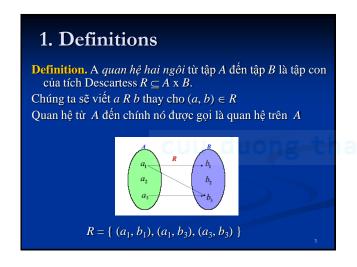
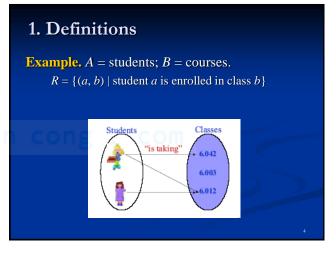
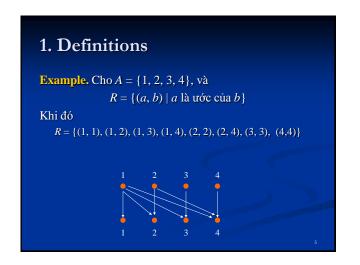


Relations 1. Định nghĩa và tính chất 2. Biểu diễn quan hệ 3. Quan hệ tương đương. Đồng dư. Phép toán số học trên \mathbb{Z}_n 4. Quan hệ thứ tự. Hasse Diagram

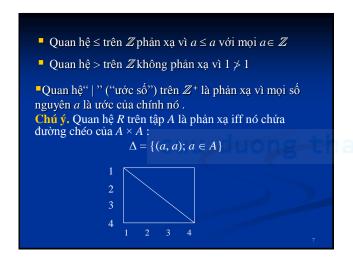
cuu duong than cong . com

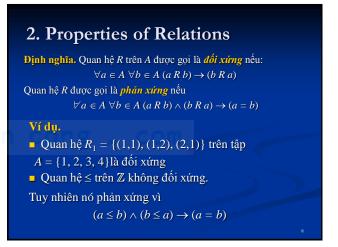


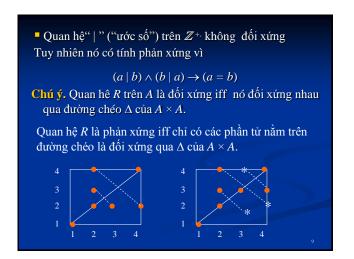


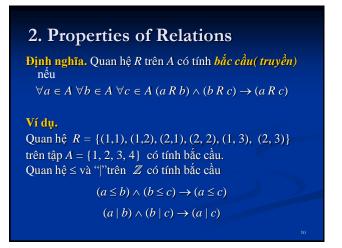


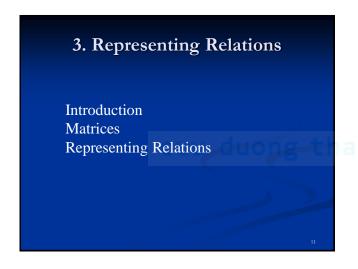


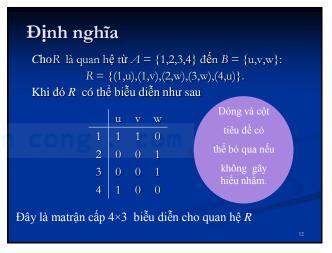


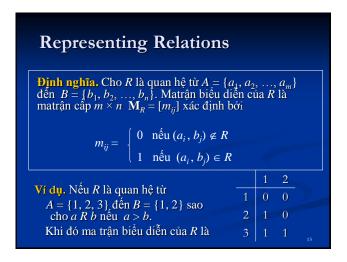










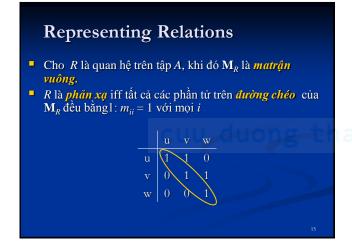


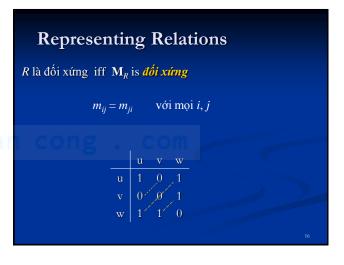
$$m_{ij} = \begin{cases} 1 & \text{if } (a_i, b_j) \in R \\ 0 & \text{if } (a_i, b_j) \notin R \end{cases}$$

