ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

TÀI LIỆU BÀI GIẢNG

ĐẠI SỐ HIỆN ĐẠI

Giảng viên: TS. Trịnh Thanh Đèo
Khoa Toán – Tin học
Trường Đại học Khoa học tự nhiên
Đại học Quốc gia Thành phố Hồ Chí Minh

LƯU HÀNH NỘI BỘ

Chương 1

LÝ THUYẾT NHÓM

Giảng viên: **TS. TRỊNH THANH ĐÈO**

Khoa Toán - Tin học
Trường Đại học Khoa học Tự nhiên, ĐHQG-HCM

NỘI DUNG

§1. Nhóm và đồng cấu nhóm

Nhóm

Cho G là một tập khác rỗng và $*$ là một phép toán trên G. Khi đó, G được gọi là một *nhóm* với phép toán $*$ (hay $(G,*)$ là một nhóm) nếu các tính chất sau được thỏa mãn:
(G1) Với mọi $a,b \in G$, $a*b \in G$ (tính đóng).
(G2) Với mọi $a,b,c \in G$, $(a*b)*c = a*(b*c)$ (tính kết hợp).
(G3) Tồn tại $e \in G$, sao cho $\forall a \in G,\ a*e = e*a = a$.
(G4) Với mỗi $a \in G$, tồn tại $a' \in G$, sao cho $a*a' = a'*a = e$.

- Nếu $\forall a,b \in G,\ a*b = b*a$, thì ta nói G là nhóm *giao hoán* hay nhóm *aben*.
- Nếu G có hữu hạn phần tử thì ta nói G là *nhóm hữu hạn* và số phần tử của G được gọi là *cấp* của G, ký hiệu bởi $|G|$; nếu G có vô hạn phần tử thì ta nói G là *nhóm vô hạn* (hay *nhóm có cấp vô hạn*) và ta ký hiệu $|G| = \infty$.

§1. Nhóm và đồng cấu nhóm

Nhận xét

Dễ dàng chứng minh rằng, nếu G là một nhóm thì:
- Phần tử e trong tính chất (G3) là duy nhất, gọi là *phần tử trung hòa* hay *phần tử đơn vị* của G. Ta cũng thường ký hiệu e bởi 1.
- Với mỗi $a \in G$, phần tử a' trong tính chất (G4) là duy nhất, gọi là *phần tử nghịch đảo* của a, ký hiệu là a^{-1}, và rõ ràng $(a^{-1})^{-1} = a$.

Dưới đây, nếu không nói gì thêm thì vai trò của $*$ được hiểu là phép toán nhân. Hơn nữa, ký hiệu ab được thay cho $a*b$.

§1. Nhóm và đồng cấu nhóm

Ví dụ 1

Tập $M_{m\times n}(\mathbb{R})$ các ma trận loại $m \times n$ trên $\mathbb{R}$ là một nhóm aben với phép cộng ma trận.

Ví dụ 2

Tập $GL_n(\mathbb{R})$ các ma trận khả nghịch cấp n trên $\mathbb{R}$ là một nhóm (không aben) với phép nhân ma trận, gọi là *nhóm tuyến tính tổng quát* bậc n trên $\mathbb{R}$.

Ví dụ 3

Cho X là một tập khác rỗng. Đặt S_X là tập tất cả các song ánh từ X vào X. Khi đó S_X là một nhóm với phép hợp ánh xạ, gọi là *nhóm đối xứng* trên X. Nếu X là tập gồm n phần tử thì S_X gọi là *nhóm đối xứng* bậc n, ký hiệu bởi S_n.

§1. Nhóm và đồng cấu nhóm

Lũy thừa

Giả sử G là một nhóm với phần tử đơn vị e. Với mỗi $a \in G$, *lũy thừa* n của a (ký hiệu a^n) được xác định bằng quy nạp theo n như sau:

$$a^0 = e, a^1 = a, \text{ và với mọi } n \in \mathbb{N},\ a^{n+1} = a^n.a.$$

Lũy thừa âm của a được ký hiệu là: $a^{-n} = (a^{-1})^n,\ n \in \mathbb{N}$.

Dễ dàng chứng minh rằng, với mọi $m, n \in \mathbb{Z}$ ta có $a^m a^n = a^{m+n}$ và $(a^m)^n = a^{mn}$.

§1. Nhóm và đồng cấu nhóm

Cấp của một phần tử

Cho G là một nhóm và $a \in G$.
- Nếu tồn tại n nguyên dương sao cho $a^n = e$ thì số nguyên dương n nhỏ nhất thỏa mãn điều kiện trên gọi là *cấp* của a, ký hiệu $|a| = n$.
- Nếu không tồn tại n nguyên dương sao cho $a^n = e$ thì ta nói a có *cấp vô hạn*, ký hiệu $|a| = \infty$.

Phần tử xoắn và không xoắn

Cho G là nhóm và $e \neq a \in G$. Nếu a có cấp hữu hạn thì ta nói a là *phần tử xoắn*, nếu a có cấp vô hạn thì ta nói a là *phần tử không xoắn*.

