A2 MỘT SỐ CẤU TRÚC ĐẠI SỐ

CẤU TRÚC ĐẠI SỐ

Phép toán 2-ngôi

Cho tập $A \neq \emptyset$, và phép toán 2-ngôi $\otimes$ xác định trên A^2:

$\otimes: A \times A \to A$.

Tập A được trang bị bởi phép toán $\otimes$, ký hiệu $(A, \otimes)$, được gọi là một cấu trúc đại số.

Hơn nữa:

. $a \otimes b = b \otimes a, \forall a, b \in A$, thì $\otimes$ có tính giao hoán.

. $a \otimes (b \otimes c) = (a \otimes b) \otimes c, \forall a, b, c \in A$, thì $\otimes$ có tính kết hợp.

. Nếu có $e \in A$: $a \otimes e = a = e \otimes a, \forall a \in A$, thì $(A, \otimes)$ có phần tử đơn vị.

NHÓM VÀ NHÓM CON

Cấu trúc nhóm

Cấu trúc (G, *) là nhóm (group) nếu phép toán 2-ngôi * có các tính chất:

(1) Tính kết hợp: $x * (y * z) = (x * y) * z, \forall x, y, z \in G$.

(2) Có phần tử đơn vị: $\exists e \in G: x * e = x = e * x, \forall x \in G$.

(3) Khả đảo: $\forall x \in G, \exists x^{-1} \in G: x * x^{-1} = e = x^{-1} * x$. x^{-1} được gọi là phần tử nghịch đảo của x.

Có thể chứng minh rằng

. Phần tử đơn vị là duy nhất, và

. $(x^{-1})^{-1} = x$.

Xét nhóm (G, *) và phần tử $a \in G$, ký hiệu:

. $a^n = a * a * \ldots * a$ (n lần a bên vế phải).

. $a^0 = e$.

Ta có

. $a^{-m} = (a^m)^{-1}$, và

. $a^{m+n} = a^m * a^n$.

Nhóm con

Cho nhóm (G, *). G_1 là tập con của G. (G_1, *) được gọi là nhóm con của (G, *), ký hiệu $G_1 \leq G$, nếu G_1 cũng là nhóm với cùng phần tử đơn vị và cùng phép toán * của G.

Nhóm và nhóm con có quan hệ về số phần tử qua định lý Lagrange.

Định lý (Lagrange).

Giả sử G là nhóm hữu hạn và H ≤ G. Ta có số phần tử của H, ký hiệu |H|, là ước của |G|.

Nhóm sinh

Xét nhóm (G, *) và A là tập con khác rỗng của G.

. Nhóm con sinh bởi A, ký hiệu <A>, là nhóm con nhỏ nhất của G chứa tập A.

. Nếu A chỉ có 1 phân tử, A = {x} thì <A> = <x> được gọi là nhóm đơn sinh hay nhóm tuần hoàn (cyclic).

Nhóm đơn sinh

Nhóm (G, *) được gọi là nhóm đơn sinh nếu có một a ∈ G sao cho <a> = G.

Khi ấy, mọi phần tử của G đều có thể viết dưới dạng a^m với một $m \in \mathbb{Z}$.

Cho nhóm (G, *) và phần tử a ∈ G. Nếu nhóm <a> hữu han thì ta gọi số phần tử của <a> là cấp của a, ký hiệu ord(a), và là số nguyên dương m nhỏ nhất sao cho a^m = e là phần tử đơn vị của G.

VÀNH, MIỀN NGUYÊN, TRƯỜNG

Cấu trúc vành

Trên tập hợp R khác rỗng, có trang bị 2 phép toán 2-ngôi * và +.

Cấu trúc (R, +, *) được gọi là vành nếu

. (R, +) là nhóm giáo hoán (phép + có tính giao hoán), có phần tử đơn vị, ký hiệu là 0.

. Phép * có tính kết hợp.

. Phép * có tính phân phối với phép cộng: x * (y + z) = x * y + x* z và (x + y) * z = x * z + y * z, ∀x, y, z ∈ R.

Xét vành (R, +, *). Nếu

. Phép * có tính giao hoán, thì R được gọi là vành giao hoán.

. Phép nhân * có phần tử đơn vi, ký hiệu là 1, thì R được gọi là vành có đơn vị.

Miền nguyên

Một vành giao hoán (R, +, *), có đơn vị 1 ≠ 0, được gọi là mien nguyên nếu có them tính chất:

∀x, y ∈ R, nếu x * y = 0 thì x = 0 hay y = 0.

Chẳng hạn, $\mathbb{Z}$ với hai phép + và * thông thường là vành. Hơn nữa,

Với mọi số nguyên tố p, $\mathbb{Z}_p$ với hai phép + (mod p) và * (mod p) là một miền nguyên.

