Phần III
Cấu trúc đại số

Quan hệ
RELATIONS

Relations

1. Định nghĩa và tính chất
2. Biểu diễn quan hệ
3. Quan hệ tương đương. Đồng dư. Phép toán số học trên $\mathbf{Z}_n$
4. Quan hệ thứ tự. Hasse Diagram

1. Định nghĩa

Quan hệ hai ngôi từ tập A đến tập B là tập con của tích Descartess $R \subseteq A \times B$.

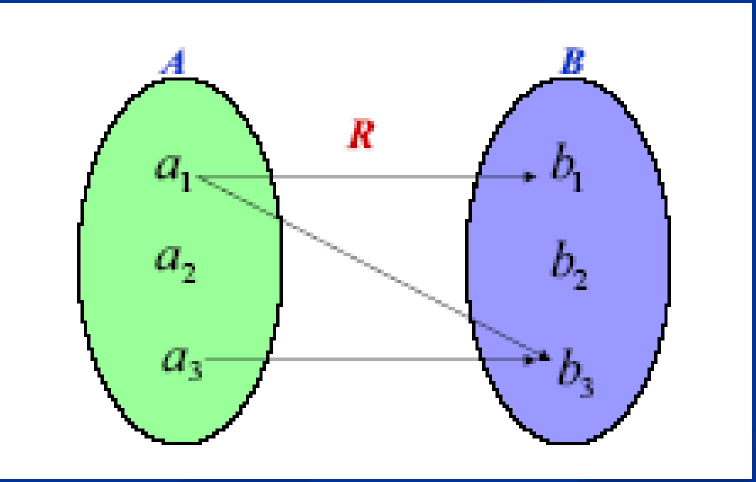
Chúng ta sẽ viết $a\ R\ b$ thay cho $(a, b) \in R$

Quan hệ từ A đến chính nó được gọi là quan hệ trên A

Chú ý: Thông thường tập $\mathscr{R}$ được cho bởi một thuộc tính P nào đó.

Tức là:

$\mathscr{R} = \{ (x,y) \in X^2 \mid (x,y)$ có tính chất P$\}$

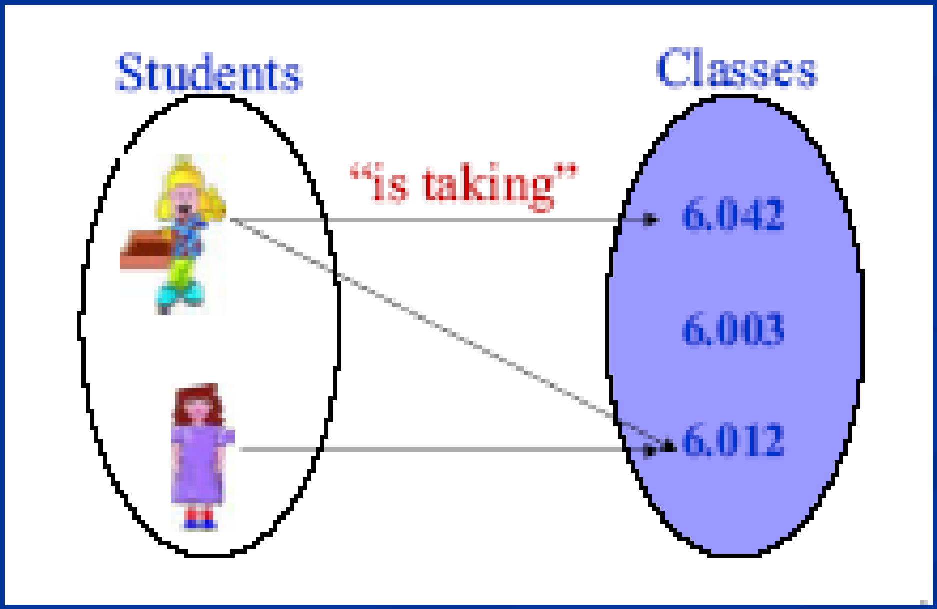


$$R = \{ (a_1, b_1), (a_1, b_3), (a_3, b_3) \}$$

1. Định nghĩa

Ví dụ. A = students; B = courses.