§1. Nhóm và đồng cấu nhóm

Nhóm con

Cho G là nhóm và H là tập hợp con khác rỗng của G.
- Nếu $\forall a, b \in H, a^{-1}b \in H$ thì ta nói H là *nhóm con* của G, ký hiệu $H \leq G$.
- Nếu H là nhóm con của G và $H \neq G$ thì ta nói H là *nhóm con thực sự* của G. Khi đó ta ký hiệu $H < G$ hay $H \lneqq G$.

Rõ ràng, nếu H là nhóm con của G thì H cũng là nhóm với phép toán đã được trang bị trên G, và phần tử đơn vị của G cũng chính là phần tử đơn vị của H.

Ví dụ 4

Các tập hợp $\mathbb{Z}, \mathbb{Q}$ là nhóm con của $\mathbb{R}$ với phép toán cộng thông thường.

§1. Nhóm và đồng cấu nhóm

Ví dụ 5

Đặt $SL_n(\mathbb{R})$ là tập hợp tất cả các ma trận cấp n trên $\mathbb{R}$ có định thức bằng 1. Khi đó $SL_n(\mathbb{R})$ là một nhóm con của $GL_n(\mathbb{R})$ (với phép toán nhân ma trận), nhóm này được gọi là *nhóm tuyến tính đặc biệt* bậc n trên $\mathbb{R}$.

Ví dụ 6

Các nhóm con của S_n được gọi là các *nhóm hoán vị* bậc n.

Mệnh đề 1

Cho G là một nhóm. Khi đó, giao của một họ các nhóm con của G cũng là một nhóm con của G.

§1. Nhóm và đồng cấu nhóm

Nhóm con sinh bởi một tập hợp

Cho G là một nhóm và $\emptyset \neq S \subseteq G$. Khi đó giao của tất cả các nhóm con của G chứa S được gọi là *nhóm con sinh bởi tập hợp* S, ký hiệu là $\langle S \rangle$.

- Hiển nhiên $\langle S \rangle$ là nhóm con nhỏ nhất của G chứa tập S.
- Nếu $\langle S \rangle = G$ thì S được gọi là một *tập sinh* của G.
- Nếu G có một tập sinh chỉ gồm 1 phần tử thì ta nói G là nhóm *đơn sinh* hay nhóm *cyclic*.

Định lý 2

Cho G là một nhóm và S là tập con khác rỗng của G. Khi đó:
$$\langle S\rangle = \{a_1^{n_1}...\, a_k^{n_k} | a_i \in S, n_i \in \mathbb{Z}\}.$$

Chứng minh

Đặt H là tập hợp ở vế phải trong đẳng thức trên. Dễ thấy H kín đối với phép toán nhân và phép lấy nghịch đảo nên H là nhóm con của G. Vì vậy, mọi nhóm con của G chứa S đều chứa H. Do đó H chính là nhóm con nhỏ nhất của G chứa S, hay theo nhận xét ở trên thì $H = \langle S\rangle$.

Trong nhiều trường hợp, đối với nhóm aben, phép cộng "$+$" được thay cho phép nhân ".". Khi đó, có một số thay đổi về ký hiệu và tên gọi như sau:

Nhóm $(G,.)$	**Nhóm** $(G,+)$
tích của a với b: ab	tổng của a với b: $a+b$
phần tử đơn vị: $e;1$	phần tử không: 0
phần tử nghịch đảo của a: a^{-1}	phần tử đối của a: $-a$
lũy thừa bậc n của a: a^n	n lần a: na

Lớp kề

Cho G là một nhóm, H là nhóm con của G và $a \in G$. Đặt:
$$aH = \{ah |\ h \in H\} \quad \text{và} \quad Ha = \{ha |\ h \in H\}.$$
Ta gọi aH là *lớp kề trái* và Ha là *lớp kề phải* của G theo nhóm con H.

Mệnh đề 3

Cho G là nhóm, H là nhóm con của G và $a, b \in G$. Khi đó:
i) $aH = bH \Leftrightarrow b^{-1}a \in H$. Tương tự, $Ha = Hb \Leftrightarrow ab^{-1} \in H$.
ii) Hai lớp kề trái (hoặc phải) khác nhau của G theo H là rời nhau.

Chứng minh

i) Nếu $aH = bH$ thì $a = a.1 \in aH = bH$ nên tồn tại $h \in H$ sao cho $a = bh$, do đó $b^{-1}a = h \in H$. Ngược lại, nếu $b^{-1}a \in H$ thì với mọi $x \in aH$, tồn tại $h \in H$ sao cho $x = ah$, suy ra $x = b[(b^{-1}a)h] \in bH$, do đó $aH \subset bH$. Tương tự, với mọi $x \in bH$, tồn tại $h \in H$ sao cho $x = bh$, suy ra $x = a[(b^{-1}a)^{-1}h] \in aH$, do đó $bH \subset aH$. Như vậy $aH = bH$. Phần còn lại chứng minh tương tự.
ii) Giả sử aH và bH là hai lớp kề trái của G theo H $(a, b \in G)$ và $x \in aH \cap bH$. Khi đó, tồn tại $h, h' \in H$ sao cho $ah = x = bh'$, suy ra $b^{-1}a = h'h^{-1} \in H$. Do đó $aH = bH$. Chứng minh tương tự cho lớp kề phải.

Định lý 4

Cho G là một nhóm và H là nhóm con của G. Khi đó, tồn tại một song ánh giữa tập tất cả các lớp kề trái và tập tất cả các lớp kề phải của G theo H.