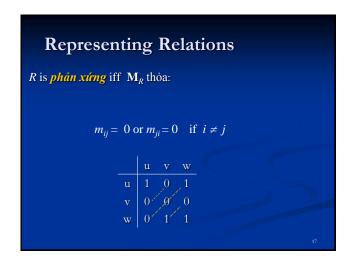
$$\text{Ví dụ. Cho } R \text{ là quan hệ từ } A = \{a_1, a_2, a_3\} \text{ đến } B = \{b_1, b_2, b_3, b_4, b_5\} \text{ được biểu diễn bởi matrận } b_1 \ b_2 \ b_3 \ b_4 \ b_5$$

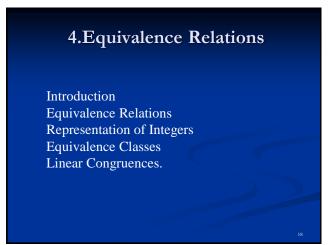
$$\mathbf{M}_R = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{array}{c} a_1 \\ a_2 \\ a_3 \end{cases}$$

$$\text{Khi đó } R \text{ gồm các cặp:} \{(a_1, b_2), (a_2, b_1), (a_2, b_3), (a_2, b_4), (a_3, b_1), (a_3, b_3), (a_3, b_5)\}$$

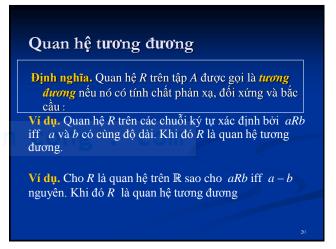












Recall that if a and b are integers, then a is said to be *divisible* by b, or a is a *multiple* of b, or b is a *divisor* of a, or b *divides* a if there exists an integer k such that a = kb

Example. Let m be a positive integer and R the relation on \mathbb{Z} such that aRb if and only if a-b is divisible by m, then R is an equivalence relation

- The relation is clearly reflexive and symmetric.
- Let a, b, c be integers such that a b and b c are both divisible by m, then a c = a b + b c is also divisible by m. Therefore R is transitive
- ■This relation is called the *congruence modulo m* and we write

 $a \equiv b \pmod{m}$

instead of aRb

Lóp tương đương

Dịnh 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

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

cuu duong than cong . com

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

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

Tương tự

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

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

23

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) $a R b \text{ iff } [a]_R = [b]_R$

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

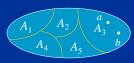
Chú ý. Các lóp tương đương theo một quan hệ tương đương trên *A* tạo nên một phân họach trên *A*, nghĩa là chúng chia tập A thành các tập con rời nhau.

24

Note. Cho $\{A_1, A_2, \dots\}$ 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 $a \in A_i$



25

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

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

26

7

cuu duong than cong . com

5 Linear Congruences

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

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

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

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

Example. $7 \equiv 2 \pmod{5}$ và $11 \equiv 1 \pmod{5}$. Ta có $7 + 11 \equiv 2 + 1 \equiv 3 \pmod{5}$

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

Note. Các phép tóan "+" và "ד 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 $[x]_{26} \rightarrow [x]_{26} + [3]_{26}$ 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: $A \rightarrow 0$, $B \rightarrow 1$, ..., $Z \rightarrow 25$

Mỗi chữ cái sẽ được mã hóa bằng cách cộng thêm 3. Chẳng hạn A $\frac{duợc}{ma}$ 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

MEET YOU IN THE PARK 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

<u>PHH</u>W BRX LQ WKH SDUN

cuu duong than cong . com

Để giải mã, ta dùng ánh xạ ngược:

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

P H H W tương ứng với 15 7 7 22

1111

Lấy ảnh qua ánh xa ngược: 12 4 4 19

Ta thu được chữ đã được mã

MEET

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 $f: [x]_{26} \rightarrow [ax+b]_{26}$ 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

