Contents

Wiki:

1. Các Kí Hiệu?

$$A \overset{def}{=} B$$

⇨ Câu này dịch như sau, theo định nghĩa, thì A bằng B

Set – Tập Hợp:

1. Kí Hiệu?

⇨ Cho V là tập hợp gồm các phần tử nào đó

⇨ Cách 1, liệt kê

$$V = \{1,2,3\}$$

⇨ Cách 2, dùng biến và các điều kiện, ngăn cách bởi dấu gạch hoặc 2 chấm

$$V = \{< Variable > | < Conditions >\}$$

⇨ Ví dụ

$$V = \{x|x > 1, x < 5\}$$

2. Tập Hợp Bằng Nhau?

⇨ Các phần tử trong tập hợp không quan tâm thứ tự và số lần xuất hiện

⇨ Ví dụ

$$\{1,2,3\} = \{3,3,2,1,1,2,3\}$$

3. Tập Lồi (Convex Set)?

⇨ Là 1 tập hợp các điểm trong không gian, sao cho tất cả điểm trên đường nối 2 điểm bất kì trong tập thì thuộc tập

4. Sơ Đồ Venn?

- ⇨ Bao gồm 1 tập vũ trụ, kí hiệu là U, chứa tất cả mọi thứ trên đời, tương ứng hình chữ nhật bao ngoài
- ⇨ Các bao đóng bên trong biểu diễn tập hợp
- ⇨ Các điểm biểu diễn phần tử trong tập hợp

5. Tập Rỗng (Empty Set) Và Tập Đơn (Singleton Set)?

- ⇨ 1 tập rỗng không chứa gì cả kí hiệu là {} hoặc ∅
- ⇨ 1 tập đơn chỉ chứa 1 phần tử duy nhất, ví dụ {∅} là 1 tập đơn do nó chứa đúng 1 phần tử là 1 tập rỗng

6. Tập Con Thực Sự (Proper Subset)?

- ⇨ Là tập con và không = tập cha, ví dụ {1, 2, 3} là tập con của {1, 2, 3} nhưng không phải tập con thực sự

7. Tập Hữu Hạn?

- ⇨ Giả sử 1 tập S có n phần tử riêng biệt, khi này bản số (Cardinality) của tập là

$$|S| = n$$

8. Tập Lũy Thừa (Power Set)?

- ⇨ Cho tập S, tập lũy thừa P(S) hay 2^S là tập hợp mà mỗi phần tử là tập con của S, chứa toàn bộ tập con của S
- ⇨ Cho A và B là tập bất kì, ta có các định lý sau

$$P(A \cap B) = P(A) \cap P(B)$$
$$|P(A)| = 2^{|A|}$$

- ⇨ Ví dụ

$$P(\{1,2,3\}) = 2^{\{1,2,3\}} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$$

- ⇨ Nếu S có n phần tử thì P(S) có 2^n phần tử

9. Dãy Sắp Thứ Tự (Ordered N Tuple)?

- ⇨ Là 1 dãy số a_1, a_2, a, …, a_N
- ⇨ Ví dụ
- ⇨ 3 – Tuple như (2, 5, 9) hoặc (4, 5, 8), …
- ⇨ 2 Tuple chỉ bằng nhau khi các phần tử tương ứng bằng nhau, ví dụ (1, 2, 3) = (1, 2, 3) nhưng không = (3, 2, 1)

10. Tích Cartesian (Tích Đề Các)?

- ⇨ Là tích của N tập hợp, kết quả trả về là 1 tập hợp mà càng phần tử đều là N – Tuple, mỗi Tuple gồm N giá trị tương ứng của N tập hợp theo đúng thứ tự

$$A \times B \times C \times \ldots = \{(a, b, c, \ldots) | a \in A, b \in B, c \in C, \ldots\}$$

- ⇨ Tưởng tượng tích Đề Các tạo thành 1 bảng trong trường hợp tích 2 tập hợp, 1 khối hộp trong trường hợp tích 3 tập hợp, …, với mỗi chiều đại diện cho 1 tập hợp
- ⇨ Ví dụ

$$\{1,2,3\} \times \{q, w\} \times \{A, B\} = \begin{Bmatrix} (1,q,A),(1,q,B),(1,w,A),(1,w,B),(2,q,A),(2,q,B), \\ (2,w,A),(2,w,B),(3,q,A),(3,q,B),(3,w,A),(3,w,B) \end{Bmatrix}$$

- ⇨ Ta còn sử dụng kí hiệu của tích Đề Các để định nghĩa hàm
- ⇨ Ví dụ

$$f: A \times B \to C$$

- ⇨ Nghĩa là hàm f sẽ ánh xạ mỗi cặp 2 – Tuple (a, b), a thuộc A, b thuộc B tới 1 phần tử c thuộc C
- ⇨ Mỗi phần tử trong tích Đề Các của 1 nhóm tập hợp còn gọi là 1 kết hợp giữa các nhóm đó

⇨ Ta có các công thức, được suy ra từ việc tưởng tượng bảng, khối hộp chữ nhật, …

$A \times B = A \times C \Leftrightarrow B = C$ $A \times (B \cap C) = (A \times B) \cap (A \times C)$ $(A \cap B) \times C = (A \times C) \cap (B \times C)$ $A \times (B \cup C) = (A \times B) \cup (A \times C)$ $(A \cup B) \times C = (A \times C) \cup (B \times C)$ $A \times (B - C) = (A \times B) - (A \times C)$ $(A - B) \times C = (A \times C) - (B \times C)$

11. Hợp (Union)?

$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n$

⇨ Để tìm số phần tử của 1 hợp, cộng tất cả số phần tử của từng tập hợp, trừ số phần tử của giao của mỗi bộ 2 tập hợp, cộng số phần tử của giao của mỗi bộ 3 tập hợp, trừ số phần tử của giao của mỗi bộ 4 phần tử, …

⇨ Ví dụ

$\lvert A_1 \cup A_2 \cup A_3 \cup A_4 \rvert =$ $\lvert A_1 \rvert + \lvert A_2 \rvert + \lvert A_3 \rvert + \lvert A_4 \rvert$ $-\lvert A_1 \cap A_2 \rvert - \lvert A_1 \cap A_3 \rvert - \lvert A_1 \cap A_4 \rvert - \lvert A_2 \cap A_3 \rvert - \lvert A_2 \cap A_4 \rvert - \lvert A_3 \cap A_4 \rvert$ $+\lvert A_1 \cap A_2 \cap A_3 \rvert + \lvert A_1 \cap A_2 \cap A_4 \rvert + \lvert A_1 \cap A_3 \cap A_4 \rvert + \lvert A_2 \cap A_3 \cap A_4 \rvert$ $-\lvert A_1 \cap A_2 \cap A_3 \cap A_4 \rvert$

12. Giao (Intersection)?

$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap A_3 \cap \ldots \cap A_n$

13. Hiệu (Difference)?

⇨ Là các phần tử thuộc tập hợp này nhưng không thuộc tập kia

$A - B = A \backslash B = \{x \mid x \in A, x \notin B\}$

⇨ Ví dụ

$\{1,2,3,4\} - \{2,3,9,8\} = \{1,4\}$

14. Hiệu Đối Xứng (EX – OR)?

⇨ Là các phần tử chỉ thuộc 1 trong 2 tập hợp, không được thuộc cả 2

$A \oplus B = \{x \mid x \in A \cup B, x \notin A \cap B\}$

15. Phần Bù (Complement)?

⇨ Là tất cả những gì không thuộc về tập hợp

$\bar{A} = A' = A^c = \{x \mid x \notin A\}$

16. Công Thức Giao Hợp?

⇨ Thế giao thành AND, hợp thành OR, các công thức y chang trong hệ thống số

17. Quan Hệ (Relation)?

⇨ Là khái niệm mở rộng ra từ hàm, ví dụ hàm y = 2x biểu diễn mối quan hệ tuyến tính giữa y và x, bản chất quan hệ là 1 tập hợp các điểm trong không gian tuân theo 1 quy luật nào đó

⇨ Cho 2 tập hợp A và B, C là tích Đề Các của chúng, R là 1 tập con bất kì của C, khi này R chính là 1 quan hệ từ A đến B, khi chỉ có 2 tập hợp, thì ta gọi là quan hệ 2 ngôi (Binary Relation) và mỗi 2 – Tuple trong quan hệ 2 ngôi gọi là cặp có thứ tự (Ordered Pair)

⇨ Mở rộng ra cho N tập hợp, R là 1 tập con bất kì của tích Đề Các của chúng, thì R gọi là quan hệ N ngôi

- ⇨ Ví dụ cho A = B = tập hợp số thực, khi này tích Đề Các của chúng sẽ là tập hợp toàn bộ tọa độ điểm trong không gian 2D, lấy 1 tập con của nó, giả sử tập con này bao gồm toàn bộ điểm tạo thành đồ thị hàm số bậc 2, thì rõ ràng đây chính là 1 quan hệ 2 ngôi giữa hoành độ và tung độ
- ⇨ Xét mệnh đề

$$aRb$$

- ⇨ Mệnh đề này tương đương

$$(a, b) \in R$$

- ⇨ 1 quan hệ trên 1 tập hợp là 1 quan hệ từ 1 tập hợp tới chính nó, ví dụ cho tập A, R là 1 tập con của tích Đề Các A x A thì R là 1 quan hệ trên A
- ⇨ Loại quan hệ từ 1 tập A tới chính nó sẽ có hoặc không có các tính chất sau
- ⇨ Tính phản xạ (Reflexive), (x, x) thuộc R

$$xRx, \forall x \in A$$

- ⇨ Số quan hệ có tính phản xạ trên tập có n phần tử là

$$2^{n(n-1)}$$

- ⇨ Tính phi phản xạ (Irreflexive), (x, x) không thuộc R

$$\overline{xRx}, \forall x \in A$$

- ⇨ Số quan hệ có tính phi phản xạ trên tập có n phần tử là

$$2^{n(n-1)}$$

- ⇨ Tính đối xứng (Symmetric), (x, y) thuộc R thì (y, x) cũng phải thuộc R

$$xRy \to yRx, \forall x, y \in A$$

- ⇨ Số quan hệ có tính đối xứng trên tập có n phần tử là

$$2^{\frac{n(n+1)}{2}}$$

- ⇨ Tính phản đối xứng, hay phản xứng (Antisymmetric), giả sử x khác y, (x, y) thuộc R thì (y, x) không được thuộc R

$$(xRy \wedge yRx) \to x = y, \forall x, y \in A$$

- ⇨ Số quan hệ có tính phản đối xứng trên tập có n phần tử là

$$2^n 3^{\frac{n(n-1)}{2}}$$

- ⇨ Tính phi đối xứng (Asymmetric), vừa phản đối xứng vừa phi phản xạ

$$\begin{cases} xRy \to \overline{yRx}, \forall x \neq y \in A \\ \qquad \overline{xRx}, \forall x \in A \end{cases}$$