Chứng minh

Đặt $\mathfrak{L}$ và $\mathfrak{R}$ tương ứng là tập tất cả các lớp kề trái và kề phải của G theo H. Xét tương ứng $f : \mathfrak{L} \to \mathfrak{R}$ xác định bởi $f(aH) = Ha^{-1}$. Với mọi $aH, bH \in \mathfrak{L}$, nếu $aH = bH$ thì từ Bổ đề 1 suy ra $b^{-1}a \in H$ nên $Ha^{-1} = Hb^{-1}$, hay $f(aH) = f(bH)$, do đó f là một ánh xạ. Hơn nữa, dễ dàng kiểm tra f là song ánh, do đó $\mathfrak{L}$ và $\mathfrak{R}$ có cùng lực lượng, nên ta được điều phải chứng minh.

Chỉ số của một nhóm con

Cho G là nhóm và H là nhóm con của G. Ta gọi lực lượng của tập tất cả các lớp kề trái (hoặc phải) của G theo H là *chỉ số* của H trong G, ký hiệu là $[G:H]$.

Định lý 5 (Định lý Lagrange)

Cho G là nhóm hữu hạn và H là nhóm con của G. Khi đó $|H|$ là ước số của $|G|$ và $|G| = [G:H].|H|$.

Chứng minh

Giả sử $[G:H] = m$. Do hai lớp kề trái khác nhau của G theo H là rời nhau nên G phân hoạch thành hợp rời nhau của m lớp kề trái $G = g_1H \cup ... \cup g_mH$. Do đó $|G| = |g_1H| + ... + |g_mH|$. Nhưng, dễ thấy các ánh xạ $f_i : H \to g_iH; h \mapsto g_ih$ là các song ánh, nên $|g_iH| = |H|, i = 1, ..., m$. Do đó $|G| = m.|H| = [G:H].|H|$.

Tích của hai tập con

Cho G là nhóm và H, K là hai tập con của G. Đặt $HK := \{hk \mid h \in H, k \in K\}$. Ta gọi HK là *tích* của H và K.

Định lý 6 (Công thức tích)

Cho H và K là các nhóm con hữu hạn của nhóm G. Khi đó

$$|HK| = \frac{|H|.|K|}{|H \cap K|}.$$

Chứng minh

Xét ánh xạ $\varphi : H \times K \to HK; (h,k) \mapsto hk$. Rõ ràng φ là một toàn ánh, do đó chỉ cần chứng minh với mọi $x \in HK$, $|\varphi^{-1}(x)| = |H \cap K|$ là đủ. Thật vậy, với mỗi $x \in HK$, tồn tại $h \in H, k \in K$ sao cho $x = hk$.
Xét ánh xạ $\psi : H \cap K \to H \times K; d \mapsto (hd, d^{-1}k)$. Khi đó, ψ là một đơn ánh và $\varphi(\psi(d)) = hk = x$, nên với mọi $d \in H \cap K$, $\psi(d) \in \varphi^{-1}(x)$. Do đó ψ là đơn ánh từ $H \cap K$ vào $\varphi^{-1}(x)$. Hơn nữa, với mọi $(h', k') \in \varphi^{-1}(x)$, $hk = x = \varphi(h', k') = h'k'$ nên $kk'^{-1} = h^{-1}h' \in H \cap K$.
Đặt $d = h^{-1}h' = kk'^{-1}$, suy ra $(h', k') = (hd, d^{-1}k) = \psi(d)$.
Do đó ψ là một toàn ánh từ $H \cap K$ vào $\varphi^{-1}(x)$. Vậy, ψ là một song ánh từ $H \cap K$ vào $\varphi^{-1}(x)$. Hơn nữa, H và K hữu hạn, nên $|H \cap K| = |\varphi^{-1}(x)|$.

Với mỗi $x, y \in G$, và $\emptyset \neq S \subset G$, ký hiệu $x^y = y^{-1}xy$ và $S^x = \{s^x | \ s \in S\}$.

Nhóm con liên hợp

Cho G là nhóm, H là nhóm con của G và $x \in G$. Dễ thấy H^x cũng là nhóm con của G và $H^x \cong H$. Ta gọi H^x là *nhóm con liên hợp* với H trong G.

Nhóm con chuẩn tắc

Nếu $\forall x \in G, H^x = H$ thì ta nói H là nhóm con *chuẩn tắc* của G, ký hiệu $H \trianglelefteq G$.

Mệnh đề 7

Cho G là nhóm và $H \leq G$. Khi đó, nếu $\forall x \in G, H^x \leq H$ thì $H \trianglelefteq G$.

Chứng minh

Do $\forall x \in G$, $H^x \leq H$ nên $H^{x^{-1}} \leq H$, suy ra $H \leq H^x$, do đó $H^x = H$. Vậy $H \trianglelefteq G$.

Định lý 8

Nếu H là nhóm con chuẩn tắc của nhóm G thì tập tất cả các lớp kề của G theo H là một nhóm, gọi là *nhóm thương* của G theo H, ký hiệu là G/H.