$R = \{(a, b) \mid \text{student } a \text{ is enrolled in class } b\}$



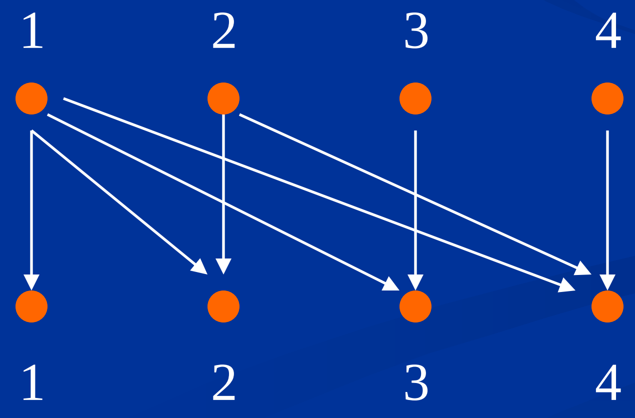
1. Định nghĩa

Ví dụ. Cho $A = \{1, 2, 3, 4\}$, và

$$R = \{(a, b) \mid a \text{ là ước của } b\}$$

Khi đó

$$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4,4)\}$$



1. Định nghĩa

Ví dụ.

- $\mathcal{R}_1$: $x\mathcal{R}_1y \Leftrightarrow x \vdots y$ (x chia hết cho y) $\forall x,y \in \mathbb{N}$
- $\mathcal{R}_2$: $x\mathcal{R}_2y \Leftrightarrow (x, y) = 1$ (x và y nguyên tố cùng nhau) $\forall x,y \in \mathbb{Z}$.
- Nếu A là tập người trên hành tinh và trên A cho một quan hệ $S = \{(x;y) \in A^2 | \text{ x là vợ của y}\}$. Khi đó, quan hệ S được diễn đạt là: S là quan hệ vợ chồng trên A hay xSy nếu như x là vợ của y.
- Cho p là số nguyên dương cố định. Ta xác định một quan hệ S trong $\mathbb{Z}$ như sau $S = \{ (x;y) \in \mathbb{Z}^2 \mid \text{nếu } (x - y) \text{ chia hết cho } p\}$. Quan hệ này chính là quan hệ đồng dư theo modulo p.

2. Tính chất

Với $\mathcal{R}$ là một quan hệ hai ngôi trên tập X, khi đó $\mathcal{R}$ được gọi là có:

- Tính phản xạ: nếu $a\mathcal{R}a$, $\forall a \in X$
- Tính đối xứng: nếu $a\mathcal{R}b$ thì $b\mathcal{R}a$ $\forall a,b \in X$
- Tính phản đối xứng: nếu $a\mathcal{R}b$ và $b\mathcal{R}a$ thì $a \equiv b$ $\forall a,b \in X$
- Tính bắc cầu: nếu $a\mathcal{R}b$ và $b\mathcal{R}c$ thì $a\mathcal{R}c$ $\forall a,b,c \in X$

2. Tính chất

Định nghĩa. Quan hệ R trên A được gọi là *phản xạ* nếu:

$$(a, a) \in R \text{ với mọi } a \in A$$

Ví dụ. Trên tập $A = \{1, 2, 3, 4\}$, quan hệ:

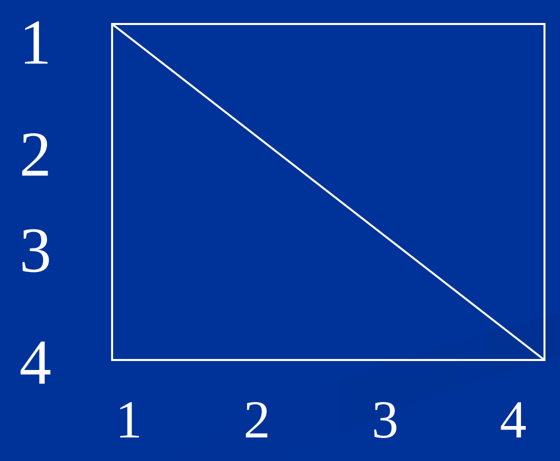
- $R_1 = \{(1,1), (1,2), (2,1), (2, 2), (3, 4), (4, 1), (4, 4)\}$ không phản xạ vì $(3, 3) \notin R_1$
- $R_2 = \{(1,1), (1,2), (1,4), (2, 2), (3, 3), (4, 1), (4, 4)\}$ phản xạ vì $(1,1), (2, 2), (3, 3), (4, 4) \in R_2$