- ⇨ Số quan hệ có tính phi đối xứng trên tập có n phần tử là

$$3^{\frac{n(n-1)}{2}}$$

- ⇨ Tính bắc cầu (Transitive), (x, y) và (y, z) thuộc R thì (x, z) cũng phải thuộc R

$$(xRy \wedge yRz) \to xRz, \forall x, y, z \in A$$

- ⇨ Ví dụ xét tập sau là tập ước số trên Z^+

$$R = \{(a, b) | a, b \in Z^+, a|b\}$$

- ⇨ Dễ thấy R có tính phản xạ, do a | a
- ⇨ R không có tính đối xứng, do a | b thì chưa chắc b | a
- ⇨ R có tính phản đối xứng, do a | b và b | a thì a phải = b
- ⇨ R có tính bắc cầu, a | b, b | c, thì đương nhiên a | c
- ⇨ Các quan hệ bản chất là tập hợp, do đó chúng có thể giao hợp các thứ để tạo ra quan hệ mới

18. Quan Hệ Hợp (Composition Relation)?

- ⇨ Khác với hàm, thay vì 1 điểm chỉ ánh xạ tới 1 điểm thì nó có thể ánh xạ tới nhiều điểm
- ⇨ Cho quan hệ R từ tập A tới B và quan hệ S từ tập B tới C, tưởng tượng 1 điểm a trong A, bị R ánh xạ tới 2 điểm trong B, 2 điểm này lại bị S ánh xạ tới tổng cộng 3 điểm trong C, như vậy, sẽ có 3 điểm trong C có thể đến được từ a thông qua R rồi S, bây giờ ta bỏ đi B, nối thẳng a vào 3 điểm trong C, khi này được quan hệ hợp

$$S \circ R = \{(a, c) \in A \times C | \exists b \in B, aRb \land bSc\}$$

- ⇨ Nghĩa là lấy tích Đề Các giữa A và C để xác định không gian mà quan hệ hợp thuộc về, nếu tồn tại 1 điểm cầu nối b trong B nối từ điểm a trong A tới c trong C thì cặp (a, c) sẽ hợp lệ, tức là a có thể tới c
- ⇨ Ví dụ

$$\{(a,5),(b,6),(a,0),(0,e)\} \circ \{(0,a),(1,b),(0,c),(2,d)\} = \{(0,5),(0,0),(1,6)\}$$

- ⇨ Cho A, B, C là các quan hệ trên tập A, ta có các định lý sau

$(A \circ B) \circ C = A \circ (B \circ C)$
Nếu A và B cùng phản xạ thì quan hệ hợp của A và B cũng phản xạ
Cho dù A và B cùng phi phản xạ/đối xứng/phản đối xứng/phi đối xứng thì chưa chắc quan hệ hợp của A và B phi phản xạ/đối xứng/phản đối xứng/phi đối xứng, kể cả khi A = B
Nếu A và B khác nhau và cùng bắc cầu, thì chưa chắc quan hệ hợp của A và B là bắc cầu

19. Quan Hệ Đường Chéo (Diagonal Relation)?

- ⇨ Cho Δ là quan hệ trên tập A, Δ là quan hệ đường chéo khi

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

- ⇨ Quan hệ đường chéo là quan hệ duy nhất có đủ 4 tính chất phản xạ, đối xứng, phản đối xứng và bắc cầu

20. Quan Hệ Ngược (Inverse Relation)?

- ⇨ Là thay đổi thứ tự của cặp giá trị trong mỗi Tuple của 1 quan hệ, ví dụ

$$R = \{(1,a),(2,b),(3,c)\} \Rightarrow R^{-1} = \{(a,1),(b,2),(c,3)\}$$

21. Quan Hệ Mũ (Power Of Relation)?

- ⇨ Cho quan hệ R, khi đó R^n = n hàm R hợp lồng lên nhau, ví dụ

$$R^4 = \big((R \circ R) \circ R\big) \circ R$$

- ⇨ Nếu R có tính bắc cầu thì R^n với n bất kì cũng có tính bắc cầu, không chắc $R^n = R$
- ⇨ Nếu R là quan hệ tương đương, thì $R^n = R$ với mọi n nguyên dương

22. Biểu Diễn Quan Hệ Bằng Ma Trận?

- ⇨ Cho tập A = {a, b, c, d, …}, cho tập B = {x, y, z, t, …}, R là quan hệ từ A tới B, = {(a, y), (c, z), …}
- ⇨ Bước 1, đặt các phần tử của A theo thứ tự từ trên xuống ở cạnh trái
- ⇨ Bước 2, đặt các phần tử của B theo thứ tự từ trái sang ở cạnh trên
- ⇨ Bước 3, ô nào thuộc R thì đánh 1, còn lại đánh 0

	x	Y	z	t	…
a	0	1	1	1	…
b	0	0	0	0	…
c	0	0	1	0	…

d	1	0	0	0	…
..	…	…	…	…	…

⇨ Ta được ma trận nhị phân biểu diễn R

23. Tính Nhanh Quan Hệ Hợp Bằng Ma Trận?

⇨ Cho S và R đều là quan hệ trên tập A, gọi biểu diễn ma trận của S là S' và R là R', khi này biểu diễn ma trận của S ∘ R chính bằng tích Boolean của R' với S'

⇨ Ví dụ

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

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

$$S' = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, R' = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$S \circ R = R' \circ S' = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \odot \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} =$$

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

24. Check Xem 1 Quan Hệ Có Tính Bắc Cầu Không?

⇨ Bước 1, lập biểu diễn ma trận của quan hệ R

⇨ Bước 2, tính R^2, nếu có 1 cặp (a, b) tồn tại trong R^2 mà không có trong R, nghĩa là hàng a cột b trong R^2 có giá trị = 1 còn hàng a cột b trong R có giá trị = 0, thì kết luận ngay R không có tính bắc cầu, nếu không tồn tại cặp nào như vậy thì kết luận có tính bắc cầu

⇨ Ví dụ 1

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

$$\Rightarrow R = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \Rightarrow R^2 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \odot \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

⇨ Dễ thấy phần tử hàng 1 cột 2 trong R^2 = 1 nhưng trong R thì = 0, do đó R không bắc cầu

⇨ Ví dụ 2

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

$$\Rightarrow R = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \Rightarrow R^2 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \odot \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

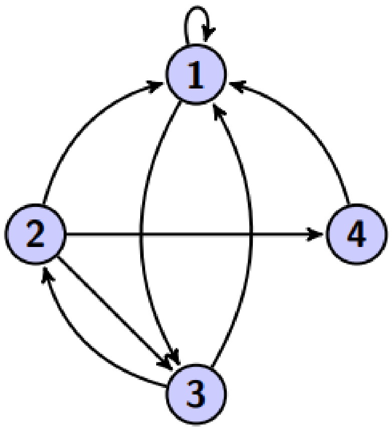
⇨ Dễ thấy R^2 y chang R, nghĩa là không tồn tại phần tử nào trong R^2 = 1 mà phần tử tương ứng trong R = 0, nên R bắc cầu

25. Biểu Diễn Quan Hệ Bằng Đồ Thị Có Hướng?

⇨ Giả sử R là quan hệ trên 1 tập hợp, ví dụ R là quan hệ trên tập số nguyên và = {(1, 1), (1, 3), (2, 1), (2, 3), (2, 4), (3, 1), (3, 2), (4, 1)}

⇨ Bước 1, vẽ các đỉnh là các số xuất hiện trong R

⇨ Bước 2, vẽ mũi tên, ví dụ (1, 2) thì mũi tên từ đỉnh 1 chĩa tới đỉnh 2



26. Bao Đóng (Closure)?

⇨ Bao đóng của 1 quan hệ R trên 1 tập theo 1 tính chất nào đó, ví dụ phản xạ, đối xứng, … là 1 quan hệ khác, mà quan hệ này là quan hệ có kích thước nhỏ nhất sao cho bao R, và thỏa mãn tính chất đó

⇨ Ví dụ, cho R = {(a, b), (c, d), (a, c), (b, b)}, ta có bao đóng phản xạ của nó là {(a, b), (c, d), (a, c), (b, b), (a, a), (c, c), (d, d)}

⇨ Tổng quát

⇨ Bao đóng phản xạ

$R \cup \Delta$

⇨ Để vẽ đồ thị có hướng của bao đóng phản xạ, chỉ cần vẽ thêm 1 mũi tên từ mỗi Node vào chính nó, nếu chưa có

⇨ Bao đóng đối xứng

$R \cup R^{-1}$

⇨ Để vẽ đồ thị có hướng của bao đóng đối xứng, chỉ cần lặp qua tất cả các mũi tên nối từ 1 Node tới Node khác, rồi vẽ thêm 1 mũi tên theo chiều ngược lại, nếu chưa có

⇨ Bao đóng bắc cầu, R là quan hệ trên tập có m phần tử

$\bigcup_{i=1}^{i=m} R^i$

27. Quan Hệ Tương Đương (Equivalence Relation)?

⇨ R gọi là quan hệ tương đương chỉ khi nó thỏa mãn 3 tính chất là phản xạ, đối xứng và bắc cầu, tính phản đối xứng có thể có hoặc không

⇨ Giả sử tập A là tập các số nguyên dương từ 1 đến 6, để xây dựng 1 quan hệ tương đương trên A, ta làm các bước sau

⇨ Bước 1, kẻ ma trận 6 x 6

6						
5						
4						
3						
2						
1						
	1	2	3	4	5	6

⇨ Bước 2, chia phần tập A, nói cách khác là chia A thành các phân hoạch, các phần có thể không liên tục, các phần khác nhau không giao nhau, tất cả các phần hợp lại thành A, ví dụ chia A thành {1, 2, 3}, {4, 5}, {6} hoặc {1, 4, 5}, {2, 3, 6}, …

⇨ Bước 3, với mỗi phần, thực hiện quét ngang và dọc ứng với phần đó, đánh dấu phần giao nhau, ví dụ phần {1, 4, 5} thì quét hàng 1, 4, 5, sau đó quét 1, 4, 5

⇨ Quét hàng

6						
5	x	x	x	x	x	x
4	x	x	x	x	x	x
3						
2						
1	x	x	x	x	x	x
	1	2	3	4	5	6

⇨ Quét tiếp cột

6	x			x	x	
5	x			x	x	
4	x			x	x	
3	x			x	x	
2	x			x	x	
1	x			x	x	
	1	2	3	4	5	6

⇨ Lấy phần vừa được quét hàng vừa được quét cột

6						
5	x			x	x	
4	x			x	x	
3						
2						
1	x			x	x	
	1	2	3	4	5	6

⇨ Tiếp tục thực hiện với các phần còn lại, rồi hợp lại, ví dụ nếu chia phần là {1, 4, 5}, {2, 3, 6} thì ta sẽ có ma trận

6		x	x			x
5	x			x	x	
4	x			x	x	
3		x	x			x
2		x	x			x
1	x			x	x	
	1	2	3	4	5	6

⇨ Đây chính là biểu diễn ma trận của 1 quan hệ tương đương trên tập A

⇨ Với mỗi cách chia phần khác nhau, sẽ tạo ra 1 quan hệ tương đương khác nhau, và với toàn bộ cách chia phần, ta có thể tạo ra mọi quan hệ tương đương có thể có

28. Số Cách Chia Phần 1 Tập Hợp?

⇨ Cho tập S gồm m phần tử, ta muốn chia S ra làm n tập con không rỗng, sao cho chúng hợp thành S và không giao nhau, số cách chia như vậy gọi là số Stirling loại 2 (Stirling Number Of The Second Kind), kí hiệu S(m, n)

$$S(m,n) = \left\{ {m \atop n} \right\} = \frac{1}{n!}\sum_{i=0}^{i=n}(-1)^{n-i}C_n^i i^m$$