Chứng minh

Do $H \trianglelefteq G$ nên, với mọi $x \in G$, $xH = Hx$. Do đó, tập các lớp kề trái của G theo H cũng chính là tập các lớp kề phải của G theo H. Hơn nữa, với mọi $a, b \in G$, $aHbH = ab(b^{-1}Hb)H = abHH = abH$, nên tích hai lớp kề trong G lại là một lớp kề trong G. Dễ dàng chứng minh rằng, với phép toán trên thì tập các lớp kề của G theo H là một nhóm với phần tử đơn vị là $H = 1H$ và nghịch đảo của phần tử aH là $a^{-1}H$.

Từ Định lý Lagrange ta được, nếu G là nhóm hữu hạn và $H \lhd G$ thì

$$|G/H| = \frac{|G|}{|H|}.$$

§1. Nhóm và đồng cấu nhóm

Chuẩn hóa tử

Cho G là một nhóm và H là nhóm con của G. Đặt $N_G(H) = \{x \in G |\ H^x = H\}$ và ta gọi $N_G(H)$ là *chuẩn hóa tử* của H trong G.

Nhận xét

i) $N_G(H) \leq G$ và $H \trianglelefteq N_G(H)$.
ii) Nếu $K \leq G$ sao cho $H \trianglelefteq K$ thì $K \leq N_G(H)$.

§1. Nhóm và đồng cấu nhóm

Mệnh đề 9

Cho G là nhóm, H là nhóm con chuẩn tắc của G và K là nhóm con của G. Khi đó HK và KH là nhóm con của G và $HK = KH = \langle H \cup K \rangle$.

Chứng minh

Với mọi $hk, h'k' \in HK$, đặt $t = k'k^{-1}$. Vì $H \trianglelefteq G$ nên
$$(hk)(h'k')^{-1} = hkk'^{-1}h'^{-1} = ht^{-1}h'^{-1} = [h(h'^{-1})^t]t^{-1} \in HK.$$
Do đó $HK \leq G$. Chứng minh tương tự ta được $KH \leq G$.
Rõ ràng $H \cup K \subset HK, KH \subset \langle H \cup K \rangle$, mà $\langle H \cup K \rangle$ là nhóm con nhỏ nhất của G chứa $H \cup K$ nên $HK = KH = \langle H \cup K \rangle$.

§1. Nhóm và đồng cấu nhóm

Tâm hóa tử và tâm

Cho G là nhóm và $a \in G$. Đặt

$$C(a) = \{x \in G \mid a^x = a\} \text{ và } Z(G) = \{x \in G \mid x^y = x, \forall y \in G\}.$$

Ta gọi $C(a)$ là *tâm hóa tử của a trong G* và $Z(G)$ là *tâm của G*.

Mệnh đề 10

Cho G là nhóm và $a \in G$. Khi đó:
i) $C(a)$ là nhóm con của G và $Z(G)$ là nhóm con chuẩn tắc của G;
ii) $Z(G) \subset C(a)$; $C(a) = G \Leftrightarrow a \in Z(G)$; $Z(G) = G \Leftrightarrow G$ là nhóm aben.

Chứng minh

Dễ dàng chứng minh.

§1. Nhóm và đồng cấu nhóm

Hoán tử và nhóm con hoán tử

Cho G là một nhóm. Với mỗi $a, b \in G$, đặt $[a, b] = a^{-1}b^{-1}ab$ và ta gọi $[a, b]$ là *hoán tử* của a và b. Nhóm con của G sinh bởi tất cả các hoán tử được gọi là *nhóm con hoán tử* hay *đạo nhóm* của G, ký hiệu là $[G, G]$ hay G'.

Định lý 11

Cho G là một nhóm. Khi đó:
i) $[G,G] \trianglelefteq G$ và $G/[G,G]$ là nhóm aben.
ii) Nếu $H \trianglelefteq G$ và G/H aben thì $[G,G] \leq H$.

Chứng minh

i) Với mọi $a,b,x \in G$, $[a,b]^x = [a^x, b^x] \in [G,G]$, suy ra $[G,G]^x \leq [G,G]$.
Do đó $[G,G] \trianglelefteq G$.
Rõ ràng với mọi $a,b \in G$, $a^{-1}b^{-1}ab = [a,b] \in [G,G]$, nên $ab[G,G] = ba[G,G]$.
Do đó $G/[G,G]$ là nhóm aben.
ii) Nếu $H \trianglelefteq G$ và G/H aben thì với mọi $a,b \in G$, $abH = baH$, nên $[a,b] \in H$.
Do đó $[G,G] \subset H$.

Đồng cấu nhóm

Cho G và G' là các nhóm và $f : G \to G'$ là một ánh xạ từ G vào G'. Nếu với mọi a,b thuộc G ta có $f(ab) = f(a)f(b)$ thì f được gọi là một *đồng cấu*.
Hơn nữa, nếu đồng cấu f là một song ánh (tương ứng: đơn ánh, toàn ánh) thì f được gọi là một *đẳng cấu* (tương ứng: *đơn cấu*, *toàn cấu*).

- Nếu $f : G \to G$ là một đồng cấu (tương ứng: đẳng cấu) thì f được gọi là một *tự đồng cấu* (tương ứng: *tự đẳng cấu*).
- Nếu tồn tại một đẳng cấu $f : G \to G'$ thì ta nói G và G' *đẳng cấu* với nhau, ký hiệu $G \cong G'$.

