a) **Q**() và **Q**() là trường con của trường **R**.

b) ánh xạ f : **Q**() → **Q**()

a+b   a+ b

không phải là đẳng cấu trường.

c) Không tồn tại một đẳng cấu nào giữa **Q**() và **Q**().

9. Cho X là một vành. Trên tập **Z** × X xét các phép toán

(m, x) + (n, y) = (m + n, x + y)

(m, x) . (n, y) = (mn, nx + my + xy)

Chứng minh rằng:

a) (**Z** × X, +,.) là một vành có đơn vị.

b) ánh xạ h : X → **Z** × X, h(x) = (0, x) là đơn cấu vành. Do đó một vành bất kỳ đều có thể coi là vành con của một vành có đơn vị.

10. Trong một trường sắp thứ tự, chứng minh rằng

a) 0 < 1;

b) $0 < a \Leftrightarrow 0 < a^{-1}$.

c) $a < b < 0 \Leftrightarrow a^{-1} > b^{-1}$

d) a < b thì tồn tại vô số x để a < x < b.