⇨ Ví dụ 1

⇨ Số cách chia trong trường hợp S có 4 phần tử và ta muốn chia làm 3 tập con là

$$S(4,3) = \left\{ {4 \atop 3} \right\} = \frac{1}{3!}\sum_{i=0}^{i=3}(-1)^{3-i}C_3^i i^4 = \frac{1}{3!}(-C_3^0 0^4 + C_3^1 1^4 - C_3^2 2^4 + C_3^3 3^4) = 6$$

⇨ Ví dụ 2

⇨ Số cách chia trong trường hợp S có 7 phần tử và ta muốn chia làm 4 tập con là

$$S(7,4) = \left\{ {7 \atop 4} \right\} = \frac{1}{4!}\sum_{i=0}^{i=4}(-1)^{4-i}C_4^i i^7 = \frac{1}{4!}(C_4^0 0^7 - C_4^1 1^7 + C_4^2 2^7 - C_4^3 3^7 + C_4^4 4^7) = 350$$

⇨ Ta có công thức truy hồi sau

$$\left\{ {n+1 \atop k} \right\} = k\left\{ {n \atop k} \right\} + \left\{ {n \atop k-1} \right\}$$

⇨ Nghĩa là giả sử ta đang chia 10 cái bánh khác nhau cho 5 người, thêm 1 cái bánh khác vào 10 cái này, ta được 11 cái, và số cách chia mới cho 5 người được tính như sau

⇨ Trường hợp 1, cái bánh mới thêm vào là 1 nhóm, nghĩa là đưa nó cho 1 người, và người đó chỉ sở hữu cái bánh này, như vậy 10 cái bánh còn lại chia cho 4 người còn lại, có tổng cộng 34105 cách chia

⇨ Trường hợp 2, ta chia 10 cái bánh cũ cho 5 người trước đã, có 42525 cách chia, sau đó đưa cái bánh mới cho 1 trong 5 người, như vậy có tổng cộng 5 * 42525 cách chia

⇨ Tổng cộng 2 trường hợp, ta có 5 * 42525 + 34105 = 246730 cách chia, = S(11, 5)

⇨ Cho tập S gồm n phần tử, ta muốn chia S ra làm các tập con không rỗng, sao cho chúng hợp thành S và không giao nhau, số cách chia như vậy gọi là số Bell (Bell Number), kí hiệu B_n, nó = số quan hệ tương đương trên tập n phần tử

$$B_n = \sum_{i=0}^{i=n}\left\{ {n \atop i} \right\} = \sum_{i=0}^{i=n-1} C_{n-1}^i B_i = \frac{d^n}{dx^n}e^{e^x-1}\Big|_{x=0}$$

⇨ Ví dụ

⇨ Số cách chia phần tập 5 phần tử là

$$B_5 = \frac{d^5}{dx^5}e^{e^x-1}\Big|_{x=0} = 52$$

29. Lớp Tương Đương (Equivalence Class)?

⇨ Cho R là 1 quan hệ tương đương trên tập A, xét tất cả Tuple trong R có phần tử đầu tiên = a, ví dụ (a, a), (a, b), (a, foo), …, khi này tập hợp tất cả phần tử thứ 2 = {a, b, foo, …} gọi là lớp tương đương của a, kí hiệu

$$[a]_R = \{s|(a,s) \in R\}$$

⇨ Cách xác định nhanh lớp tương đương là sử dụng biểu diễn ma trận của nó, ta sẽ thấy có nhiều cột giống y chang nhau, và nếu xếp tất cả cột này gộp lại, sẽ được 1 ma trận vuông, tức là các cột giống nhau thì chung 1 lớp

⇨ Ví dụ, xét quan hệ tương đương trên tập {1, 2, 3, 4, 5, 6} có biểu diễn ma trận

6		x	x			x
5	x			x	x	
4	x			x	x	
3		x	x			x
2		x	x			x
1	x			x	x	
	1	2	3	4	5	6

⇨ Dễ thấy 2, 3, và 6 cùng chung 1 lớp, 1, 4, và 5 cùng chung 1 lớp, các lớp này sẽ không giao nhau, và hợp thành A

⇨ Nếu R là quan hệ tương đương trên tập A, ta có các định lý sau

$$aRb \leftrightarrow [a]_R = [b]_R \leftrightarrow [a]_R \cap [b]_R \neq \emptyset$$

⇨ Nghĩa là nếu lớp a = lớp b, hoặc chỉ cần lớp a và lớp b có 1 điểm chung, thì chắc chắn R chứa điểm (a, b)

⇨ Chứng minh

⇨ Vì R là quan hệ tương đương trên tập A, nên nếu (a, b) thuộc R, thì (b, a) cũng thuộc R, xét 1 điểm (b, x) thuộc R, thì do bắc cầu, (a, x) cũng thuộc R, do đó lớp a bao lớp b, mặt khác, xét 1 điểm (a, y) thuộc R, thì do bắc cầu (b, y) cũng thuộc R, hay lớp b bao lớp a, do đó lớp a phải = lớp b, ta chứng minh được chiều thuận của phép tương đương thứ nhất, mà lớp a = lớp b thì chúng phải có ít nhất 1 điểm giao nhau, chứng minh được chiều thuận của phép tương đương thứ 2

⇨ Tiếp nữa, giả sử lớp a và lớp b có 1 điểm giao nhau là x, nên (a, x) thuộc R, (b, x) thuộc R, mà (b, x) thuộc R nên (x, b) cũng thuộc R, bắc cầu ta được (a, b) thuộc R, chứng minh được chiều nghịch của phép tương đương thứ 2, mà lớp a = lớp b thì nó phải chứa 1 điểm chung, do đó chứng minh được chiều nghịch phép tương đương thứ 1

30. Quan Hệ Có Thứ Tự Bộ Phận (Partial Order Relation)?

⇨ Giống y chang quan hệ tương đương, chỉ khác là phải có tính phản đối xứng, tính đối xứng có thể có hoặc không

⇨ Ví dụ xét quan hệ có thứ tự bộ phận R trên tập A = {1, 2, 3, 4, 5, 6}, khi đó biểu diễn ma trận của R có thể là

6		x	x			x
5	x			x	x	
4	x			x		
3		x	x			
2		x				
1	x					
	1	2	3	4	5	6

⇨ Dễ thấy chỉ cần bỏ đi 1 nửa tam giác dưới hoặc trên của quan hệ tương đương là được 1 quan hệ có thứ tự bộ phận

⇨ Quan hệ sau cũng tính là loại quan hệ có thứ tự bộ phận

6						x
5					x	
4		x		x		
3			x		x	
2		x				
1	x					
	1	2	3	4	5	6

⇨ Tập có thứ tự bộ phận (Poset) là 1 tập S bình thường đi kèm với 1 quan hệ R có thứ tự bộ phận trên tập đó, kí hiệu (S, R), thông thường R được thay bằng dấu lớn, bé, thuộc, … để chỉ quan hệ mà mỗi cặp (a, b) trong đó, a đều lớn hơn, bé hơn, thuộc, … b, viết lại tổng quát như sau (S, ≼), dấu gạch ở dưới đại diện cho quan hệ đường chéo, dấu ≺ đại diện cho quan hệ so sánh

⇨ Ví dụ

⇨ Xét tập số nguyên Z, quan hệ R trên Z bao gồm tất cả các cặp (a, b) thỏa mãn a ≤ b, dễ thấy đây là quan hệ có thứ tự bộ phận, kí hiệu Poset ứng với Z và R như sau

$$\boxed{(Z, \leq)}$$

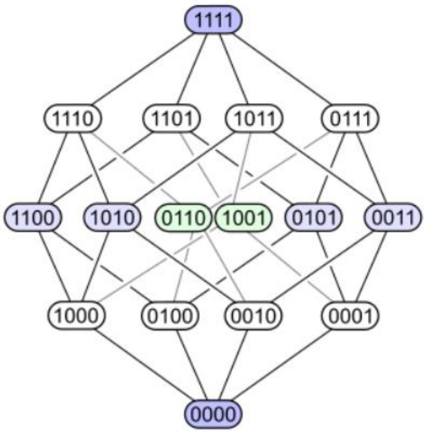
31. Biểu Diễn Quan Hệ Có Thứ Tự Bộ Phận Bằng Đồ Thị Hasse (Hasse Diagram)?

⇨ Cho Poset (A, R), để biểu diễn Poset này, ta làm các bước sau

⇨ Bước 1, liệt kê tất cả phần tử cực tiểu của (A, R)

⇨ Bước 2, lặp qua tất cả phần tử trên, vẽ mỗi phần tử thành hàng ngang

⇨ Bước 3, với mỗi điểm vừa vẽ, ví dụ điểm a, xét toàn bộ cặp (a, b) trong R, với b khác a và không tồn tại c sao cho (a, c) và (c, b) cùng thuộc R, rồi từ a vẽ đoạn thẳng hưởng lên trên, đầu trên vẽ điểm b
⇨ Bước 4, tiếp tục lặp qua tất cả điểm vừa vẽ và làm tương tự như bước 3
⇨ Ví dụ cho Poset (P(S), ⊆), S là tập gồm 4 phần tử {a, b, c, d}, P(S) là tập lũy thừa của S, kí hiệu mỗi phần tử trong P(S) là số nhị phân, ví dụ 0100 thì tương đương tập {b}, 1010 thì tương đương tập {a, c}, biểu diễn bằng đồ thị Hasse như sau



⇨ Bước 1, vẽ 0000 tương đương tập rỗng, dễ thấy nó là giá trị nhỏ nhất của (P(S), ⊆), do đó, nó là cực tiểu duy nhất
⇨ Bước 2, nối 0000 tới các tập 1000, 0100, 0010, 0001, do các tập này là các tập con nhỏ nhất chứa tập rỗng, lưu ý vẽ đường nối hướng lên trên
⇨ Bước 3, nối 1000 với 1100, 1010 và 1001, do các tập này đều là tập con nhỏ nhất chứa 1000
⇨ Bước 4, làm tương tự như bước 3 với 0100, 0010, …
⇨ Cuối cùng ta sẽ được đồ thị như trên
⇨ Dựa vào đồ thị Hasse, ta dễ dàng xác định được cực tiểu, cực đại, giá trị nhỏ nhất, lớn nhất, cận trên và cận dưới của Poset

32. So Sánh Được (Comparability)?

⇨ Cho Poset (A, R), khi này nếu (a, b) thuộc R, a khác b thì ta nói a bé hơn b và b lớn hơn a, nếu (a, b) và (b, a) đều không thuộc R, ta nói a và b không so sánh được với nhau
⇨ Cực đại của (A, R) là phần tử m sao cho nó phải luôn là phần tử thứ 2 trong tất cả 2 – Tuple thuộc R chứa nó không nằm trên đường chéo
⇨ Cực tiểu của (A, R) là phần tử n sao cho nó phải luôn là phần tử thứ 1 trong toàn bộ 2 – Tuple thuộc R chứa nó không nằm trên đường chéo
⇨ Giá trị lớn nhất của (A, R) là phần tử g sao cho với mọi x thuộc A, (x, g) thuộc R
⇨ Giá trị nhỏ nhất của (A, R) là phần tử h sao cho với mọi x thuộc A, (h, x) thuộc R
⇨ Cho Poset (A, R) bất kì, ta có các định lý sau