Mệnh đề 12

Cho G và G' là các nhóm (với phần tử đơn vị tương ứng là $e \in G$ và $e' \in G'$). Khi đó, nếu $f : G \to G'$ là một đồng cấu thì:
i) $f(e) = e'$;
ii) $\forall a \in G, f(a^{-1}) = f(a)^{-1}$;
iii) $\forall a \in G, \forall n \in \mathbb{Z},\ f(a^n) = f(a)^n$;
iv) tập hợp $\ker f = \{x \in G | f(x) = e'\}$ là một nhóm con của G;
v) tập hợp $\mathrm{Im} f = \{f(x) | x \in G\}$ là một nhóm con của G'.

Các nhóm con $\ker f$ và $\mathrm{Im} f$ như trên được gọi là *nhân* và *ảnh* của đồng cấu f.

Chứng minh

Xem như bài tập.

Định lý 13 (Định lý đẳng cấu 1)

Cho G và G' là các nhóm và $f : G \to G'$ là đồng cấu. Khi đó
$$\ker f \trianglelefteq G \text{ và } G/\ker f \cong \mathrm{Im} f.$$

Chứng minh

i) Với mọi $a \in \ker f$, $f(a) = 1$ nên với mọi $x \in G$, $f(x^{-1}ax) = f(x)^{-1}f(a)f(x) = f(x)^{-1}f(x) = 1$. Do đó, với mọi $x \in G$, $a^x = x^{-1}ax \in \ker f$. Mà a bất kỳ thuộc $\ker f$ nên $(\ker f)^x \leq \ker f$. Vậy $\ker f \trianglelefteq G$.
ii) Đặt $H = \ker f$, ta được $H \trianglelefteq G$. Xét ánh xạ $\varphi : G/H \to G'; xH \mapsto f(x)$. Rõ ràng, với mọi $a, b \in G$, $aH = bH \Leftrightarrow b^{-1}a \in H \Leftrightarrow f(b^{-1}a) = 1 \Leftrightarrow f(a) = f(b)$. Do đó φ xác định và là đơn ánh. Mặt khác, với mọi $a, b \in G$, $\varphi(aHbH) = \varphi(abH) = f(ab) = f(a)f(b) = \varphi(aH)\varphi(bH)$, nên φ là đồng cấu. Hơn nữa, rõ ràng $\mathrm{Im}\varphi = \mathrm{Im} f$, do đó φ là đẳng cấu.

Định lý 14 (Định lý đẳng cấu 2)

Cho H, K là các nhóm con của G, với $H \trianglelefteq G$. Khi đó
$$H \cap K \trianglelefteq K \text{ và } K/(H \cap K) \cong HK/H.$$

Chứng minh

Do $H \trianglelefteq G$ nên $HK \leq G$ và $H \trianglelefteq HK$. Xét ánh xạ $\varphi : K \to HK/H; x \mapsto xH$. Rõ ràng φ là một đồng cấu nhóm. Mặt khác, với mọi $xH \in HK/H$, tồn tại $h \in H, k \in K$ sao cho $x = hk$, suy ra $xH = hkH = k(k^{-1}hk)H = kH = \varphi(k)$, do đó φ là một toàn cấu. Từ Định lý đẳng cấu 1 suy ra $HK/H \cong K/\ker\varphi$. Hơn nữa, với mọi $x \in K$, $x \in \ker\varphi \Leftrightarrow \varphi(x) = H \Leftrightarrow xH = H \Leftrightarrow x \in H \Leftrightarrow x \in H \cap K$, nên $\ker\varphi = H \cap K$.

Định lý 15 (Định lý đẳng cấu 3)

Cho H, K là các nhóm con chuẩn tắc của G, với $K \leq H$. Khi đó
$$H/K \trianglelefteq G/K \text{ và } G/H \cong (G/K)/(H/K).$$

Chứng minh

Xét ánh xạ $f : G/K \to G/H; aK \mapsto aH$. Dễ dàng chứng minh f xác định và là một toàn cấu, với $\ker f = H/K$. Do đó, từ Định lý đẳng cấu 1 suy ra điều phải chứng minh.

Định lý 16 (Định lý về sự tương ứng)

Cho G là một nhóm và $H \trianglelefteq G$. Ký hiệu $L(G)$ là tập hợp tất cả các nhóm con của G và $L(H,G)$ là tập hợp tất cả các nhóm con của G chứa H. Khi đó, tương ứng $S \mapsto S/H$ là một song ánh từ $L(H,G)$ vào $L(G/H)$. Hơn nữa, nếu ký hiệu $S^* = S/H$ và $T^* = T/H$ với $H \leq S, T \leq G$ thì:
i) $T \leq S \Leftrightarrow T^* \leq S^*$ và $[S:T] = [S^*:T^*]$;
ii) $T \trianglelefteq S \Leftrightarrow T^* \trianglelefteq S^*$ và $S/T \cong S^*/T^*$.