- Quan hệ $\leq$ trên $\mathbb{Z}$ phản xạ vì $a \leq a$ với mọi $a \in \mathbb{Z}$
- Quan hệ $>$ trên $\mathbb{Z}$ không phản xạ vì $1 \not> 1$

- Quan hệ“ | ” (“ước số”) trên $\mathbb{Z}^+$ là phản xạ vì mọi số nguyên *a* là ước của chính nó .

Chú ý. Quan hệ *R* trên tập *A* là phản xạ iff nó chứa đường chéo của $A \times A$:

$$\Delta = \{(a, a); a \in A\}$$



2. Tính chất

Định nghĩa. Quan hệ R trên A được gọi là ***đối xứng*** nếu:

$$\forall a \in A\ \forall b \in A\ (a\ R\ b) \rightarrow (b\ R\ a)$$

Quan hệ R được gọi là ***phản xứng*** nếu

$$\forall a \in A\ \forall b \in A\ (a\ R\ b) \wedge (b\ R\ a) \rightarrow (a = b)$$

Ví dụ.

- Quan hệ $R_1 = \{(1,1), (1,2), (2,1)\}$ trên tập $A = \{1, 2, 3, 4\}$ là đối xứng
- Quan hệ $\leq$ trên $\mathbb{Z}$ không đối xứng.

Tuy nhiên nó phản xứng vì

$$(a \leq b) \wedge (b \leq a) \rightarrow (a = b)$$

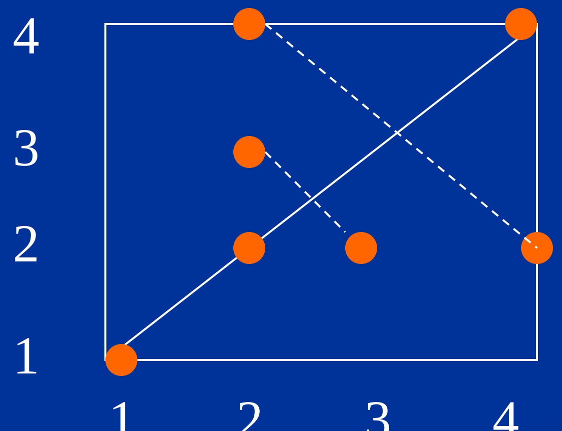
- Quan hệ“ | ” (“ước số”) trên $\mathbb{Z}^{+}$. không đối xứng

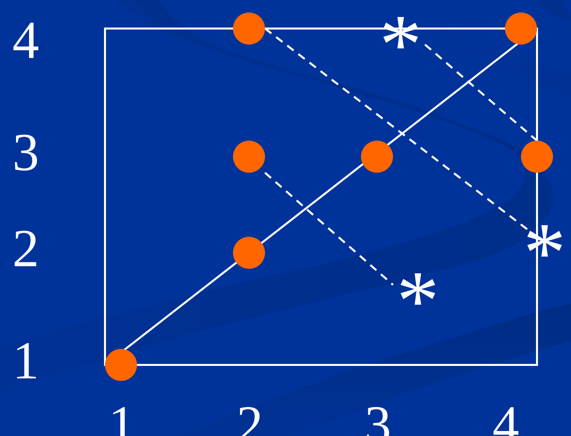
Tuy nhiên nó có tính phản xứng vì

$$(a \mid b) \wedge (b \mid a) \rightarrow (a = b)$$

Chú ý. Quan hê R trên A là đối xứng iff nó đối xứng nhau qua đường chéo Δ của $A \times A$.