Giá trị lớn nhất của (A, R) nếu tồn tại thì là độc nhất và nó cũng là cực đại duy nhất của (A, R) Giá trị nhỏ nhất của (A, R) nếu tồn tại thì là độc nhất và nó cũng là cực tiểu duy nhất của (A, R)

33. Tập Có Thứ Tự Toàn Phần (Totally Ordered Set)?

⇨ Tập có thứ tự toàn phần, còn gọi là dây xích (Chain) là Poset mà mọi phần tử trong tập tương ứng của nó có thể so sánh được với nhau thông qua quan hệ tương ứng

⇨ Ví dụ (Z, ≤) là 1 dây xích

34. Tập Có Thứ Tự Tốt (Well Ordered Set)?

⇨ Là 1 dây xích, sao cho mọi tập con bất kì của nó, đều tồn tại phần tử bé nhất

⇨ Ta có các định lý

Mọi dây xích hữu hạn đều là tập có thứ tự tốt Tập số nguyên và số thực không có thứ tự tốt, do nó không có phần tử bé nhất, cận dưới là âm vô cùng Tập số tự nhiên có thứ tự tốt, do có cận dưới là 0 Tập các số hữu tỉ dương không có thứ tự tốt, do cận dưới của nó là mở, nghĩa là dần tới 0 nhưng không chạm được tới 0 Tập các số hữu tỉ dương với mẫu số không vượt quá n cũng là không có thứ tự tốt, ví dụ nếu n = 2018, thì số –1/–100000 vẫn hợp lệ, và do đó cận dưới mở

35. Cận Trên Và Cận Dưới?

⇨ Cho 1 Poset (S, R), ta có A là tập con của S, xét Poset (A, R)

⇨ 1 phần tử u trong S được gọi là cận trên của (A, R), nếu với mọi x thuộc A, (x, u) tồn tại trong R

⇨ (A, R) có thể có nhiều cận trên, gọi tập hợp các cận trên này là U, phần tử u trong U sẽ được gọi là cận trên nhỏ nhất của (A, R), nếu với mọi x thuộc U, (u, x) thuộc R

⇨ 1 phần tử v trong S được gọi là cận dưới của (A, R), nếu với mọi x thuộc A, (v, x) tồn tại trong R

⇨ (A, R) có thể có nhiều cận dưới, gọi tập hợp các cận dưới này là V, phần tử v trong V sẽ được gọi là cận dưới lớn nhất của (A, R), nếu với mọi x thuộc V, (x, v) thuộc R

36. Đại Số Sigma (σ Algebra)?

⇨ Cho tập X bất kì, khi đó tập Σ được gọi là 1 đại số Sigma của X khi nó thỏa mãn các điều sau

Σ là tập con của tập lũy thừa tạo ra từ X Σ chứa X Nếu Σ chứa tập A thì nó cũng chứa tập X – A Nếu Σ chứa tập A và B thì nó cũng chứa tập A ∪ B

⇨ Hệ quả

Nếu Σ chứa tập A và B thì nó cũng chứa A ∩ B Σ luôn chứa tập rỗng ∅ Đại số Sigma ít phần tử nhất của X là {X, ∅} Đại số Sigma nhiều phần tử nhất của X là tập lũy thừa của X

⇨ 1 đại số Sigma của 1 không gian mẫu gọi là 1 tập sự kiện, kí hiệu là Q

37. Chuồng Bồ Câu (Pigeon Hole)?

⇨ Để chứng minh 1 định lý có liên quan tới 1 chuồng bồ câu, ta dùng cách chia nhóm

⇨ Ví dụ

⇨ Chứng minh trong n số tự nhiên liên tiếp, sẽ có 1 số chia hết cho n

⇨ Bước 1, chia tập hợp số tự nhiên thành các nhóm đồng dư n, nghĩa là {0, n, 2n, …} thuộc cùng nhóm, {1, n + 1, 2n + 1, …} thuộc cùng nhóm, dễ thấy có n nhóm

⇨ Bước 2, do n số liên tiếp, nên số sau phải được đặt vào nhóm đồng dư kế tiếp, cứ như vậy thì n phần tử sẽ được đặt đầy đủ vào n nhóm đồng dư, do đó chắc chắn có 1 phần tử được đặt vào nhóm đồng dư 0, nghĩa là nó chia hết cho n

Magma – Groupoid:

1. Magma?

⇨ Chỉ đơn giản là 1 tập hợp S kèm theo 1 toán tử "·", thường gọi là phép nhân, kí hiệu (S, ·) sao cho thỏa mãn điều kiện

$a \cdot b \in S, \forall a, b \in S$

Semigroup:

1. Semigroup?

⇨ Là 1 Magma (S, ·) kèm theo điều kiện sau

$(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a, b, c \in S$

Monoid:

1. Monoid?

⇨ Là 1 Semigroup (S, ·) kèm theo điều kiện sau

$\exists e \in S, a \cdot e = e \cdot a = a, \forall a \in S$

⇨ e được gọi là Identity của S

⇨ Hệ quả

Mọi Semigroup đều chỉ có duy nhất 1 Identity

Group – Nhóm:

1. Nhóm?

⇨ Là 1 Semigroup (G, ·) kèm theo điều kiện sau, e là Identity của G

$\forall a \in G, \exists b \in A, a \cdot b = b \cdot a = e$

⇨ Khi này a và b được gọi là nghịch đảo của nhau, còn được kí hiệu là $b = a^{-1}$ hoặc $a = b^{-1}$

⇨ Hệ quả

Cho phần tử a bất kì thuộc Group G, thì nó chỉ có duy nhất 1 nghịch đảo

2. Nhóm Giao Hoán (Abelian Group)?

⇨ Là 1 nhóm (A, ·) kèm theo điều kiện sau

$a \cdot b = b \cdot a, \forall a, b \in A$

3. Bậc (Order) Của 1 Nhóm?

⇨ Là bản số, nói cách khác, là số phần tử của 1 nhóm

4. Nhóm Con (Subgroup)?

⇨ Cho 1 nhóm (G, ·), nếu H là 1 tập con của G và thỏa mãn các điều kiện để trở thành 1 nhóm dưới toán tử “·” thì (H, ·) được gọi là nhóm con của (G, ·), kí hiệu $H \leq G$

⇨ Bậc của 1 nhóm luôn chia hết cho bậc của nhóm con của nó

5. Nhóm Tầm Thường (Trivial Group)?

⇨ Là nhóm chỉ bao gồm 1 phần tử, nó nhân với chính nó ra chính nó

6. Nhóm Nhị Diện (Dihedral Group)?

⇨ Cho 1 nhóm (D, ·) gồm 2n phần tử, n là số nguyên dương, các phần tử lần lượt là r_i và s_i, i chạy từ 1 đến n, nhóm này sẽ được gọi là nhóm nhị diện và được kí hiệu là D_n nếu nó thỏa mãn bảng sau

	r_1	r_2	r_3	…	r_n	s_1	s_2	s_3	…	s_n
r_1	r_1	r_2	r_3	…	r_n	s_1	s_2	s_3	…	s_n
r_2	r_2	r_3	r_4	…	r_1	s_2	s_3	s_4	…	s_1
r_3	r_3	r_4	r_5	…	r_2	s_3	s_4	s_5	…	s_2
…	…	…	…	…	…	…	…	…	…	…
r_n	r_n	r_1	r_2	…	r_{n-1}	s_n	s_1	s_2	…	s_{n-1}
s_1	s_1	s_n	s_{n-1}	…	s_2	r_1	r_n	r_{n-1}	…	r_2
s_2	s_2	s_1	s_n	…	s_3	r_2	r_1	r_n	…	r_3
s_3	s_3	s_2	s_1	…	s_4	r_3	r_2	r_1	…	r_4
…	…	…	…	…	…	…	…	…	…	…
s_n	s_n	s_{n-1}	s_{n-2}	…	s_1	r_n	r_{n-1}	r_{n-2}	…	r_1

⇨ Mỗi ô trong bảng này = phần tử tương ứng ở cột trái cùng nhân với phần tử tương ứng ở cột trên cùng, ví dụ $r_3 \cdot r_2 = r_4$

⇨ Xét phần ô màu nâu, dễ thấy nó có chiều tăng dần từ trên xuống và tăng dần từ trái sang

⇨ Phần ô màu xanh nhạt y chang phần ô màu nâu, chỉ thay r thành s

⇨ Phần ô màu xanh lam có chiều tăng dần từ trên xuống và giảm dần từ trái sang

⇨ Phần ô màu bạc y chang phần ô màu xanh, chỉ thay s thành r

⇨ Để dễ hình dung, xét đa giác n cạnh, vẽ tất cả n trục đối xứng phân biệt của nó

⇨ Phần tử r_i tương ứng với phép quay ngược chiều kim đồng hồ 360 / n * (i – 1) độ

⇨ Phần tử s_i tương ứng với phép Flip đa giác theo trục đối xứng thứ i, trục thứ 1 nằm ngang, trục thứ 2 = trục thứ 1 quay trái góc 180 / n độ, …

⇨ Giá trị trả về của a · b là việc thực hiện phép a trước sau đó thực hiện phép b lên đa giác

⇨ Ví dụ nhóm D_3

	r_1	r_2	r_3	s_1	s_2	s_3
r_1	r_1	r_2	r_3	s_1	s_2	s_3
r_2	r_2	r_3	r_1	s_2	s_3	s_1
r_3	r_3	r_1	r_2	s_3	s_1	s_2
s_1	s_1	s_3	s_2	r_1	r_3	r_2
s_2	s_2	s_1	s_3	r_2	r_1	r_3
s_3	s_3	s_2	s_1	r_3	r_2	r_1

⇨ Là nhóm quay và Flip tam giác đều

⇨ D_n là nhóm con của D_m khi và chỉ khi m chia hết cho n

7. Coset?

⇨ Cho 1 nhóm (G, ·), (H, ·) là 1 nhóm con của nó

⇨ 1 tập con của G được gọi là 1 Coset trái (Left Coset) của (H, ·) nếu nó được tạo ra bằng cách lấy 1 phần tử g nào đó trong G nhân lần lượt với toàn bộ phần tử trong H, kí hiệu g · H

- ⇨ Tương tự 1 tập con của G được gọi là 1 Coset phải (Right Coset) của (H, ·) nếu nó được tạo ra bằng cách lấy từng phần tử trong H nhân với 1 phần tử g cố định trong G, kí hiệu H · g
- ⇨ Cho 1 nhóm (G, ·) bất kì, (H, ·) là nhóm con bất kì của nó, ta có các định lý sau

H vừa là Coset trái và Coset phải của (H, ·) Số Coset trái của (H, ·) = số Coset phải của nó = bậc (Index) của (H, ·) = |G : H| = |G| / |H| Tất cả các Left Coset được tạo ra từ (H, ·) một là trùng nhau hoàn toàn, hai là không có 1 điểm chung Tất cả các Right Coset được tạo ra từ (H, ·) một là trùng nhau hoàn toàn, hai là không có 1 điểm chung Tất cả các Left Coset được tạo ra từ (H, ·) phủ kín G Tất cả các Right Coset được tạo ra từ (H, ·) phủ kín G