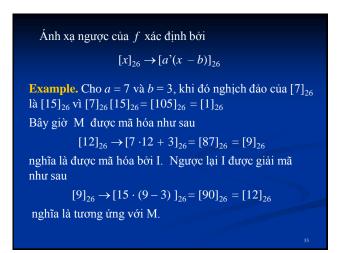
 $[a]_{26}[x]_{26} = [c]_{26}$

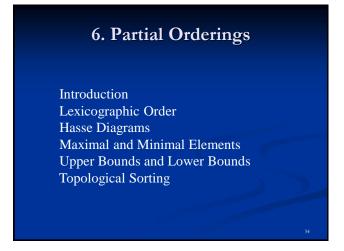
là $[x]_{26} = [a]_{26}^{-1} [c]_{26} = [a'c]_{26}$

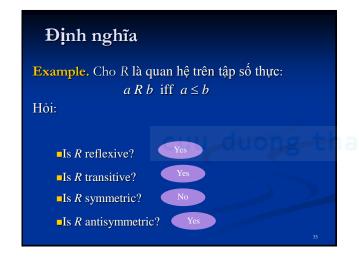
Chúng ta cũng nói nghiệm của phương trình

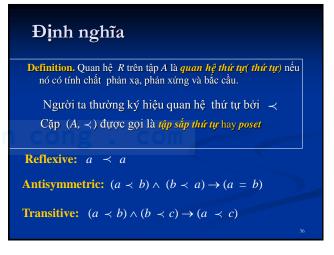
 $a\,x\equiv c\;(\mathrm{mod}\;26)$

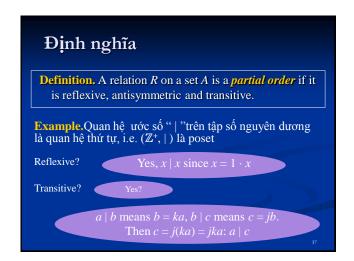
là $x \equiv a$ 'c (mod 26)

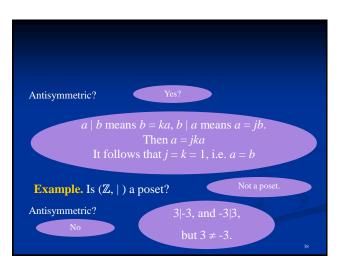


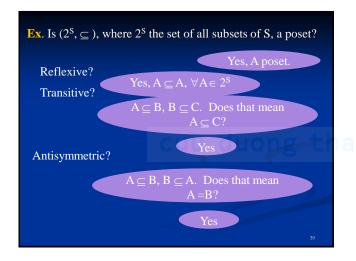


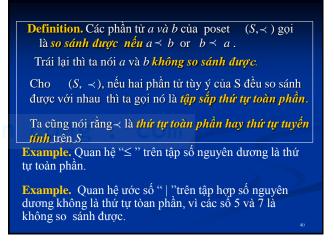












Thứ tự tự điển

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

$$a_1 a_2 \dots a_n \le b_1 b_2 \dots b_n$$

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

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, \leq) và (B, \leq') là hai tập sắp thứ tự tòan phần. Ta định nghĩa thứ tự \prec trên $A \times B$ như sau :

$$(a_1, b_1) \prec (a_2, b_2)$$
 iff
 $a_1 < a_2$ or $(a_1 = a_2 \text{ and } b_1 \le b_2)$

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

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

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

cuu duong than cong . com

Thứ tự tự điển

Cho Σ là một tập hữu hạn (ta gọi là bảng chữ cái). Tập hợp các chuỗi trên Σ , ký hiệu là Σ^* ,xác định bởi

- $\lambda \in \Sigma^*$, trong đó λ là chuỗi rỗng.
- Nếu $x \in \Sigma$, và $w \in \Sigma^*$, thì $wx \in \Sigma^*$, trong đó wx là kết nối w với x.

Example. Chẳng hạn $\Sigma = \{a, b, c\}$. Thế thì $\Sigma^* = \{\lambda, a, b, c, aa, ab, ac, ba, bb, bc, ca, cb, cc, aaa, aab,...\}$

43

Thứ tư tư điển

Giả sử \leq là thứ tự tòan phần trên Σ , khi đó ta có thể định nghĩa thứ tư toàn phần \prec trên Σ^* như sau.