Quan hệ R là phản xứng iff chỉ có các phần tử nằm trên đường chéo là đối xứng qua Δ của $A \times A$.





2. Tính chất

Định nghĩa. Quan hệ R trên A có tính ***bắc cầu(truyền)*** nếu

$$\forall a \in A\ \forall b \in A\ \forall c \in A\ (a\, R\, b) \wedge (b\, R\, c) \to (a\, R\, c)$$

Ví dụ.

Quan hệ $R = \{(1,1), (1,2), (2,1), (2,2), (1,3), (2,3)\}$ trên tập $A = \{1, 2, 3, 4\}$ có tính bắc cầu.

Quan hệ $\leq$ và "|" trên $\mathbb{Z}$ có tính bắc cầu

$$(a \leq b) \wedge (b \leq c) \to (a \leq c)$$

$$(a \mid b) \wedge (b \mid c) \to (a \mid c)$$

- Ví dụ:

Cho S = {sinh viên của lớp}, gọi

R = {(a,b): a có cùng họ với b}

Hỏi

R phản xạ? Yes

R đối xứng? Yes

R bắc cầu? Yes

Mọi sinh viên có cùng họ thuộc cùng một nhóm.

Quan hệ tương đương

Định nghĩa. Quan hệ R trên tập A được gọi là ***tương đương*** nếu nó có tính chất phản xạ, đối xứng và bắc cầu :

Ví dụ. Quan hệ R trên các chuỗi ký tự xác định bởi aRb iff a và b có cùng độ dài. Khi đó R là quan hệ tương đương.

Ví dụ. Cho R là quan hệ trên $\mathbb{R}$ sao cho aRb iff $a – b$ nguyên. Khi đó R là quan hệ tương đương

a-b nguyên, b –c nguyên

Suy ra : a-c = (a – b) + (b –c)

Lớp tương đương

Định nghĩa. Cho R là quan hệ tương đương trên A và phần tử $a \in A$. ***Lớp tương đương chứa a*** được ký hiệu bởi $[a]_R$ hoặc $[a]$ là tập

$$[a]_R = \{b \in A |\ b\ R\ a\}$$

Lớp tương đương

Ví dụ. Tìm các lớp tương đương modulo 8 chứa 0 và 1?

Giải. Lớp tương đương modulo 8 chứa 0 gồm tất cả các số nguyên *a* chia hết cho 8. Do đó

$$[0]_8 = \{ \ldots, -16, -8, 0, 8, 16, \ldots \}$$

Tương tự

$$[1]_8 = \{a \mid a \text{ chia 8 dư 1}\}$$

$$= \{ \ldots, -15, -7, 1, 9, 17, \ldots \}$$

Chú ý. Trong ví dụ cuối, các lớp tương đương $[0]_8$ và $[1]_8$ là rời nhau.

Tổng quát, chúng ta có

Theorem. Cho R là quan hệ tương đương trên tập A và $a, b \in A$, Khi đó

(i) $a\ R\ b$ iff $[a]_R = [b]_R$

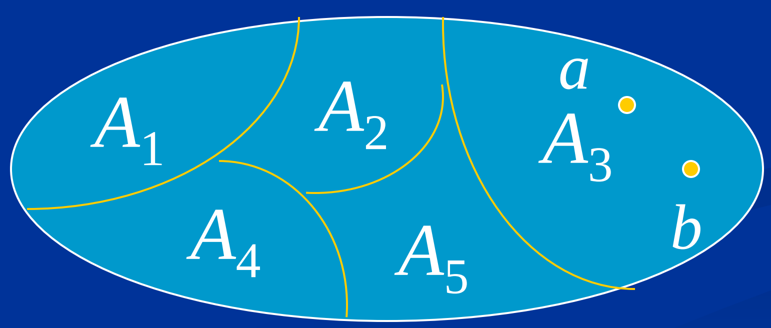
(ii) $[a]_R \neq [b]_R$ iff $[a]_R \cap [b]_R = \varnothing$

Chú ý. Các lớp tương đương theo một quan hệ tương đương trên A tạo nên một phân họach trên A, nghĩa là chúng chia tập A thành các tập con rời nhau.