8. Nhóm Con Bình Thường (Normal Subgroup)?
- ⇨ Cho 1 nhóm (G, ·), (N, ·) là 1 nhóm con của nó, khi này (N, ·) được gọi là nhóm con bình thường khi và chỉ khi với mọi g thuộc G, g · N = N · g, nói cách khác với mọi g thuộc G, g · N · g^{-1} thuộc N, kí hiệu N ◁ G
- ⇨ Mọi nhóm (G, ·) không tầm thường đều có đúng 2 nhóm con bình thường tầm thường (Trivial Normal Subgroup) là ({e}, ·) và (G, ·), e là Identity của (G, ·)

9. Nhóm Đơn Giản (Simple Group)?
- ⇨ Là 1 nhóm chỉ có đúng 2 nhóm con bình thường, là 2 nhóm con bình thường tầm thường của nó

10. Nhóm Đối Xứng (Symmetric Group)?
- ⇨ Là 1 nhóm (S, ·) có n! phần tử, thường kí hiệu S_n, với n nguyên dương, mỗi phần tử có thể được xem là 1 hoán vị riêng biệt của 1 dãy gồm n phần tử khác nhau, phép a · b có thể được hiểu là thực hiện phép hoán vị b trước, sau đó mới thực hiện phép hoán vị a
- ⇨ Cho S_n là 1 nhóm đối xứng bất kì, ta có các định lý sau

S_n là nhóm giao hoán khi và chỉ khi n ≤ 2

11. Nhóm Hoán Vị (Permutation Group)?
- ⇨ Là nhóm con bất kì của 1 nhóm đối xứng bất kì
- ⇨ Mỗi nhóm trên đời đều đẳng cấu với 1 nhóm hoán vị nào đấy

12. Nhóm Thay Thế (Alternating Group)?
- ⇨ Là 1 nhóm (A, ·) có n! / 2 phần tử, thường kí hiệu A_n, với n nguyên dương từ 2 trở lên, mỗi phần tử có thể được xem là 1 hoán vị chẵn riêng biệt của 1 dãy gồm n phần tử khác nhau, phép a · b có thể được hiểu là thực hiện phép hoán vị chẵn b trước, sau đó mới thực hiện phép hoán vị chẵn a
- ⇨ Cho A_n là 1 nhóm thay thế bất kì, ta có các định lý sau

A_n là nhóm giao hoán khi và chỉ khi n ≤ 3 A_n là nhóm đơn giản khi và chỉ khi n = 3 hoặc n ≥ 5 A_n là nhóm con không tầm thường lớn nhất của S_n

13. Nhóm Con Được Sinh Ra Từ 1 Tập Con?
- ⇨ Cho nhóm (G, ·), S là 1 tập con của nó, khi này ⟨S⟩ được gọi là nhóm con được sinh ra từ S, = nhóm con nhỏ nhất của (G, ·) chứa toàn bộ phần tử trong tập S, nói cách khác, là lấy các phần tử bất kì trong tập S rồi nhân loạn xì ngầu với nhau

⇨ Nếu ⟨S⟩ = (G, ·), ta nói S sinh ra G, hay S là tập sinh của G, các phần tử trong S gọi là phần tử sinh nhóm (Group Generator)
⇨ Nếu S là tập rỗng, thì ⟨S⟩ = nhóm con tầm thường của G
⇨ Nếu S chỉ có 1 phần tử là x, ta kí hiệu ⟨x⟩

14. Bậc (Order) Của 1 Phần Tử Trong Nhóm?
⇨ Là số lần nó phải nhân với chính nó để cho ra Identity, nói cách khác, cho phần tử x, bậc của x là số n nguyên dương nhỏ nhất sao cho x^n = Identity, kí hiệu bậc của x là |x|, nếu không tồn tại n thì |x| = vô cực

15. Nhóm Xoắn (Torsion Group, Periodic Group)?
⇨ Là nhóm mà tất cả phần tử của nó có bậc hữu hạn
⇨ Số mũ (Exponent) của 1 nhóm xoắn là bội chung nhỏ nhất của bậc của tất cả phần tử của nó

16. Nhóm Tuần Hoàn (Cyclic Group)?
⇨ Cho 1 nhóm (C, ·) gồm n phần tử, n là số nguyên dương, các phần tử kí hiệu là r_i, i chạy từ 1 đến n, nhóm này sẽ được gọi là nhóm tuần hoàn và được kí hiệu là C_n hoặc Z_n nếu nó thỏa mãn bảng sau

	r_1	r_2	r_3	…	r_n
r_1	r_1	r_2	r_3	…	r_n
r_2	r_2	r_3	r_4	…	r_1
r_3	r_3	r_4	r_5	…	r_2
…	…	…	…	…	…
r_n	r_n	r_1	r_2	…	r_{n-1}

⇨ Mỗi ô trong bảng này = phần tử tương ứng ở cột trái cùng nhân với phần tử tương ứng ở cột trên cùng, ví dụ $r_3 \cdot r_2 = r_4$
⇨ Dễ thấy bảng trên y chang phần bảng màu nâu ở nhóm nhị diện, nói cách khác, nhóm này chứa các phần tử là quay ngược chiều kim đồng hồ với một góc là bội số của 360 / n độ
⇨ Một nhóm (G, ·) là nhóm tuần hoàn khi và chỉ khi tồn tại 1 phần tử x trong nó sao cho nó sinh ra G
⇨ Nếu nhóm (G, ·) có bậc là số nguyên tố thì chắc chắn nó là nhóm tuần hoàn
⇨ Mọi nhóm tuần hoàn đều là nhóm giao hoán

17. Commutator?
⇨ Cho 1 nhóm (G, ·), a và b là 2 phần tử bất kì trong nó, khi này Commutator của a với b là

$$[a, b] = a^{-1} \cdot b^{-1} \cdot a \cdot b$$

⇨ Ta có các định lý sau, cho e là Identity của (G, ·)

$$[a, b] = [b, a]^{-1}$$
$$[a, b] = e \Leftrightarrow a \cdot b = b \cdot a$$

18. Nhóm Con Commutator (Commutator Subgroup)?
⇨ Cho 1 nhóm (G, ·), tập S là tập chứa toàn bộ các Commutator của nhóm này

$$S = \{[a, b]: a, b \in G\}$$

⇨ Khi này ⟨S⟩ được gọi là nhóm con Commutator của (G, ·)

19. Nhóm Thương (Quotient Group)?
⇨ Cho nhóm (G, ·), (N, ·) là một nhóm con bình thường của nó, khi này ta nói G / N là nhóm thương của G bởi N
⇨ G / N bao gồm các phần tử là Coset trái của N, toán tử "·" trong G / N được định nghĩa như sau, cho a · N là b · N là 2 Coset trái bất kì của N, a và b thuộc G

$(a \cdot N) \cdot (b \cdot N) = (a \cdot b) \cdot N$

⇨ G / N là nhóm giao hoán khi và chỉ khi nhóm con Commutator của (G, ·) là nhóm con của (N, ·)

⇨ Ta có 1 số công thức sau

Nhóm thương S_n / A_n đẳng cấu với nhóm tuần hoàn C_2 Nhóm thương G / {e}, e là Identity của (G, ·), đẳng cấu với (G, ·) Nhóm thương G / G, đẳng cấu với nhóm tầm thường

20. Nhóm Có Thể Giải (Solvable Group)?

⇨ Cho nhóm (G, ·), nó là nhóm có thể giải khi và chỉ khi tồn tại 1 chuỗi nhóm con bình thường sau, e là Identity của nhóm này, sao cho mọi nhóm thương G_k / G_{k-1} , với k chạy từ 1 tới n, đều là nhóm giao hoán, số n nhỏ nhất thỏa mãn điều kiện trên được gọi là chiều dài dẫn xuất (Derived Length) của nhóm (G, ·)

$e = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$

⇨ Ví dụ

⇨ Nhóm đối xứng S_5 là nhóm không thể giải vì nó chỉ có duy nhất 1 nhóm con bình thường không tầm thường là A_5, mà nhóm thương A_5 / {e} lại không phải nhóm giao hoán, e là Identity của S_5

⇨ Ta có 1 số định lý sau

Nhóm S_n là nhóm có thể giải khi và chỉ khi n ≤ 4 Mọi nhóm giao hoán đều là nhóm có thể giải Mọi nhóm con của nhóm có thể giải đều là nhóm có thể giải Cho nhóm (G, ·), nếu tồn tại 1 nhóm con bình thường (N, ·) của nó, sao cho nhóm thương G / N không thể giải, thì (G, ·) không thể giải Cho nhóm (G, ·) có thể giải, (N, ·) là 1 nhóm con bình thường của nó, thì khi này, nhóm thương G / N phải có thể giải

Rng – Chuông:

1. Chuông?

⇨ Là 1 tập hợp R kèm theo 2 toán tử, giả sử 2 toán tử này kí hiệu là "+", gọi là cộng, và "·", gọi là nhân, kí hiệu (R, +, ·), thỏa mãn các điều kiện sau

(R, +) phải là 1 nhóm giao hoán (R, ·) phải là 1 Semigroup $a \cdot (b + c) = (a \cdot b) + (a \cdot c), \forall a, b, c \in R$ $(a + b) \cdot c = (a \cdot c) + (b \cdot c), \forall a, b, c \in R$

Ring – Vành:

1. Vành?

⇨ Là 1 chuông (R, +, ·), chỉ khác ở chỗ (R, ·) phải là 1 Monoid

2. Vành Giao Hoán (Commutative Ring)?

⇨ Là 1 vành (R, +, ·) kèm theo điều kiện sau

$a \cdot b = b \cdot a, \forall a, b \in A$

3. Một Số Vành Thường Gặp?
⇨ Tập hợp số hữu tỉ với phép cộng và nhân
⇨ Tập hợp số thực với phép cộng và nhân
4. Vành Không (Zero Ring)?
⇨ Là vành chỉ có duy nhất 1 phần tử, nó vừa là Identity của phép cộng vừa là Identity của phép nhân
5. Characteristic Của 1 Vành?
⇨ Là số nguyên dương n nhỏ nhất sao cho tổng n phần tử, mỗi phần tử đều là Identity của phép nhân, = Identity của phép cộng, nếu không tồn tại thì cho = 0, kí hiệu char(R), (R, +, ·) là vành đang xét
⇨ Ta có các định lý sau

Vành (R, +, ·) có vô hạn phần tử khi và chỉ khi char(R) = 0 Vành (R, +, ·) là vành không khi và chỉ khi char(R) = 1

