Contents

[Set – Tập Hợp: 1](#_Toc158011454)

[Magma – Groupoid: 8](#_Toc158011455)

[Semigroup: 8](#_Toc158011456)

[Monoid: 9](#_Toc158011457)

[Group – Nhóm: 9](#_Toc158011458)

[Ring – Vành: 9](#_Toc158011459)

[Field – Trường: 9](#_Toc158011460)

[Map – Ánh Xạ: 10](#_Toc158011461)

Set – Tập Hợp:

1. Kí Hiệu?

* Cho V là tập hợp gồm các phần tử nào đó
* Cách 1, liệt kê

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

* Ví dụ

1. Tập Hợp Bằng Nhau?

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

1. 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

1. 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

1. 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

1. 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

1. Tập Hữu Hạn?

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

1. Tập Lũy Thừa (Power Set)?

* Cho tập S, tập lũy thừa P(S) hay 2S là tập hợp mà mỗi phần tử là tập con của S, chứa toàn bộ tập con của S
* Ví dụ

* Nếu S có n phần tử thì P(S) có 2n phần tử

1. Dãy Sắp Thứ Tự (Ordered N Tuple)?

* Là 1 dãy số a1, a2, a, …, aN
* 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)

1. 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

* Ví dụ

1. Hợp (Union)?

* 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

1. Giao (Intersection)?

1. Hiệu (Difference)?

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

* Ví dụ

1. EX – OR?

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

1. Phần Bù (Complement)?

* Là tất cả những gì không thuộc về tập hợp

1. Công Thức Giao Hợp?

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

1. 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 (hàm) từ A đến B, khi chỉ có 2 tập hợp, thì ta gọi là quan hệ 2 ngôi (Binary Relation)
* 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

* Mệnh đề này tương đương

* 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 4 tính chất sau, R là quan hệ
* Tính phản xạ (Reflexive), (x, x) thuộc R

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

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

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

* Ví dụ xét tập sau là tập ước số trên Z+

* 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, b ⋮ a, c ⋮ b, thì đương nhiên c ⋮ a
* Các quan hệ bản chất là tập hợp, do đó chúng có thể giao hợp các thứ để tạo ra quan hệ mới

1. Quan Hệ Hợp (Composition Relation)?

* Bản chất quan hệ = hàm, nhưng bây giờ 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

* 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

* Giống như hàm thông thường, quan hệ hợp có tính kết hợp

1. Quan Hệ Đường Chéo (Diagonal Relation)?

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

1. Quan Hệ Ngược (Inverse Relation)?

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

1. Quan Hệ Mũ (Power Of Relation)?

* Cho quan hệ R, khi đó Rn = n hàm R hợp lồng lên nhau, ví dụ

1. 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 phải
* 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

1. 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



1. 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

* Bao đóng đối xứng

* Bao đóng bắc cầu

1. 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
* 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, 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

1. 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

* 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

* 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

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

* Giống y chang quan hệ tương đương, chỉ khác là không có tính đối xứng, nhưng có tính phản đối xứng
* 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

1. So Sánh Được (Comparability)?

* Cho 1 quan hệ có thứ tự bộ phận R trên tập A
* Nếu chỉ cần (a, b) hoặc (b, a) thuộc R, ta nói a và b có thể so sánh được với nhau, cụ thể nếu (a, b) và (b, a) cùng thuộc R, thì a = b, nếu chỉ có (a, b) thì

a < b, nếu chỉ có (b, a), thì b > a, lưu ý ở đây các dấu chỉ là quy ước, dựa vào đây, ta nói cực đại của Poset ứng với A và R là giá trị m sao cho không tồn tại x trong A khác m, để (m, x) thuộc R và (x, m) không thuộc R, tương tự cực tiểu là giá trị n sao cho không tồn tại x trong A khác n, để (x, n) thuộc R và (n, x) không thuộc R, giá trị lớn nhất của Poset này là giá trị g sao cho mọi (x, g), x là giá trị bất kì trong A, đều thuộc R, tương tự giá trị nhỏ nhất của Poset này là giá trị l sao cho mọi (l, x), x là giá trị bất kì trong A, đều thuộc R, mỗi Poset chỉ có 1 g và 1 l

* Nếu cả 2 cùng không thuộc R, ta nói chúng không thể so sánh được với nhau
* Ví dụ nếu quan hệ R là quan hệ a chia hết b, thì 3 và 6 có thể so sánh với nhau, vì (6, 3) thuộc R, hay 6 và 6 cũng có thể so sánh với nhau, do (6, 6) thuộc R, nhưng 2 không thể so sánh với 5, do (2, 5) và (5, 2) không thuộc R

1. Quan Hệ Có Thứ Tự Toàn Phần (Totally Order Relation)?

* 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

1. Cận Trên Và Cận Dưới?

* Cho 1 Poset (S, R), ta có A là tập con của S, xét Poset (A, R)
* Nếu tồn tại một phần tử u trong S, sao cho (x, u) tồn tại trong R với mọi x trong A, thì u gọi là cận trên của Poset (A, R)
* Tương tự nếu tồn tại một phần tử l trong S, sao cho (l, x) tồn tại trong R với mọi x trong A, thì l gọi là cận dưới của Poset (A, R)