Note. Cho $\{A_1, A_2, \ldots\}$ là phân họach A thành các tập con không rỗng, rời nhau . Khi đó có duy nhất quan hệ tương đương trên A sao cho mỗi A_i là một lớp tương đương.

Thật vậy với mỗi $a, b \in A$, ta đặt $a\ R\ b$ iff có tập con A_i sao cho $a, b \in A_i$.

Dễ dàng chứng minh rằng R là quan hệ tương đương trên A và $[a]_R = A_i$ iff $a \in A_i$



Example. Cho m là số nguyên dương, khi đó có m lớp đồng dư modulo m là $[0]_m$, $[1]_m$, …, $[m-1]_m$.

Chúng lập thành phân họach của $\mathbb{Z}$ thành các tập con rời nhau.

Chú ý rằng

$$[0]_m = [m]_m = [2m]_m = \dots$$

$$[1]_m = [m+1]_m = [2m+1]_m = \dots$$

……………………………………

$$[m-1]_m = [2m-1]_m = [3m-1]_m = \dots$$

Mỗi lớp tương đương này được gọi là ***số nguyên modulo m***

.Tập hợp các số nguyên modulo m được ký hiệu bởi $\mathbb{Z}_m$

$$\mathbb{Z}_m = \{[0]_m , [1]_m , \dots, [m-1]_m\}$$

Example. Cho m là số nguyên dương, ta định nghĩa hai phép tóan " + " và " × " trên $\mathbb{Z}_m$ như sau

$$[a]_m + [b]_m = [a + b]_m$$

$$[a]_m [b]_m = [a b]_m$$

Định lý. Các phép tóan nói trên được định nghĩa tốt, i.e. Nếu $a \equiv c \pmod{m}$ và $b \equiv d \pmod{m}$, thì

$$a + b \equiv c + d \pmod{m} \quad \text{và} \quad a b \equiv c d \pmod{m}$$

Example. $7 \equiv 2 \pmod 5$ và $11 \equiv 1 \pmod 5$ .Ta có

$$7 + 11 \equiv 2 + 1 = 3 \pmod 5$$

$$7 \times 11 \equiv 2 \times 1 = 2 \pmod 5$$

- Ví dụ: nhóm $Z_8 = \{[0], [1], \ldots, [7]\}$

i.e 16 thuộc lớp [0], 27 thuộc lớp [3]

$[1] + [3] = [4]$

9 thuộc lớp [1]

11 thuộc lớp [3]

$9 + 11 = 20$ thuộc lớp [4]

$[1] . [3] = [3]$

$9.11 = 99$ thuộc lớp [3]

- Ước của 0: a khác 0, b khác 0, a.b = 0

Ví dụ: nhóm $Z_8 = \{[0], [1], \ldots, [7]\}$

Là nhóm có **ước của 0**.

Chứng minh: [2].[4] = [2.4] = [8] =[0]

$Z_{29} = \{[0], [1], \ldots, [28]\}$

A = [1]	+ = [26]
B = [2]	- = [27]
Z = [25]	* = [28]

Note. Các phép tóan " + " và " × " trên $\mathbb{Z}_m$ có các tính chất như các phép tóan trên $\mathbb{Z}$

$$[a]_m + [b]_m = [b]_m + [a]_m$$

$$[a]_m + ([b]_m + [c]_m) = ([a]_m + [b]_m) + [c]_m$$

$$[a]_m + [0]_m = [a]_m$$

$$[a]_m + [m - a]_m = [0]_m \ ,$$

Ta viết $$-[a]_m = [m - a]_m$$

$$[a]_m [b]_m = [b]_m [a]_m$$

$$[a]_m ([b]_m [c]_m) = ([a]_m [b]_m) [c]_m$$

$$[a]_m [1]_m = [a]_m$$

$$[a]_m ([b]_m + [c]_m) = [a]_m [b]_m + [a]_m [c]_m$$

Example. " Phương trình bậc nhất" trên $\mathbb{Z}_m$

$$[x]_m + [a]_m = [b]_m$$

với $[a]_m$ và $[b]_m$ cho trước, có nghiệm duy nhất:

$$[x]_m = [b\,]_m - [a]_m = [b - a]_m$$

Cho $m = 26$,phương trình $[x]_{26} + [3]_{26} = [b]_{26}$ có nghiệm duy nhất với mọi $[b]_{26}$ trong $\mathbb{Z}_{26}$.