Cho $s = a_1 a_2 \dots a_m$ và $t = b_1 b_2 \dots b_n$ là hai chuỗi trên Σ^*

Khi đó $s \prec t$ iff

• Hoặc $a_i = b_i$ đối với $1 \le i \le m$, tức là

 $t = \overline{a_1 a_2 \dots a_m b_{m+1} b_{m+2} \dots b_n}$

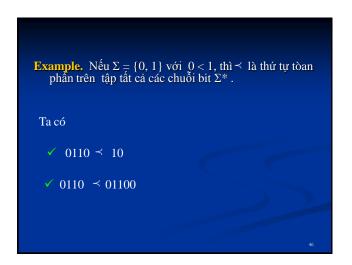
- Hoặc tồn tại k < m sao cho
 - $\checkmark a_i = b_i \text{ v\'oi } 1 \le i \le k \ v\`a$

 $\checkmark a_{k+1} < b_{k+1}$, nghĩa là

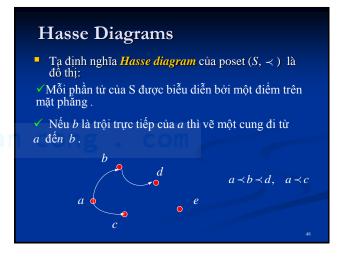
 $s = a_1 a_2 \dots a_k a_{k+1} a_{k+2} \dots a_m$ $t = a_1 a_2 \dots a_k b_{k+1} b_{k+2} \dots b_n$

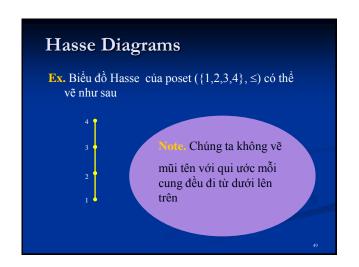
```
    Chúng ta có thể kiểm tra ≺ là thứ tự tòan phần trên Σ*
        Ta gọi nó là thứ tự từ điển trên Σ*

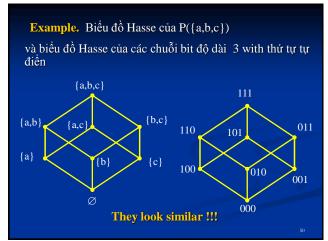
    Example. Nếu Σ là bảng chữ cái tiếng Anh với thứ tự: a < b < ... < z,thì thứ tự nói trên là thứ tự thông thường giữa các từ trong Từ điển.</li>
    For example
    ✓ discreet ≺ discrete
    ✓ discreet ≺ discrete
    ✓ discreet → discrete
    ✓ discreet → discrete
    ✓ discreet → discreetness
```