1. 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

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

Semigroup:

1. Semigroup?

* Là 1 Magma (S, ⋅) kèm theo điều kiện sau

Monoid:

1. Monoid?

* Là 1 Semigroup (S, ⋅) kèm theo điều kiện sau

* 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

* 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

1. Nhóm Giao Hoán (Abelian Group)?

* Là 1 nhóm (A, ⋅) kèm theo điều kiện sau

1. Bậc (Order) Của 1 Nhóm?

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

1. 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 ≤ G

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

1. Nhóm Tầm Thường (Trivial Group)?

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

1. Nhóm Nhị Diện (Dihedral Group)?

* Cho 1 nhóm (D, ⋅) gồm 2n phần tử, n là số nguyên dương, các phần tử lần lượt là ri và si, i chạy từ 1 đến n, nhóm này sẽ được gọi là nhóm nhị diện và được kí hiệu là Dn nếu nó thỏa mãn bảng sau

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | r1 | r2 | r3 | … | rn | s1 | s2 | s3 | … | sn |
| r1 | r1 | r2 | r3 | … | rn | s1 | s2 | s3 | … | sn |
| r2 | r2 | r3 | r4 | ... | r1 | s2 | s3 | s4 | ... | s1 |
| r3 | r3 | r4 | r5 | … | r2 | s3 | s4 | s5 | … | s2 |
| … | … | … | … | … | … | … | … | … | … | … |
| rn | rn | r1 | r2 | … | rn – 1 | sn | s1 | s2 | … | sn – 1 |
| s1 | s1 | sn | sn – 1 | … | s2 | r1 | rn | rn – 1 | … | r2 |
| s2 | s2 | s1 | sn | … | s3 | r2 | r1 | rn | … | r3 |
| s3 | s3 | s2 | s1 | … | s4 | r3 | r2 | r1 | … | r4 |
| … | … | … | … | … | … | … | … | … | … | … |
| sn | sn | sn – 1 | sn – 2 | … | s1 | rn | rn – 1 | rn – 2 | … | r1 |

* 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 r3 ⋅ r2 = r4
* 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 ri tương ứng với phép quay ngược chiều kim đồng hồ 360 / n \* (i – 1) độ
* Phần tử si 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 D3

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | r1 | r2 | r3 | s1 | s2 | s3 |
| r1 | r1 | r2 | r3 | s1 | s2 | s3 |
| r2 | r2 | r3 | r1 | s2 | s3 | s1 |
| r3 | r3 | r1 | r2 | s3 | s1 | s2 |
| s1 | s1 | s3 | s2 | r1 | r3 | r2 |
| s2 | s2 | s1 | s3 | r2 | r1 | r3 |
| s3 | s3 | s2 | s1 | r3 | r2 | r1 |

* Là nhóm quay và Flip tam giác đều
* Dn là nhóm con của Dm khi và chỉ khi m chia hết cho n

1. 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

1. 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, ⋅)

1. 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

1. Nhóm Đối Xứng (Symmetric Group)?

* Là 1 nhóm (S, ⋅) có n! phần tử, thường kí hiệu Sn, 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 Sn là 1 nhóm đối xứng bất kì, ta có các định lý sau

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

1. 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

1. Nhóm Thay Thế (Alternating Group)?

* Là 1 nhóm (A, ⋅) có n! / 2 phần tử, thường kí hiệu An, 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 An là 1 nhóm thay thế bất kì, ta có các định lý sau

An là nhóm giao hoán khi và chỉ khi n ≤ 3

An là nhóm đơn giản khi và chỉ khi n = 3 hoặc n ≥ 5

An là nhóm con không tầm thường lớn nhất của Sn

1. 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〉

1. 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 xn = Identity, kí hiệu bậc của x là |x|, nếu không tồn tại n thì |x| = vô cực

1. 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

1. Nhóm Tuần Hoàn (Cyclic Group)?

* Cho 1 nhóm (C, ⋅) gồm n phần tử, n là số nguyên dương, các phần tử kí hiệu là ri, i chạy từ 1 đến n, nhóm này sẽ được gọi là nhóm tuần hoàn và được kí hiệu là Cn hoặc Zn nếu nó thỏa mãn bảng sau

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | r1 | r2 | r3 | … | rn |
| r1 | r1 | r2 | r3 | … | rn |
| r2 | r2 | r3 | r4 | ... | r1 |
| r3 | r3 | r4 | r5 | … | r2 |
| … | … | … | … | … | … |
| rn | rn | r1 | r2 | … | rn – 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 r3 ⋅ r2 = r4
* 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

1. Commutator?

* Cho 1 nhóm (G, ⋅), a và b là 2 phần tử bất kì trong nó, khi này Commutator của a với b là

* Ta có các định lý sau, cho e là Identity của (G, ⋅)

1. Nhóm Con Commutator (Commutator Subgroup)?

* Cho 1 nhóm (G, ⋅), tập S là tập chứa toàn bộ các Commutator của nhóm này

* Khi này 〈S〉 được gọi là nhóm con Commutator của (G, ⋅)