Do đó $[x]_{26} \to [x]_{26} + [3]_{26}$ là song ánh từ $\mathbb{Z}_{26}$ vào chính nó .

Sử dụng song ánh này chúng ta thu được mã hóa Caesar:

Mỗi chữ cái tiếng Anh được thay bởi một phần tử của $\mathbb{Z}_{26}$: $A \to [0]_{26}$, $B \to [1]_{26}$, …, $Z \to [25]_{26}$

Ta sẽ viết đơn giản: $A \to 0$, $B \to 1$, …, $Z \to 25$

Mỗi chữ cái sẽ được mã hóa bằng cách cộng thêm 3 .
Chẳng hạn A *được mã hóa* bởi chữ cái tương ứng với $[0]_{26} + [3]_{26} = [3]_{26}$, nghĩa là bởi D.

Tương tự B *được mã hóa* bởi chữ cái tương ứng với $[1]_{26} + [3]_{26} = [4]_{26}$, nghĩa là bởi E, … cuối cùng Z *được mã hóa* bởi chữ cái tương ứng với $[25]_{26} + [3]_{26} = [2]_{26}$ nghĩa là bởi C.

Bức thư "MEET YOU IN THE PARK" được mã như sau

M E E T	Y O U	I N	T H E	P A R K
12 4 4 19	24 14 20	8 13	19 7 4	15 0 17 10
15 7 7 22	1 17 23	11 16	22 10 7	18 3 20 13
P H H W	B R X	L Q	W K H	S D U N

Để giải mã, ta dùng ánh xạ ngược:

$$[x]_{26} \to [x]_{26} - [3]_{26} = [x-3]_{26}$$

P H H W tương ứng với 15 7 7 22

Lấy ảnh qua ánh xạ ngược: 12 4 4 19

Ta thu được chữ đã được mã là M E E T

Mã hóa như trên còn quá đơn giản,dễ dàng bị bẻ khóa. Chúng ta có thể tổng quát mã Caesar bằng cách sử dụng ánh xạ $f : [x]_{26} \to [ax+b]_{26}$ trong đó a và b là các hằng số được chọn sao cho f là song ánh

Trước hết chúng ta chọn a khả nghịch trong $\mathbb{Z}_{26}$ i.e. tồn tại a' trong $\mathbb{Z}_{26}$ sao cho

$$[a]_{26}\,[a']_{26} = [a\,a']_{26} = [1]_{26}$$

Chúng ta viết $[a']_{26} = [a]_{26}^{-1}$ nếu tồn tại .
Nghiệm của phương trình

$$[a]_{26}\,[x]_{26} = [c]_{26}$$

là $\qquad [x]_{26} = [a]_{26}^{-1}\,[c]_{26} = [a'c]_{26}$

Chúng ta cũng nói nghiệm của phương trình

$$a\,x \equiv c \pmod{26}$$

là $\qquad x \equiv a'c \pmod{26}$

Ánh xạ ngược của f xác định bởi

$$[x]_{26} \to [a'(x - b)]_{26}$$

Example. Cho $a = 7$ và $b = 3$, khi đó nghịch đảo của $[7]_{26}$ là $[15]_{26}$ vì $[7]_{26}[15]_{26} = [105]_{26} = [1]_{26}$

Bây giờ M được mã hóa như sau

$$[12]_{26} \to [7 \cdot 12 + 3]_{26} = [87]_{26} = [9]_{26}$$

nghĩa là được mã hóa bởi I. Ngược lại I được giải mã như sau

$$[9]_{26} \to [15 \cdot (9 - 3)]_{26} = [90]_{26} = [12]_{26}$$

nghĩa là tương ứng với M.