6. Zero Divisor?
⇨ Cho vành (R, +, ·), 1 phần tử a thuộc R được gọi là Left Zero Divisor của (R, +, ·) nếu tồn tại 1 phần tử b không phải Identity của phép cộng thuộc R sao cho a · b = Identity của phép cộng
⇨ Tương tự, 1 phần tử a thuộc R được gọi là Right Zero Divisor của (R, +, ·) nếu tồn tại 1 phần tử b không phải Identity của phép cộng thuộc R sao cho b · a = Identity của phép cộng
⇨ Nếu a vừa là Left và Right Zero Divisor thì gọi là Two Sided Zero Divisor
⇨ Identity của phép cộng là 1 Two Sided Zero Divisor và còn được gọi là Zero Divisor tầm thường
7. Tập Lý Tưởng (Ideal)?
⇨ Cho vành (R, +, ·)
⇨ 1 tập con S của R được gọi là 1 tập lý tưởng trái (Left Ideal) của (R, +, ·) nếu nhóm (S, +) là nhóm con của nhóm (R, +), đồng thời lấy 1 phần tử bất kì trong R nhân với 1 phần tử bất kì trong S phải được 1 phần tử trong S
⇨ Tương tự, 1 tập con S của R được gọi là 1 tập lý tưởng phải (Right Ideal) của (R, +, ·) nếu nhóm (S, +) là nhóm con của nhóm (R, +), đồng thời lấy 1 phần tử bất kì trong S nhân với 1 phần tử bất kì trong R phải được 1 phần tử trong S
⇨ Nếu S vừa là tập lý tưởng trái và tập lý tưởng phải thì nó gọi là tập lý tưởng 2 bên (Two Sided Ideal) của (R, +, ·)
⇨ R luôn là tập lý tưởng 2 bên của (R, +, ·), gọi là tập lý tưởng đơn vị (Unit Ideal), kí hiệu (1)
⇨ {e}, với e là Identity của phép "+", luôn là tập lý tưởng 2 bên của (R, +, ·), gọi là tập lý tưởng không (Zero Ideal), kí hiệu (0)
8. Vành Đơn Giản (Simple Ring)?
⇨ Là vành khác vành không, sao cho nó chỉ có đúng 2 tập lý tưởng là tập lý tưởng đơn vị và tập lý tưởng không
9. Vành Tự Đồng Cấu (Endomorphism Ring)?
⇨ Cho nhóm giao hoán (G, ·), khi này tập hợp R chứa tất cả các phép tự đồng cấu trên (G, ·), kèm theo 2 toán tử "+" và "*", gọi là phép cộng tự đồng cấu và phép nhân tự đồng cấu, sẽ tạo thành 1 vành (R, +, *), kí hiệu End(G)
⇨ Phép cộng tự đồng cấu được định nghĩa như sau
⇨ Cho f và g là 2 phép tự đồng cấu trên (G, ·), x là 1 phần tử thuộc G, khi này

(f + g)(x) = f(x) · g(x) = h(x), như vậy f + g sẽ ra 1 phép tự đồng cấu mới là h

⇨ Identity của phép cộng tự đồng cấu là phép tự đồng cấu biến mọi phần tử trong G thành Identity của (G, ·)

⇨ Phép nhân tự đồng cấu được định nghĩa như sau

⇨ Cho f và g là 2 phép tự đồng cấu trên (G, ·), x là 1 phần tử thuộc G, khi này (f * g)(x) = f(g(x)) = h(x), như vậy f * g sẽ ra 1 phép tự đồng cấu mới là h\

⇨ Identity của phép nhân tự đồng cấu là phép tự đồng cấu biến mỗi phần tử trong G thành chính nó

10. Vành Chia (Division Ring, Skew Field)?

⇨ Là 1 vành (R, +, ·) kèm theo các điều kiện sau

Identity e_1 của nhóm (R, +) phải khác Identity e_2 của Monoid (R, ·) $\forall a \in R \backslash \{e_1\}, \exists b \in R, a \cdot b = b \cdot a = e_2$

Field – Trường:

1. Trường?

⇨ Là 1 vành (F, +, ·) vừa là vành giao hoán, vừa là vành chia

2. Một Số Trường Thường Gặp?

⇨ Tập hợp số thực với phép cộng và nhân

3. Trường Con (Subfield) Và Trường Mở Rộng (Extension Field)?

⇨ Cho 1 trường (F, +, ·), nếu N là 1 tập con của F và thỏa mãn các điều kiện để trở thành 1 trường dưới toán tử “+” và “·” thì (N, +, ·) được gọi là trường con của (F, +, ·), khi này (F, +, ·) được gọi là trường mở rộng của (N, +, ·)

⇨ Phép mở rộng trường (Field Extension) từ trường (N, +, ·) sang trường (F, +, ·) kí hiệu là F / N

⇨ Nếu (K, +, ·) là trường con của (F, +, ·) và là trường mở rộng của (N, +, ·) thì (K, +, ·) gọi là trường trung gian (Intermediate Field) của phép mở rộng F / N

⇨ Bậc (Degree) của phép mở rộng trường F / N, kí hiệu [F : N], chính là số phần tử ít nhất trong F để tất cả tổ hợp tuyến tính của chúng, với hệ số thuộc N, phủ kín F

⇨ Cho (K, +, ·) là trường trung gian của F / N, thì bậc của F / N = bậc của F / K nhân với bậc của K / N

⇨ Nếu F = N thì F / N gọi là phép mở rộng tầm thường (Trivial Extension), khi này [F : N] = 1

⇨ Nếu [F : N] = 2, thì F / N gọi là phép mở rộng bậc 2 (Quadratic Extension)

⇨ Nếu [F : N] = 3, thì F / N gọi là phép mở rộng bậc 3 (Cubic Extension)

⇨ Cho phép mở rộng F / N, S là 1 tập con của F, khi này trường con nhỏ nhất của F chứa cả N lẫn S được kí hiệu là N(S), đọc là N thêm (Adjoin) S, nếu S chỉ có 1 phần tử thì phép mở rộng N(S) / N gọi là phép mở rộng đơn giản (Simple Extension)

⇨ Ví dụ, với Q là tập hợp số hữu tỉ

$[Q(\sqrt{2}, \sqrt{3}) : Q] = 4$

4. Trường Đại Số (Algebraic Number Field)?

- ⇨ Là trường mở rộng Q(S) của trường số hữu tỉ Q đến 1 số bậc hữu hạn, nghĩa là [Q(S) : Q] hữu hạn, nếu S chỉ bao gồm 1 phần tử là 1 nghiệm phức của phương trình $x^n = 1$, với n bất kì, thì Q(S) còn gọi là trường Cyclotomic

5. Phép Mở Rộng Cyclotomic?

- ⇨ Là phép mở rộng có dạng F(S) / F, với S là 1 nghiệm phức của phương trình $x^n = 1$, với n bất kì

6. Trường Phân Rã (Splitting Field)?

- ⇨ Cho 1 trường (K, +, ·), f(x) là 1 đa thức với hệ số thuộc K, khi này (F, +, ·) được gọi là trường phân rã của f(x) trên K nếu nó là trường mở rộng nhỏ nhất của (K, +, ·) chứa toàn bộ nghiệm của phương trình f(x) = 0
- ⇨ Mở rộng ra họ các đa thức, cho 1 trường (K, +, ·), S là 1 tập hợp chứa các phần tử là đa thức với hệ số thuộc K, khi này (F, +, ·) được gọi là trường phân rã của f(x) trên họ đa thức S nếu nó là trường mở rộng nhỏ nhất của (K, +, ·) chứa hợp của tất cả tập nghiệm của các đa thức trong S

7. Phép Mở Rộng Căn (Radical Extension)?

- ⇨ Phép mở rộng F / K được gọi là phép mở rộng căn nếu F = K(S), với S là 1 tập hợp gồm các phần tử, sao cho với mỗi phần tử a, tồn tại 1 số nguyên dương n sao cho a^n = một số nào đó trong K
- ⇨ Ví dụ sau đây là phép mở rộng căn, Q là tập số hữu tỉ

$$Q\left(\sqrt{2}, \sqrt[3]{5}, e^{\frac{2}{3}\pi i}\right)/Q$$

8. Đa Thức Nhỏ Nhất (Minimal Polynomial)?

- ⇨ Cho trường (F, +, ·) và (N, +, ·) là 1 trường con của nó, cho 1 phần tử a bất kì thuộc F, khi này đa thức nhỏ nhất của a trên N là đa thức f(x) có bậc nhỏ nhất với các hệ số thuộc N, sao cho hệ số ứng với x mũ lớn nhất, là = 1, và a là 1 nghiệm của phương trình f(x) = 0
- ⇨ Đa thức nhỏ nhất nếu tồn tại, thì là độc nhất
- ⇨ Ví dụ
- ⇨ Cho trường số phức với trường con là số hữu tỉ, khi này đa thức nhỏ nhất của số i trên trường số hữu tỉ là

$$f(x) = x^2 + 1$$

9. Phần Tử Đại Số (Algebraic Element) Và Phần Tử Siêu Việt (Transcendental Element)?

- ⇨ Cho phép mở rộng F / N, a là 1 phần thuộc F, khi này a sẽ được gọi là phần tử đại số trên N nếu tồn tại 1 đa thức f(x) bậc > 0 với hệ số thuộc N, sao cho a là nghiệm của phương trình f(x) = 0
- ⇨ Nếu a không phải là phần tử đại số trên N thì nó gọi là phần tử siêu việt trên N

10. Phép Mở Rộng Đại Số (Algebraic Extension) Và Phép Mở Rộng Siêu Việt (Transcendental Extension)?

- ⇨ Phép mở rộng F / N được gọi là phép mở rộng đại số nếu mọi phần tử thuộc F đều là phần tử đại số trên N
- ⇨ Nếu F / N không phải phép mở rộng đại số thì nó gọi là phép mở rộng siêu việt

11. Phép Mở Rộng Bình Thường (Normal Extension)?

- ⇨ Phép mở rộng đại số F / N được gọi là bình thường nếu thỏa mãn điều kiện sau
- ⇨ Xét mọi đa thức f(x) bậc > 0 với hệ số thuộc N, sao cho f(x) không thể phân tách thành 2 nhân tử, mà mỗi nhân tử này là 1 đa thức bậc > 0 với hệ số thuộc N, nếu

phương trình f(x) = 0 có 1 nghiệm thuộc F thì toàn bộ nghiệm của phương trình f(x) = 0 đều thuộc F

12. Trường Đại Số Đóng (Algebraically Closed Field)?
- ⇨ Là trường (F, +, ·), sao cho mọi đa thức f(x) bậc > 0 với hệ số thuộc F, đều có ít nhất một nghiệm thuộc F
- ⇨ Hệ quả

Trường số phức là trường đại số đóng Mọi đa thức f(x) bậc > 0 với hệ số thuộc F đều có nguyên tập nghiệm thuộc F

13. Bao Đóng Đại Số (Algebraic Closure)?
- ⇨ Cho trường (N, +, ·), (F, +, ·) là 1 trường mở rộng của nó, khi này (F, +, ·) được gọi là bao đóng đại số của (N, +, ·) khi và chỉ khi F / N là 1 phép mở rộng đại số và (F, +, ·) là trường đại số đóng
- ⇨ Bao đóng đại số của trường (N, +, ·) chính là trường mở rộng lớn nhất của (N, +, ·), do đó nó là độc nhất

14. Đa Thức Có Thể Phân Chia (Separable Polynomial)?
- ⇨ Cho trường (N, +, ·), (F, +, ·) là bao đóng đại số của nó, cho đa thức f(x) với hệ số thuộc N, khi này f(x) được gọi là đa thức có thể phân chia khi và chỉ khi tất cả các nghiệm của phương trình f(x) = 0 đều nằm trong F, và chúng phân biệt, nghĩa là số nghiệm bằng bậc của f(x)

15. Phép Mở Rộng Có Thể Phân Chia (Separable Extension)?
- ⇨ Cho phép mở rộng đại số F / N, nó sẽ được gọi là phép mở rộng có thể phân chia nếu với mọi phần tử a thuộc F, đa thức nhỏ nhất của a trên K là đa thức có thể phân chia

16. Phép Mở Rộng Galois (Galois Extension)?
- ⇨ Là phép mở rộng F / N vừa bình thường vừa có thể phân chia, tương đương F là trường phân rã của 1 đa thức có thể phân chia với hệ số thuộc N