Chứng minh

Xét tương ứng $\varphi : L(H,G) \to L(G/H); S \mapsto S/H$. Rõ ràng φ là một ánh xạ và là một đơn ánh. Với mỗi $K^* \leq G/H$, đặt $K = \{x \in G | xH \in K^*\}$. Khi đó K là một nhóm con của G chứa H và $K^* = K/H = \varphi(K)$, do đó φ là một toàn ánh. Vậy φ là một song ánh.
i) Rõ ràng $T \leq S \Leftrightarrow T^* \leq S^*$, nên chỉ cần chứng minh $[S:T] = [S^*:T^*]$. Thật vậy, dễ dàng chứng minh tương ứng $\alpha : sT \mapsto (sH)T^*$ xác định một song ánh từ tập hợp các lớp kề của S theo T vào tập hợp các lớp kề của S^* theo T^*. Do đó $[S:T] = [S^*:T^*]$.
ii) Dễ dàng chứng minh $T \trianglelefteq S \Leftrightarrow T^* \trianglelefteq S^*$. Từ Định lý đẳng cấu 3 suy ra, $(S/H)/(T/H) \cong S/T$, hay $S^*/T^* \cong S/T$.

Định lý 17 (Định lý Cayley)

Mọi nhóm G đều có thể nhúng vào nhóm S_G. Nói riêng, nếu $|G| = n$ thì G có thể nhúng vào S_n.

Chứng minh

Với mỗi $a \in G$, xét ánh xạ $\mathcal{L}_a : G \to G; x \mapsto ax$. Dễ dàng chứng minh $\mathcal{L}_a$ là một song ánh, nghĩa là $\mathcal{L}_a \in S_G$. Như vậy, tương ứng $a \mapsto \mathcal{L}_a$ xác định một ánh xạ $\mathcal{L} : G \to S_G$ thỏa mãn $\mathcal{L}(a) = L_a$. Rõ ràng, với mọi $x \in G$, $\mathcal{L}_{ab}(x) = (abx) = \mathcal{L}_a(bx) = \mathcal{L}_{a\circ}\mathcal{L}_b(x)$, nghĩa là $\mathcal{L}_{ab} = \mathcal{L}_{a\circ}\mathcal{L}_b$, do đó $\mathcal{L}$ là đồng cấu. Hơn nữa, $\mathcal{L}(a) = 1 \Leftrightarrow \forall x \in G, ax = x \Leftrightarrow a = 1$, do đó $\mathcal{L}$ là đơn cấu.

Cho $H, K \leq G$. Xét phép toán $(h,k)(h',k') := (hh', kk'), \forall h, h' \in H, \forall k, k' \in K$. Khi đó $H \times K$ với phép toán trên là một nhóm với phần tử đơn vị là $(1,1)$ và phần tử nghịch đảo của (h,k) là (h^{-1}, k^{-1}).

Định lý 18

Giả sử $H, K \trianglelefteq G$ và $H \cap K = 1$. Khi đó $HK \cong H \times K$.

Chứng minh

Do $H, K \trianglelefteq G$ nên, với mọi $(h,k) \in H \times K$, $h^{-1}k^{-1}hk \in H \cap K = 1$. Suy ra, $hk = kh$. Xét ánh xạ $f : H \times K \to HK; (h,k) \mapsto hk$. Rõ ràng f là một toàn ánh. Hơn nữa, với mọi $(h,k), (h'k') \in H \times K$, $f(hh', kk') = hh'kk' = hkh'k' = f(h,k)f(h',k')$, nên f là đồng cấu. Đồng thời $f(h,k) = 1 \Leftrightarrow hk = 1 \Leftrightarrow k = h^{-1} \in H \cap K = 1$, suy ra $h = k = 1$, nghĩa là f đơn cấu. Vậy f là đẳng cấu.

BÀI TẬP

Bài 1.1

Cho G là một nhóm và $\emptyset \neq S \subset G$. Chứng minh rằng, nếu S hữu hạn và $SS = S$ thì S là một nhóm con của G (trong đó ký hiệu $SS = \{st |\ s, t \in S\}$). Cho một ví dụ chứng tỏ điều trên không đúng trong trường hợp S vô hạn.

Bài 1.2

Cho G là một nhóm và cho ánh xạ $f : G \to G$ xác định bởi $f(a) = a^{-1}, \forall a \in G$. Chứng minh rằng, G là nhóm aben khi và chỉ khi f là đồng cấu.

Bài 1.3

Cho G là nhóm và $H \lneqq G$. Chứng minh rằng $\langle G \backslash H \rangle = G$.

BÀI TẬP

Bài 1.4

Cho G là nhóm và H, K là các nhóm con của nhóm G. Chứng minh rằng:
a) HK là nhóm con của G khi và chỉ khi $HK = KH$.
b) Nếu H và K chuẩn tắc trong G thì HK chuẩn tắc trong G.

Bài 1.5

Cho G là một nhóm và $H, K \leq G$. Chứng minh rằng:
a) $[H : H \cap K] \leq [G : K]$.
b) $[G : H \cap K]$ hữu hạn khi và chỉ khi $[G : H]$ và $[H : H \cap K]$ cùng hữu hạn.
c) Nếu $[G : H \cap K]$ hữu hạn thì $[G : H \cap K] = [G : H].[H : H \cap K]$.

BÀI TẬP

Bài 1.6

Cho n là một số nguyên dương. Chứng minh rằng $[\mathbb{Z} : n\mathbb{Z}] = n$.

