Date: . . No:

*Nhóm

- Nhóm là tập hợp G với phép toán nhân nếu thoả mãn với mọi ptử a, b, c thuộc G
  + Tính kết hợp $(a.b).c = a.(b.c)$
  + Có pt đơn vị e: $e.a = a.e = a$
  + Có nghịch đảo (a^{-1}): $a.a^{-1} = e$
  + Nếu có thêm tính giao hoán $a.b = b.a$ gọi là Nhóm Aben hay nhóm giao hoán
- Nhóm Xyelic
  + Định nghĩa luỹ thừa như là việc áp dụng lập phép toán
  + Đơn vị: $e = a^0$
  + Nếu mọi ptử đều là luỹ thừa của 1 ptử nào đó. VD: $b = a^k$ đối với a có tính và b trong nhóm. Khi đó a gọi là ptử sinh của nhóm
  VD: tập số nguyên Z

* Vành

- Cho 1 tập $R \neq \emptyset$ với phép toán 2 ngôi $(+, *)$ để gọi là vành nếu
  + Với phép cộng R là nhóm Aben
  + Với phép nhân, có: - tính đóng và tính kết hợp
    - tính phân phối vs phép cộng
  + Nếu phép nhân có tính giao hoán thì tạo thành vành giao hoán
  + Nếu phép nhân có nghịch đảo và không có ước của 0 (tức là không có 2 ptử 0 mà tích của chúng lại bằng 0) thì tạo thành

Date: . . No:

miền nguyên

VD:

+ Tập hợp các số nguyên với phép (+) và (*) thông thường là 1 vành

+ Tập hợp ma trận vuông cùng cấp n (n×n) với phép cộng và phép nhân ma trận là 1 vành

* Trường

– là 1 tập hợp F với hai phép toán là phép cộng và phép nhân, thoả mãn tính chất

+ F là 1 vành

+ Với phép nhân F trừ phần tử 0 là nhóm Abel nhân, của số khác 0. Phép trừ được xem là phép cộng với số đối của phép cộng và phép chia là phép nhân với nghịch đảo của phép nhân

– Tính chất: cho a, b, c là n° phần tử ∈ F

+ Tính kết hợp (+) và (*)

$a + (b+c) = (a+b) + c$

$a.(bc) = (ab).c$

+ Tính giao hoán của (+) và (*)

$a+b = b+a$; $ab = ba$

+ Phần tử cộng và phần tử nhân: tồn tại 2 phần tử khác nhau 0 và 1 ∈ F sao cho:

~~a ≠ 0~~ $a+0 = a$ và $a.1 = a$

+ Nghịch đảo phép cộng: $a + (-a) = 0$

+ Nghịch đảo phép nhân: $a.a^{-1} = 1$

+ Tính phân phối $a.(b+c) = ab + ac$

Date: . . No:

VD:

Số hữu tỉ

$$\frac{b}{a} \cdot \frac{a}{b} = \frac{ba}{ab} = 1 \quad (a, b \neq 0)$$

(*) Trường hữu hạn

- Là trường hữu hạn số phử, số này gọi là bậc của trường đó

VD: Trường $\mathbb{F}_4$ có 4 phử, trường $\mathbb{Z}_2$ là trường nhỏ nhất (do theo định nghĩa phải có ít nhất 2 phử phbiệt $\neq 1, 0$)

- THH đơn giản I' với lời là số ngtố có thể xdựng trên số học modulo với 1 số nguyên dương n cho trước, số học "modulo n" nghĩa là làm việc với các số:

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$$

- Phép cộng và phép nhân thực hiện trên tập $\mathbb{Z}$ chia cho n rồi lấy số dư là Kp cuối cùng tạo nhận 1 trường khi và chỉ khi n là 1 số nguyên tố

- Mọi THH F có $q = p^n$ phử, với p là số ngtố và $n \neq 1$. Điều này có thể suy ra từ việc xem trường F là 1 không gian vectơ trên trường ngtố của nó

- Một trường với $q = p^n$ phử có thể xdựng từ trường phân rã đa thức

$$f(x) = x^4 - x$$

- Một trường phân rã như thế là 1 mở rộng

KI.ONG

của F_p trong đó đa thức F có q nghiệm. Điều này có nghĩa F có nhiều nghiệm nhất có thể do bậc của F là q. Với $q = 2^2 = 4$, có thể kiểm tra bằng tính toán rằng cả 4 phần tử của F_4 thoả $x^4 = x$, vậy nên chúng đều là nghiệm của F. Mặt khác F_2, F chỉ có 2 nghiệm (0,1) nên F không phân rã ra thừa số bậc nhất trong trường này. Sử dụng khái niệm khác trong lí thuyết này

⊛ Xây dựng trường từ vành (Ideal)

— Một vành giao hoán là 1 tập hợp, cùng với phép toán cộng và nhân, thoả mãn tất cả tiên đề của trường. Ngoại trừ việc nghịch đảo phép nhân a^{-1}

VD: tập $\mathbb{Z}$ tạo thành vành giao hoán nhưng không phải 1 trường, nghịch đảo của 1 số nguyên n không phải là 1 số nguyên trừ khi $n = \pm 1$

— Trường có thể coi là vành giao hoán R mà trong đó bất kì phần tử $\neq 0$ nào là đơn vị (nghĩa là chúng khả nghịch). Trường cũng là vành giao hoán mà trong đó (0) là ideal ngặt duy nhất

— Ideal: đối với 1 vành tuỳ ý $(R, +, *)$ là nhóm cộng nên của nó, 1 tập hợp con để gọi là ideal đơn vị

Date: . . No:

- Một ideal khác 0 và 1 gọi là 1 ideal thích thực
- Các số chẵn tạo thành ideal của vành số nguyên $\mathbb{Z}$, nó ký hiệu là $2\mathbb{Z}$, tương tự các bội số nguyên n thì ký hiệu là $n\mathbb{Z}$
- Tập hợp các đa thức chia hết cho x^2+1 là 1 ideal chính của vành đa thức
- Tập hợp các ma trận $n \times n$ với hàng dưới cùng bằng 0 là 1 ideal phải của vành ma trận. Nó không phải là ideal trái
- Vành $C(\mathbb{R})$ các hàm liên tục f từ $\mathbb{R} \to \mathbb{R}$ chứa ideal các hàm f sao cho $f(x)=0$ (ideal các hàm số triệt tiêu tại 1, đây là 1 ideal tối đại).