17. Nhóm Tự Đẳng Cấu (Automorphism Group) Của 1 Phép Mở Rộng?
- ⇨ Cho phép mở rộng F / N, khi này nhóm tự đẳng cấu của phép mở rộng này, kí hiệu Aut(F / N), chứa tất tần tật các phép tự đẳng cấu từ F tới chính nó, sao cho các phần tử trong N không bị thay đổi

18. Nhóm Galois (Galois Group)?
- ⇨ Là nhóm tự đẳng cấu của 1 phép mở rộng Galois F / N, kí hiệu Gal(F / N)
- ⇨ Cho trường (N, +, ·), (F, +, ·) là trường phân rã của đa thức f(x) trên N, f(x) là đa thức có thể phân chia, khi này nhóm Gal(F / N) đẳng cấu với với nhóm S_n, n là số nghiệm của phương trình f(x) = 0, nghĩa là nhóm Gal(F / N) bản chất chứa các phần tử là hoán vị các nghiệm của phương trình f(x) = 0

19. Phép Mở Rộng Kummer (Kummer Extension)?
- ⇨ Là phép mở rộng F / N, sao cho N chứa tập nghiệm phức của phương trình $x^n = 1$, với n là 1 số nguyên dương nào đó, đồng thời nhóm Gal(F / N) phải là nhóm giao hoán và cũng là nhóm xoắn, với số mũ là n

21. Nhóm Tuyến Tính Tổng Quát (General Linear Group)?
- ⇨ Cho nhóm (G, ·), có các phần tử là ma trận không suy biến kích thước n x n, các phần tử trong ma trận đều thuộc trường hoặc vành F, toán tử "·" được hiểu là phép nhân ma trận, thì khi này (G, ·) được gọi là nhóm tuyến tính tổng quát của ma trận không suy biến cấp n trên trường F, kí hiệu là $GL_n(F)$

22. Nhóm Tuyến Tính Đặc Biệt (Special Linear Group)?

- ⇨ Cho nhóm tuyến tính tổng quát $GL_n(F)$, gọi e là Identity của phép nhân của trường hoặc vành F, khi này nhóm con của $GL_n(F)$ chỉ chứa toàn bộ các ma trận có định thức = e được gọi là nhóm tuyến tính đặc biệt của ma trận không suy biến cấp n trên trường hoặc vành F, kí hiệu $SL_n(F)$

23. Cách Tìm Phần Dư Của Phép Chia Đa Thức Nhanh Nhất?

- ⇨ Cho đa thức f(x) và g(x), ta muốn tìm phần dư của phép chia f(x) cho g(x)
- ⇨ f(x) có thể được viết dưới dạng q(x)g(x) + r(x), trong đó q(x) và r(x) đều là đa thức, và r(x) có bậc nhỏ hơn q(x)
- ⇨ g(x) tách thành các nhân tử dạng $(x – a)^k$, a là nghiệm phức của phương trình g(x) = 0, k là bội đại số của nó
- ⇨ Để tìm các hệ số của r(x), ta sẽ thế a vào phương trình f(x) = q(x)g(x) + r(x), khi này ta sẽ được 1 phương trình nhiều ẩn f(a) = r(a), với các ẩn là hệ số của r(x), tiến hành làm như vậy với các nghiệm còn lại, ta sẽ được 1 hệ các phương trình
- ⇨ Tuy nhiên, nếu k > 1, thì số phương trình sẽ < số ẩn, để bù thêm phương trình, ta đạo hàm 2 vế của f(x) = q(x)g(x) + r(x), rồi tiếp tục thế a vào và ra được phương trình mới, nếu vẫn không đủ thì đạo hàm cấp 2, 3, …, ta cần phải đạo hàm m – 1 lần, với m là số k lớn nhất trong các nhân tử
- ⇨ Ví dụ 1

$$f(x) = x^{11}, g(x) = (x-1)(x-2)(x-3), r(x) = ax^2 + bx + c$$

- ⇨ Ta có

$$f(1) = q(1)g(1) + r(1) \Leftrightarrow 1 = a + b + c \ (1)$$
$$f(2) = q(2)g(2) + r(2) \Leftrightarrow 2^{11} = 4a + 2b + c \ (2)$$
$$f(3) = q(3)g(3) + r(3) \Leftrightarrow 3^{11} = 9a + 3b + c \ (3)$$
$$(1) \wedge (2) \wedge (3) \Rightarrow \begin{cases} a = 86526 \\ b = -257531 \\ c = 171006 \end{cases}$$
$$\Rightarrow f(x) \ mod \ g(x) = 86526x^2 - 257531x + 171006$$

- ⇨ Ví dụ 2

$$f(x) = x^{10} + 5, g(x) = (x-2)^3(x+3), r(x) = ax^3 + bx^2 + cx + d$$
$$f(x) = q(x)g(x) + r(x) \Rightarrow \begin{cases} f'(x) = q'(x)g(x) + q(x)g'(x) + r'(x) \\ f''(x) = q''(x)g(x) + 2q'(x)g'(x) + q(x)g''(x) + r''(x) \end{cases}$$

- ⇨ Ta có

$$f(2) = q(2)g(2) + r(2) \Leftrightarrow 2^{10} + 5 = 8a + 4b + 2c + d \ (1)$$
$$f(-3) = q(-3)g(-3) + r(-3) \Leftrightarrow (-3)^{10} + 5 = -27a + 9b - 3c + d \ (2)$$
$$f'(2) = q'(2)g(2) + q(2)g'(2) + r'(2) \Leftrightarrow 10 \times 2^9 = 12a + 4b + c \ (3)$$
$$f''(2) = q''(2)g(2) + 2q'(2)g'(2) + q(2)g''(2) + r''(x) \Leftrightarrow$$
$$90 \times 2^8 = 12a + 2b \ (4)$$
$$(1) \wedge (2) \wedge (3) \wedge (4) \Rightarrow \begin{cases} a = 1635 \\ b = 1710 \\ c = -21340 \\ d = 23789 \end{cases}$$
$$\Rightarrow f(x) \ mod \ g(x) = 1635x^3 + 1710x^2 - 21340x + 23789$$

- ⇨

Map – Ánh Xạ:

1. Phép Đồng Cấu (Homomorphism)?

⇨ Cho nhóm (A, +) và nhóm (B, ·), khi này 1 ánh xạ f từ A tới B được gọi là 1 phép đồng cấu nếu nó thỏa mãn điều kiện

$$f(x+y) = f(x) \cdot f(y), \forall x, y \in A$$

⇨ Hệ quả, e_1 là Identity của (A, +), e_2 là Identity của (B, ·)

$$f(e_1) = e_2$$
$$f(x^{-1}) = f(x)^{-1}, \forall x \in A$$

⇨ Cho chuông (A, +, ·) và chuông (B, x, *), khi này 1 ánh xạ f từ A tới B được gọi là 1 phép đồng cấu nếu nó thỏa mãn 2 điều kiện

$$f(x+y) = f(x) \times f(y), \forall x, y \in A$$
$$f(x \cdot y) = f(x) * f(y), \forall x, y \in A$$

⇨ Cho vành (A, +, ·) và vành (B, x, *), khi này 1 ánh xạ f từ A tới B được gọi là 1 phép đồng cấu nếu nó thỏa mãn 3 điều kiện, e_1 là Identity của phép "·", e_2 là Identity của phép "*"

$$f(x+y) = f(x) \times f(y), \forall x, y \in A$$
$$f(x \cdot y) = f(x) * f(y), \forall x, y \in A$$
$$f(e_1) = e_2$$

⇨ Hệ quả, e_3 là Identity của phép "+", e_4 là Identity của phép "x", nghịch đảo của a ứng với phép "+" hoặc "x" kí hiệu là –a

$$f(e_3) = e_4$$
$$f(-x) = -f(x), \forall x \in A$$

char(A) chia hết cho char(B)

2. Nhân (Kernel)?

⇨ Xét 1 phép đồng cấu f từ A tới B, nó có thể ánh xạ nhiều phần tử trong A tới chỉ 1 phần tử trong B, khi này tập hợp các phần tử trong A được ánh xạ tới Identity của B được gọi là nhân của f, kí hiệu ker(f)

3. Phép Đẳng Cấu (Isomorphism)?

⇨ Là 1 phép đồng cấu nhưng song ánh

⇨ Kí hiệu nhóm hoặc vành A đẳng cấu với nhóm hoặc vành B

$$A \cong B$$

4. Phép Tự Đồng Cấu (Endomorphism)?

⇨ Là 1 phép đồng cấu từ nhóm hoặc vành A vào chính nó

5. Phép Tự Đẳng Cấu (Automorphism)?

⇨ Là phép tự đồng cấu nhưng song ánh

Number – Số:

1. Dãy Số Nguyên Tố?

2, 3, 5, 7, 11, …

2. Dãy Số Chính Phương (Square Number)?

0, 1, 4, 9, 16, …

3. Dãy Hợp Số (Composite Number)?

4, 6, 8, 9, 10, 12, …

4. Ước Chung Lớn Nhất Của 0 Với 1 Số?

⇨ Cho x là số tự nhiên bất kì khác 0, ta có bội chung lớn nhất giữa 0 và x = gcd(0, x) = x
⇨ gcd(0, 0) không được định nghĩa
5. Tập Hợp Các Số Tự Nhiên Có Cùng Ước Số Nguyên Tố Lớn Nhất?
⇨ Tập hợp các số tự nhiên có cùng ước chung lớn nhất là 2, là lũy thừa bậc 1 trở lên của 2, kí hiệu P_2

P_2 = 2, 4, 8, 16, 32, 64, …

⇨ Tập hợp các số tự nhiên có cùng ước chung lớn nhất là 3, là lấy dãy lũy thừa bậc 1 trở lên của 3 nhân tích Đề Các với P_2 có thêm phần tử 1 ở đầu, thay mỗi cặp (a, b) thành a nhân b, kí hiệu P_3

(3, 9, 27, 81, 273, …) x (1, 2, 4, 8, 16, 32, 64, …) =
P_3 = 3, 6, 9, 12, 18, 24, 27, 36, 48, 54, 72, 81, 96, 108, 144, 162, 192, 216, …

⇨ Tương tự, tập hợp các số tự nhiên có cùng ước chung lớn nhất là m, m là số nguyên tố, đạt được bằng cách nhân tích đề các giữa dãy lũy thừa bậc 1 trở lên của m với hợp của tất cả các dãy P_n, với n là các số nguyên tố < m, hợp này có chèn thêm phần tử 1 ở đầu, sau đó thế mỗi cặp (a, b) thành tích của chúng, kí hiệu P_m
6. Phỏng Đoán Goldbach (Goldbach’s Conjecture)?
⇨ Phỏng đoán chưa có lời giải này cho rằng mọi số chẵn > 2 đều có thể phân tích thành tổng của 2 số nguyên tố
7. Một Số Hàm Trả Về Số Nguyên Tố?