Bài 1.7

Cho $\mathbb{C}^*$ là nhóm nhân tất cả các số phức khác 0. Chứng minh rằng nếu H là nhóm con có chỉ số hữu hạn trong $\mathbb{C}^*$ thì $H = \mathbb{C}^*$.

Bài 1.8

Chứng minh rằng, nếu H là một nhóm con có chỉ số 2 trong một nhóm G thì $H \trianglelefteq G$. Hãy tổng quát kết quả trên.

BÀI TẬP

Bài 1.9

Cho G, G' là các nhóm và $H \trianglelefteq G, H' \trianglelefteq G'$. Chứng minh rằng $H \times H' \trianglelefteq G \times G'$ và $(G \times G')/(H \times H') \cong (G/H) \times (G'/H')$.

Bài 1.10

Chứng minh rằng $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ nhưng $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Bài 1.11

Cho G là nhóm và H, K là các nhóm con của G. Chứng minh rằng, nếu $G = H \times K$ thì $G/H \cong K$.

BÀI TẬP

Bài 1.12

Cho một ví dụ về một nhóm G và một nhóm con $H \trianglelefteq G$ sao cho G không chứa nhóm con đẳng cấu với G/H.

Bài 1.13

Cho $f : X \to Y$ là một song ánh giữa hai tập hợp X và Y. Chứng minh rằng ánh xạ $\varphi : S_X \to S_Y$ xác định bởi: $\forall \alpha \in S_X,\ \varphi(\alpha) = f\alpha f^{-1}$ là một đẳng cấu.

Bài 1.14

Cho $\emptyset \neq X \subseteq Y$. Chứng minh rằng S_X có thể được *nhúng* vào S_Y, nghĩa là S_X đẳng cấu với một nhóm con của S_Y.

§2. Tác động của một nhóm lên một tập hợp

Tác động của nhóm lên tập hợp

Cho một nhóm G, một tập S khác rỗng và một ánh xạ

$$* : S \times G \to S;\ (s, x) \mapsto s * x.$$

Ta nói $*$ là *tác động* (phải) của nhóm G lên tập S nếu:

i) $\forall s \in S,\ s * 1 = s$,

ii) $\forall x, y \in G, \forall s \in S,\ (s * x) * y = s * (xy)$.

Nếu tồn tại một tác động của nhóm G lên tập S thì ta nói S là một *G-tập*.

Tác động trái của G lên S được định nghĩa tương tự.

§2. Tác động của một nhóm lên một tập hợp

Ví dụ 1

Cho G là nhóm, $S = G$ và cho $*$ xác định bởi $s * x = sx, \forall s \in S, \forall x \in G$.
Khi đó $*$ là một tác động của G lên S, gọi là *tác động nhân* (phải).

Ví dụ 2

Cho G là nhóm, $S = G$ và cho $*$ xác định bởi $s * x = x^{-1}sx, \forall s \in S, \forall x \in G$.
Khi đó $*$ là một tác động của G lên S, gọi là *tác động liên hợp* lên chính G.
Chú ý rằng, nếu G là nhóm aben thì tác động này là tầm thường, do $s * x = s, \forall s, x \in G$.

§2. Tác động của một nhóm lên một tập hợp

Ví dụ 3

Cho G là nhóm và S là tập tất cả các nhóm con của S. Đặt
$$H * x = H^x \text{ với mọi } H \in S \text{ và } x \in G.$$
Khi đó $*$ là một tác động của G lên S, gọi là *tác động liên hợp của G lên tập S các nhóm con của G*.

Ví dụ 4

Cho $G = S_4$, $S = \{1, 2, 3, 4\}$ và cho $*$ xác định bởi $i * \sigma = \sigma(i), \forall i \in S, \forall \sigma \in G$.
Khi đó $*$ là một tác động của G lên S.
Chẳng hạn, nếu $\sigma = (1\ 3\ 4)$ thì $1 * \sigma = 3$; $2 * \sigma = 2$; $3 * \sigma = 4$; $4 * \sigma = 1$.

§2. Tác động của một nhóm lên một tập hợp

Mệnh đề 1

Cho G là một nhóm, S là một G-tập và $s \in S$. Đặt $G_s = \{x \in G \mid s * x = s\}$. Khi đó G_s là một nhóm con của G.

Chứng minh

Ta có $s * 1 = s$ nên $1 \in G_s$, do đó $G_s \neq \emptyset$. Mặt khác, với mọi $x, y \in G_s$, $s * x = s = s * y$, nên $s * (xy^{-1}) = s$ hay $xy^{-1} \in G_s$, nghĩa là $G_s \leq G$.

Nhóm con đẳng hướng

Nhóm con G_s của G như trên gọi là *nhóm con đẳng hướng* của s trong G.

§2. Tác động của một nhóm lên một tập hợp

Ví dụ 5

- Với tác động như trong Ví dụ 1, ta có $G_s = \{1\}$ với mọi $s \in S$.
- Với tác động như trong Ví dụ 2, ta có $G_s = C(s)$ với $s \in S$.
- Với tác động như trong Ví dụ 3, ta có $G_H = N_G(H)$.
- Với tác động như trong Ví dụ 4, ta có $G_i = S_{\{1,2,3,4\}\setminus\{i\}}$, là nhóm đối xứng trên tập $\{1,2,3,4\}\setminus\{i\}$. Chẳng hạn, $G_2 = \{e, (1\ 3), (1\ 4), (3\ 4), (1\ 3\ 4), (1\ 4\ 3)\}$.