1. 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 ⋅ N) ⋅ (b ⋅ N) = (a ⋅ b) ⋅ 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 Sn / An đẳng cấu với nhóm tuần hoàn C2

Nhóm thương G / {e}, e là Identity của (G, ⋅), đẳng cấu với (G, ⋅)

Nhóm thương G / G, đẳng cấu với nhóm tầm thường

1. 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

Gk / Gk – 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, ⋅)

* Ví dụ
* Nhóm đối xứng S5 là nhóm không thể giải vì nó chỉ có duy nhất 1 nhóm con bình thường không tầm thường là A5, mà nhóm thương A5 / {e} lại không phải nhóm giao hoán, e là Identity của S5
* Ta có 1 số định lý sau

Nhóm Sn 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

Ring – Vành:

1. Vành?

* Là 1 chuông (R, +, ⋅), chỉ khác ở chỗ (R, ⋅) phải là 1 Monoid

1. Vành Giao Hoán (Commutative Ring)?

* Là 1 vành (R, +, ⋅) kèm theo điều kiện sau

1. Một Số Vành Thường Gặp?

* Tập hợp số hữu tỉ với phép cộng và nhân
* Tập hợp số thực với phép cộng và nhân

1. 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

1. 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

1. 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

1. 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)

1. 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

1. 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

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

* Là 1 vành (R, +, ⋅) kèm theo các điều kiện sau

Identity e1 của nhóm (R, +) phải khác Identity e2 của Monoid (R, ⋅)

Field – Trường:

1. Trường?

* Là 1 vành (F, +, ⋅) vừa là vành giao hoán, vừa là vành chia

1. Một Số Trường Thường Gặp?

* Tập hợp số thực với phép cộng và nhân

1. 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

1. 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 xn = 1, với n bất kì, thì Q(S) còn gọi là trường Cyclotomic

1. Phép Mở Rộng Cyclotomic?

* Là phép mở rộng có dạng F(S) / F, với S là 1 nghiệm phức của phương trình

xn = 1, với n bất kì

1. 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

1. 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 an = một số nào đó trong K
* Ví dụ sau đây là phép mở rộng căn, Q là tập số hữu tỉ

1. 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

1. 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

1. 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

1. 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

1. 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

1. 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

1. 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)

1. 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

1. 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

1. 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

1. 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 Sn, 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

1. Phép Mở Rộng Kummer (Kummer Extension)?

* Là phép mở rộng F / N, sao cho N chứa tập nghiệm phức của phương trình

xn = 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

1. 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 GLn(F)

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

* Cho nhóm tuyến tính tổng quát GLn(F), gọi e là Identity của phép nhân của trường hoặc vành F, khi này nhóm con của GLn(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 SLn(F)

1. 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

* Ta có

* Ví dụ 2

* Ta có

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

* Hệ quả, e1 là Identity của (A, +), e2 là Identity của (B, ⋅)

* 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

* 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, e1 là Identity của phép “⋅”, e2 là Identity của phép “\*”

* Hệ quả, e3 là Identity của phép “+”, e4 là Identity của phép “x”, nghịch đảo của a ứng với phép “+” hoặc “x” kí hiệu là –a

char(A) chia hết cho char(B)

1. 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)

1. 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

1. Phép Tự Đồng Cấu (Endomorphism)?

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

1. Phép Tự Đẳng Cấu (Automorphism)?

* Là phép tự đồng cấu nhưng song ánh

Quintic:

Def:

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

Proof:

Gọi là 5 nghiệm thật của phương trình

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

nghiệm

Gọi công thức tổng quát

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

đổi

Giả sử công thức tổng quát không có căn thức

Từ từ tráo đổi vị trí của bất kì, vì là hàm chỉ trả về một kết quả và các hệ

số không đổi nên không đổi, loại

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

Không mất tính tổng quát, tráo , tráo 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 không Abelian, còn vẫn giữ nguyên vì mỗi lần hoán vị

theo chiều kim đồng hồ thì bị hoán vị theo kiểu xoay theo chiều kim đồng

hồ và ngược lại, nên tổng Phase thay đổi , loại

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

Sử dụng Commutator 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

cũng làm căn thức bên trong trở về ban đầu, nhưng đồng thời làm sao cho

Commutator của và làm căn thức bên ngoài trở về ban đầu

Đối với căn thức trong căn thức trong căn thức … lần thì chúng ta chỉ việc

lấy Commutator của Commutators của Commutators … lần và chứng minh

Commutator Subgroup cuối cùng chứa những nhóm hoán vị khác Identity, do

đó có thể bị hoán vị còn thì không, hoàn thành việc chứng minh

Với phương trình bậc , Commutator Subgroup của nhóm là , 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 lại là chính nó, do đó nếu lấy Commutator vô hạn lần thì

vẫn là , chứa những phần tử khác Identity, hoàn thành chứng minh

Với phương trình bậc , là Subgroup của nên khi lấy

Commutator, vẫn luôn còn , có những phần tử hoán vị khác

Identity, hoàn tất chứng minh