$x^2 + x + 41, x \in N, x \in [0,39]$
$x^2 - x + 41, x \in N, x \in [0,40]$

8. Túc Thừa (Tetration)?

$a \uparrow\uparrow b = a[4]b = H_4(a,b) = a^{a^{a^{\cdots^{a}}}}$

⇨ Đọc là a tức thừa b, vế phải có b số a
⇨ Nếu b = 0 thì a tức thừa b = 1
⇨ Ví dụ

$4 \uparrow\uparrow 3 = 4^{4^4}$

9. Ngũ Thừa (Pentation)?

$a \uparrow\uparrow\uparrow b = a[5]b = H_5(a,b) = a \uparrow\uparrow \left(a \uparrow\uparrow \left(a \uparrow\uparrow (a \uparrow\uparrow \cdots)\right)\right)$

⇨ Đọc là a ngũ thừa b, vế phải cùng có b số a
⇨ Nếu b = 0 thì a ngũ thừa b = 1
⇨ Ví dụ

$4[5]3 = 4 \uparrow\uparrow (4 \uparrow\uparrow 4)$

10. N Thừa?

$a \uparrow^n b = a \uparrow\uparrow\uparrow \cdots \uparrow b$

⇨ Đọc là a n thừa b, vế phải có n mũi tên
⇨ Nếu b = 0 thì a n thừa b = 1
⇨ Ví dụ

$4 \uparrow^3 2 = 4 \uparrow\uparrow\uparrow 2$

Complex Number – Số Phức:

1. Logarithm Của Số Âm?

$$ln(x) = ln(|x|) + i\pi, x < 0$$

2. Hàm Phức 1 Biến?

⇨ Để dễ hình dung, tưởng tượng hàm phức biến đổi lưới tọa độ của mặt phẳng phức

3. Mở Rộng Hàm Riemann Zeta Ra Mặt Phẳng Phức?

⇨ Xét hàm Riemann Zeta ζ(x), hàm này xác định khi và chỉ khi x là số phức với phần thực > 1

⇨ Ví dụ

$$\zeta(2 + i) = \frac{1}{1^{2+i}} + \frac{1}{2^{2+i}} + \frac{1}{3^{2+i}} + \cdots \approx 1.150356 - 0.437531i$$

⇨ Tuy nhiên, ta có thể mở rộng hàm này ra miền số phức với phần thực từ 1 trở xuống, bằng cách sử dụng đạo hàm liên tục tại những điểm có phần thực = 1

⇨ Ta có 1 số định lý sau

$$\zeta(-2n) = 0, \forall n \in N^*$$

$$\zeta(0) = -\frac{1}{2}$$

x = 1 là cực của hàm Riemann Zeta, nghĩa là hàm đạt vô cực tại điểm này

4. Giả Thuyết Riemann (Riemann Hypothesis)?

⇨ Là phỏng đoán cho rằng ngoài x là các số nguyên âm chẵn, hàm Riemann Zeta ζ(x) sẽ trả về 0 chỉ khi x có phần thực = 0.5, và các giá trị x thỏa mãn điều này có 1 mối liên hệ nào đó với phân phối của số nguyên tố

Polynomial – Đa Thức:

1. Ma Trận Sylvester (Sylvester Matrix)?

⇨ Cho 2 đa thức f(x) có bậc n > 0 và g(x) có bậc m > 0

⇨ Bước 1, khởi tạo ma trận M kích thước (n + m) x (n + m)

⇨ Bước 2, hàng đầu tiên, từ trái sang phải, lần lượt viết các hệ số của f(x) từ hệ số ứng với bậc cao nhất đến hệ số tự do, sau đó các ô còn lại điền 0

⇨ Bước 3, hàng thứ 2 = hàng 1 dịch sang phải 1 ô, hàng thứ 3 = hàng thứ 2 dịch sang phải 1 ô, …, làm cho đến hết hàng thứ m

⇨ Bước 4, hàng thứ m + 1, từ trái sang phải, lần lượt viết các hệ số của g(x) từ hệ số ứng với bậc cao nhất đến hệ số tự do, sau đó các ô còn lại điền 0

⇨ Bước 5, hàng thứ m + 2 = hàng thứ m + 1 dịch sang phải 1 ô, hàng thứ m + 3 = hàng thứ m + 2 dịch sang phải 1 ô, …, làm cho đến hết hàng thứ m + n

⇨ Cuối cùng, ta được ma trận Sylvester của f(x) với g(x), kí hiệu $S_{f,g}$

⇨ Nếu n = 0, m > 0, thì f(x) = a, a là 1 hằng số, thì ma trận Sylvester của f(x) với g(x) sẽ là ma trận đường chéo cấp m với các phần tử trên đường chéo chính đều = a

⇨ Nếu m = 0, n > 0, thì g(x) = a, a là 1 hằng số, thì ma trận Sylvester của f(x) với g(x) sẽ là ma trận đường chéo cấp n với các phần tử trên đường chéo chính đều = a

⇨ Nếu m = n = 0, thì ma trận Sylvester của f(x) với g(x) là ma trận rỗng

⇨ Ví dụ 1

$$f(x) = 3x^3 + 4x^2 + 5x + 6, g(x) = 7x^2 + 8x + 9$$

$$S_{f,g} = \begin{pmatrix} 3 & 4 & 5 & 6 & 0 \\ 0 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 0 & 0 \\ 0 & 7 & 8 & 9 & 0 \\ 0 & 0 & 7 & 8 & 9 \end{pmatrix}$$

⇨ Ví dụ 2

$f(x) = 3x^3 + 4x^2 + 5x + 6, g(x) = 9$

$$S_{f,g} = \begin{pmatrix} 9 & 0 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & 9 \end{pmatrix}$$

⇨ Ví dụ 3

$f(x) = 5, g(x) = 9$

$S_{f,g} = ()$

⇨ Cho $S_{f,g}$ là ma trận Sylvester của đa thức f(x) bất kì với đa thức g(x) bất kì, với hệ số của chúng thuộc trường (F, +, ·), ta có các định lý sau, e là Identity của nhóm (F, +)

Định thức của $S_{f,g}$ gọi là kết quả (Resultant) của f(x) với g(x), kí hiệu $Res_x(f, g)$
$Res_x(f, g)$ = e khi và chỉ khi phương trình f(x) = e và g(x) = e có ít nhất 1 nghiệm chung thuộc 1 trường mở rộng của (F, +, ·)

2. Biệt Thức (Discriminant)?

⇨ Cho đa thức f(x) bậc n với hệ số thuộc trường (F, +, ·), f'(x) là đạo hàm của f(x), a là hệ số ứng với bậc lớn nhất trong f(x), e là Identity của phép "·", –e là nghịch đảo của nó qua phép "+", a^{-1} là nghịch đảo của a qua phép "·", k = e khi n mod 4 = 0 hoặc 1, k = –e khi n mod 4 = 2 hoặc 3, khi này biệt thức của f(x) chính bằng $k \cdot a^{-1} \cdot Res_x(f, f')$, kí hiệu $Disc_x(f)$

⇨ Cho $Disc_x(f)$ là biệt thức của 1 đa thức f(x) bất kì với hệ số thuộc trường (F, +, ·), ta có các định lý sau

$Disc_x(f)$ = 0 khi và chỉ khi phương trình f(x) = 0 có nghiệm bội m > 1 trên trường mở rộng của (F, +, ·)
Nếu (F, +, ·) là trường số thực, và phương trình f(x) = 0 không có nghiệm bội m > 1 trên trường số phức, thì $Disc_x(f) > 0$ khi và chỉ khi số nghiệm không thuần thực của phương trình f(x) = 0 là bội số của 4 (0, 4, 8, 12, …), ngược lại $Disc_x(f) < 0$

⇨ Ví dụ 1

$f(x) = ax^3 + bx^2 + cx + d$

$\Rightarrow f'(x) = 3ax^2 + 2bx + c$

$$\Rightarrow S_{f,f'} = \begin{pmatrix} a & b & c & d & 0 \\ 0 & a & b & c & d \\ 3a & 2b & c & 0 & 0 \\ 0 & 3a & 2b & c & 0 \\ 0 & 0 & 3a & 2b & c \end{pmatrix}$$

$\Rightarrow Res_x(f, f') = |S_{f,f'}| = 27a^3d^2 - 18a^2bcd + 4a^2c^3 + 4ab^3d - ab^2c^2$

$\Rightarrow Disc_x(f) = -\frac{Res_x(f,f')}{a} = -27a^2d^2 + 18abcd - 4ac^3 - 4b^3d + b^2c^2$

⇨ Ví dụ 2

$f(x) = ax^2 + bx + c$

$\Rightarrow f'(x) = 2ax + b$

$$\Rightarrow S_{f,f'} = \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix}$$
$$\Rightarrow Res_x(f,f') = |S_{f,f'}| = -ab^2 + 4a^2c$$
$$\Rightarrow Disc_x(f) = -\frac{Res_x(f,f')}{a} = b^2 - 4ac$$

Quintic:

Def:

Không có công thức tổng quát dưới dạng căn thức cho phương trình bậc ≥ 5

Proof:

Gọi r_1, r_2, r_3, r_4, r_5 là 5 nghiệm thật của phương trình

$x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0 \Leftrightarrow$

$(x - r_1)(x - r_2)(x - r_3)(x - r_4)(x - r_5) = 0$

Như vậy hệ số của phương trình có thể biểu diễn bằng biểu thức của các nghiệm

Gọi công thức tổng quát

$x_1, x_2, x_3, x_4, x_5 = f(a, b, c, d, e)$

Công thức tổng quát phải thỏa mãn khi tráo đổi vị trí r thì x cũng phải tráo đổi

Giả sử công thức tổng quát không có căn thức

Từ từ tráo đổi vị trí của r bất kì, vì f là hàm chỉ trả về một kết quả và các hệ số không đổi nên f không đổi, loại

Giả sử công thức tổng quát có một căn thức bậc bất kì, dùng Commutator

Không mất tính tổng quát, tráo r_1, r_2, tráo r_2, r_3 theo chiều kim đồng hồ rồi lặp lại lần hai theo chiều ngược kim đồng hồ, kết quả các nghiệm thực bị hoán vị vì nhóm S_3 không Abelian, còn f vẫn giữ nguyên vì mỗi lần hoán vị theo chiều kim đồng hồ thì x bị hoán vị theo kiểu xoay theo chiều kim đồng hồ và ngược lại, nên tổng Phase thay đổi $= 0$, loại

Giả sử công thức tổng quát có căn thức trong căn thức

Sử dụng Commutator c_1 cho căn thức bên trong trở về ban đầu, nhưng căn thức bên ngoài có thể không trở về ban đầu nên sử dụng thêm Commutator c_2 cũng làm căn thức bên trong trở về ban đầu, nhưng đồng thời làm sao cho Commutator của c_1 và c_2 làm căn thức bên ngoài trở về ban đầu

Đối với căn thức trong căn thức trong căn thức … n lần thì chúng ta chỉ việc lấy Commutator của Commutators của Commutators … n lần và chứng minh Commutator Subgroup cuối cùng chứa những nhóm hoán vị khác Identity, do đó r có thể bị hoán vị còn x thì không, hoàn thành việc chứng minh

Với phương trình bậc 5, Commutator Subgroup của nhóm S_5 là A_5, các phần tử trong Commutator Subgroup được tạo ra bằng cách lấy Commutator của hai phần tử bất kì rồi loại bỏ trùng lặp

Commutator của A_5 lại là chính nó, do đó nếu lấy Commutator vô hạn lần thì vẫn là A_5, A_5 chứa những phần tử khác Identity, hoàn thành chứng minh

Với phương trình bậc $n \geq 5$, A_5 là Subgroup của A_n nên khi lấy Commutator, A_n vẫn luôn còn A_5, A_n có những phần tử hoán vị khác Identity, hoàn tất chứng minh