Quan hệ thứ tự

Định nghĩa. Quan hệ R trên tập A là ***quan hệ thứ tự(thứ tự)*** nếu nó có tính chất phản xạ, phản xứng và bắc cầu.

Người ta thường ký hiệu quan hệ thứ tự bởi $\prec$

Cặp $(A, \prec)$ được gọi là ***tập sắp thứ tự*** hay ***poset***

Phản xạ: $a \prec a$

Phản đối xứng: $(a \prec b) \land (b \prec a) \to (a = b)$

Bắc cầu: $(a \prec b) \land (b \prec c) \to (a \prec c)$

Quan hệ thứ tự

Ví dụ:

Trong $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, quan hệ "$x \le y$" là một quan hệ thứ tự.

Nhưng quan hệ nhỏ hơn thực sự "$x < y$" không phải là quan hệ thứ tự vì vi phạm tính phản xạ.

Trong $\mathbb{N}$, quan hệ "$x \vdots y$" là một quan hệ thứ tự.

Trong $\mathcal{P}(X)$ - tập tất cả các tập con của X, quan hệ "$A \subset B$" là một quan hệ có thứ tự

Quan hệ thứ tự toàn phần

Quan hệ thứ tự "$\leq$" trên X được gọi là quan hệ thứ tự toàn phần nếu hai phần tử bất kỳ của X đều so sánh được với nhau. Nghĩa là với mọi x, y $\in$ X thì $x \leq y$ hoặc $y \leq x$.

Quan hệ thứ tự không toàn phần được gọi là quan hệ thứ tự bộ phận.

Tập X với quan hệ thứ tự "$\leq$" được gọi là tập được sắp.

Nếu quan hệ thứ tự "$\leq$" là toàn phần thì X được gọi là tập được sắp toàn phần hay sắp tuyến tính.

Quan hệ thứ tự toàn phần

Ví dụ:

Các tập: ($\mathbb{N}$,$\leq$), ($\mathbb{Z}$, $\leq$), ($\mathbb{Q}$, $\leq$), ($\mathbb{R}$, $\leq$) được sắp toàn phần

Các tập: ($\mathbb{N}$, $\vdots$) và ((X), $\subset$) được sắp bộ phận (nếu X có nhiều hơn 1 phần tử)

Thứ tự tự điển

Ex. Trên tập các chuỗi bit có độ dài n ta có thể định nghĩa thứ tự như sau:

$$a_1a_2\ldots a_n \le b_1b_2\ldots b_n$$

iff $a_i \le b_i$, $\forall\ i$.

Với thứ tự này thì các chuỗi 0110 và 1000 là không so sánh được với nhau .Chúng ta không thể nói chuỗi nào lớn hơn.

Trong tin học chúng ta thường sử dụng thứ tự tòan phần trên các chuỗi bit .

Đó là thứ tự tự điển.

Thứ tự tự điển

Cho (A, ≤) và (B, ≤'), (C, ≤') là hai tập sắp thứ tự tòan phần. Ta định nghĩa thứ tự trên $A \times B \times C$ như sau : $(a_1, b_1, c_1) \prec (a_2, b_2, c_2)$ iff

$a_1 < a_2$ or $(a_1 = a_2$ and $b_1 \leq b_2)$ or $(a_1 = a_2$ and $b_1 = b_2$ and $c_1 \leq c_2$

Dễ dàng thấy rằng đây là thứ tự tòan phần trên $A \times B \times C$ Ta gọi nó là **thứ tự tự điển .**

Chú ý rằng nếu A và B *và* C được sắp tốt bởi ≤ và ≤ ' ,tương ứng thì $A \times B \times C$ cũng được sắp tốt bởi thứ tự

Chúng ta cũng có thể mở rộng định nghĩa trên cho tích Descartess của hữu hạn tập sắp thứ tự tòan phần.