Vành chia và trường

Vành chia (division ring) và trường (field) là hai cấu trúc có chú ý đến tính khả nghịch của các phần tử khác 0. Và được định nghĩa như sau.

. Vanh chia (R, +, *) có đơn vị $1 \neq 0$, nếu mọi phần tử khác 0 đều khả nghịch.

. Trường là một vành chia giao hoán (phép nhân * có tính giao hoán).

Ta có các kết quả sau:

. Mọi miền nguyên hữu hạn đều là trường.

. $\mathbb{Z}_p$ là trường nếu chỉ nếu p là số nguyên tố.

. Mọi vành chia hữu hạn đều là trường.

Đặc số nguyên tố của trường

Giả sử F là trường với $1 \in$ F. Với mọi số nguyên dương n, ta định nghĩa

T(n) = 1 + … + 1 (n lần), ký hiệu, $T(n) = \sum_{i=1}^{n} 1$.

Với mọi số nguyên dương m và n, ta luôn có

. T(m + n) = T(m) + T(n) ; nếu m > n thì T(m – n) = T(m) – T(n).

. T(m*n) = T(m)*T(n).

Ký hiệu 0 và 1 lần lượt là 2 phần tử đơn vị theo phép + và *. Có 2 trường hợp xảy ra:

. Trường hợp 1: tồn tại số nguyên dương n sao cho n * 1 = 0.

. Trường hợp 2: với mọi số nguyên dương n, n * 1 ≠ 0.

Mọi trường F chỉ thuộc trường hợp 1 hay trường hợp 2.

. Nếu F thuộc trường hợp 1, ta nói F là trường hữu hạn. Ví dụ $\mathbb{Z}_3$, ta có $3 * 1 \equiv 1 + 1 + 1 \equiv 0 \pmod 3$.

. Nếu F thuộc trường hợp 2, ta nói F là trường không hữu hạn. Ví dụ, $\mathbb{Z}$.

Trong trường hữu hạn F. Gọi p là là số nguyên dương nhỏ nhất thỏa p * 1 = 0. Thì

. p được gọi là đặc trưng hay đặc số của F.

. p luôn tốn tại nếu F là trượng hữu hạn.

Ta có kết quả sau:

. F là trường có đặc số p nguyên dương, thì p là số nguyên tố.

. Mọi trường hữu hạn luôn có đặc số và đặc số này là số nguyên tố.

TRƯỜNG HỮU HẠN

Trước hết, ta biết rằng mọi trường hữu hạn luôn có đặc số nguyên tố p. Gọi q là số phần tử của trường hữu hạn F, ta ký hiệu

F = GL(q) – Galois fields.

Khi ấy,

Với mọi $a \in GL(q) \setminus \{0\}$, ta luôn có $a^{q-1} = 1$.

Định lý sau đặc trưng hóa cấu trúc của một trường hữu hạn bất kỳ.

Định lý. Giả sử GF(q) là trường hữu hạn với đặc số nguyên tố p và trường con F_p của GF(q) được xây dựng theo

$F_p = \{T(m) = \sum_{i=1}^{m} 1 : m \in \mathbb{Z}\}$. Ta có,

. Tồn tại số nguyên dương m và $a_1, \ldots, a_m \in GL(q)$ thỏa mã các điều kiện

- Mọi phân tử $a \in GF(q)$ đều có thể biểu diễn dạng $a = \alpha_1 a_1 + \alpha_m a_m$ trong đó $\alpha_1, \ldots, \alpha_m \in F_q$.

- Với mỗi $k \in \{1, \ldots, m\}$, đặt $A_k = \{ \alpha_1 a_1 + \alpha_k a_k$ sao cho $\alpha_1, \ldots, \alpha_k \in F_p\}$, thì $a_{k+1} \notin A_k$, với mọi $k = 1, \ldots, m - 1$.

- Nếu $\alpha_1 a_1 + \alpha_m a_m = \beta_1 a_1 + \ldots + \beta_m a_m$, với $\alpha_k, \beta_k \in F_p$, với $k \in \{1, \ldots, m\}$ thì $\alpha_k = \beta_k$.

. Trường GF(q) có đúng p^m phần tử, tức là $q = p^m$.

Xét trường $GF(p^m)$ với đặc số nguyên tố p.

. Mọi phần tử khác 0 đều là nghiệm đa thức $x^{p^m-1} - 1$.

.Tập các phần tử của $GF(p^m)$ là tập nghiệm của đa thức $x^{p^m} - x$.

. Nếu p = 2, tập các phần tử $GF(2^m)$ là tập nghiệm của đa thức $x^{2^m} - x$.

Cuối cùng, ta có

Giả sử $GF(p^m)$ là trường hữu hạn với đặc số nguyên tố p. Gọi $F^* = GF(p^m) \setminus \{0\}$, thì F^* là nhóm đơn sinh.