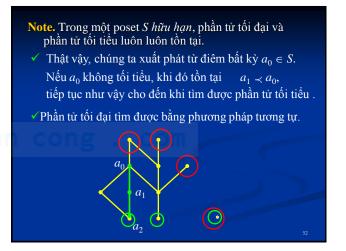


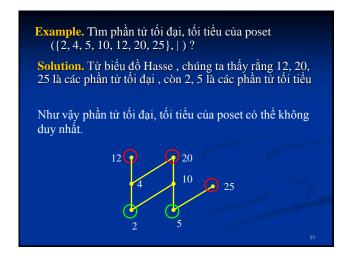


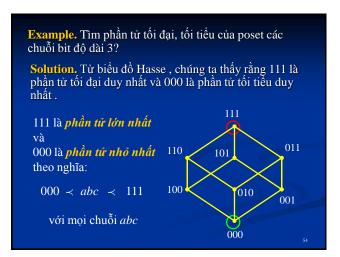


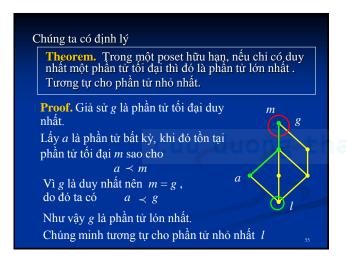


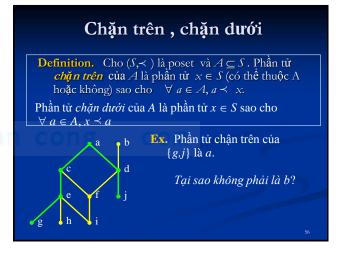


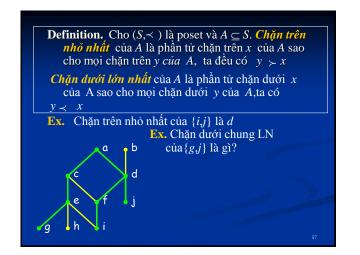


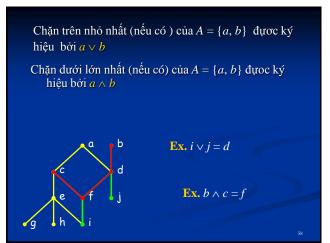


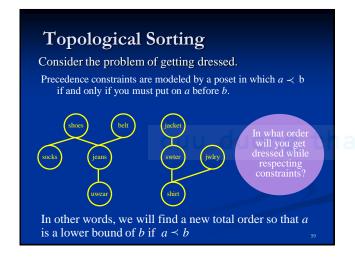


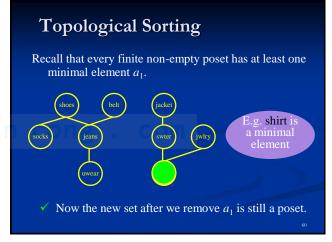


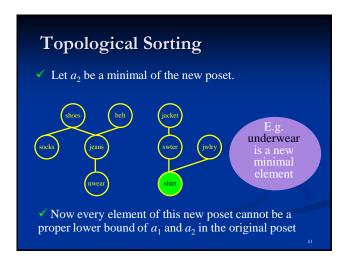


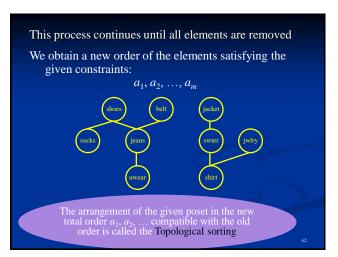












Bài tập

- 1. Khảo sát các tính chất của các quan hệ R sau. Xét xem quan hệ R nào là quan hệ tương đương. Tìm các lớp tương đương cho các quan hệ tương đương tương
- a) $\forall x, y \in \mathbb{R}, x\Re y \Leftrightarrow x^2 + 2x = y^2 + 2y$;
- b) $\forall x, y \in \mathbb{R}, x\Re y \Leftrightarrow x^2 + 2x \leq y^2 + 2y$;
- c) $\forall x, y \in \mathbb{R}, x\Re y \Leftrightarrow$

$$x^3 - x^2y - 3x = y^3 - xy^2 - 3y;$$

 $x^3-x^2y-3x=y^3-xy^2-3y;$ d) $\forall x,y\in\mathbb{R}^+,x\Re y\Leftrightarrow x^3-x^2y-x=y^3-xy^2-y.$

Bài tập

- 2. Khảo sát tính chất của các quan hệ sau a) $\forall x, y \in \mathbb{Z}$, $x\Re y \Leftrightarrow x|y$;
 - b) $\forall x, y \in \mathbb{R}, x\Re y \Leftrightarrow x = y \text{ hay } x < y + 1.$
- c) $\forall x, y \in \mathbb{R}$, $x\Re y \Leftrightarrow x = y \text{ hay } x < y 1$.
- d) $\forall (x, y); (z, t) \in \mathbb{Z}^2$, $(x, y) \le (z, t) \Leftrightarrow x \le z$ hay $(x = z \text{ và } y \le z)$
- e) $\forall (x, y); (z, t) \in \mathbb{Z}^2$, $(x, y) \le (z, t) \Leftrightarrow x < z \text{ hay } (x = z \text{ và } y \le z)$