§2. Tác động của một nhóm lên một tập hợp

Quỹ đạo

Cho G là nhóm và S là một G-tập. Ta định nghĩa quan hệ $\sim$ trên S như sau:

$$s \sim s' \Leftrightarrow \text{tồn tại } x \in G \text{ sao cho } s * x = s'.$$

Dễ dàng chứng minh rằng $\sim$ là một quan hệ tương đương.

Với mỗi $s \in S$, ta gọi lớp tương đương chứa s theo quan hệ $\sim$ là một *quỹ đạo* (của S) chứa s, ký hiệu bởi $\mathcal{O}(s)$. Vậy $\mathcal{O}(s) = s * G = \{s * x \mid x \in G\}$.

Ví dụ 6

- Với tác động như trong Ví dụ 1, ta có $\mathcal{O}(s) = G$ với mọi $s \in G$.
- Với tác động như trong Ví dụ 2, ta có $\mathcal{O}(s) = \{s^x \mid x \in G\}$.
- Với tác động như trong Ví dụ 3, ta có $\mathcal{O}(H) = \{H^x \mid x \in G\}$
- Với tác động như trong Ví dụ 4, và $\sigma = (1\ 2), \tau = (1\ 2\ 3)$. Ta có $\mathcal{O}(\sigma) = \{(1\ 2), (1\ 3), (2\ 3)\}$ và $\mathcal{O}(\tau) = \{(1\ 2\ 3), (1\ 3\ 2)\}$.

§2. Tác động của một nhóm lên một tập hợp

Mệnh đề 2

Cho G là nhóm, S là một G-tập và $s \in S$. Khi đó tồn tại một song ánh từ quỹ đạo $\mathcal{O}(s)$ lên tập tất cả các lớp kề phải của G theo nhóm con đẳng hướng G_s.

Chứng minh

Xét tương ứng $f : \mathcal{O}(s) \to G/G_s; s * x \mapsto G_s x$. Khi đó, với mọi $x, y \in G$, $s * x = s * y \Leftrightarrow s * (xy^{-1}) = s \Leftrightarrow xy^{-1} \in G_s \Leftrightarrow G_s x = G_s y$, nên f là ánh xạ và là một đơn ánh. Hơn nữa, rõ ràng f là một toàn ánh, do đó f là một song ánh.

Hệ quả 3

Cho G là một nhóm, S là một G-tập và $s \in S$. Khi đó:
i) $|\mathcal{O}(s)| = [G : G_s]$.
ii) $|G| = |\mathcal{O}(s)|.|G_s|$.

Hệ quả 4

Cho G là một nhóm hữu hạn và $H \leq G$. Khi đó, số các nhóm con của G liên hợp với H bằng chỉ số của $N_G(H)$ trong G.

Chứng minh

Áp dụng Hệ quả 3i) với tác động như trong Ví dụ 3 ta được kết quả.

Định lý 5 (Công thức phân tích thành quỹ đạo)

Cho G là một nhóm, S là một G-tập và gọi Γ là tập hợp đầy đủ các phần tử đại diện của các quỹ đạo của S. Khi đó: $S = \bigcup_{s \in \Gamma} \mathcal{O}(s)$. (1)

Công thức (1) được gọi là *công thức phân tích S thành quỹ đạo*.

Chứng minh

Hiển nhiên do sự phân hoạch S thành các lớp tương đương $\mathcal{O}(s)$ theo quan hệ $\sim$.

Hệ quả 6

Nếu S là tập hợp hữu hạn thì $|S| = \sum_{s \in \Gamma} |\mathcal{O}(s)| = \sum_{s \in \Gamma} [G : G_s]$. (2)

Từ (2) và từ Mệnh đề 2 ta được kết quả sau:

Định lý 7 (Công thức lớp)

Cho G là nhóm hữu hạn. Gọi Γ là tập đầy đủ các phần tử của G đôi một không liên hợp nhau và không nằm trong $Z(G)$. Khi đó:

$$|G| = |Z(G)| + \sum_{a\in\Gamma}[G:C(a)]. \quad (3)$$

Công thức (3) được gọi là *công thức lớp*.

BÀI TẬP

Bài 2.1

Xét $G = S_5$, $X = \{1,2,3,4,5\}$ và ánh xạ $* : X \times G \to X; i * \sigma = \sigma(i)$.
a) Chứng minh $*$ là một tác động của G lên X.
b) Xác định các quỹ đạo của $i \in X$.
c) Mô tả các nhóm con đẳng hướng G_i, với $i \in X$.

Bài 2.2

Xét $G = \langle\{(1\ 2), (3\ 4\ 6)\}\rangle$ là nhóm con của S_6, $X = \{1,2,3,4,5,6\}$ và ánh xạ $* : X \times G \to X; i * \sigma = \sigma(i)$.
a) Chứng minh $*$ là một tác động của G lên X.
b) Xác định các quỹ đạo của $i \in X$.
c) Mô tả các nhóm con đẳng hướng G_i, với $i \in X$.

BÀI TẬP

Bài 2.3

Cho $G = \langle a, b \rangle$ là nhóm con của nhóm nhân các ma trận vuông cấp 2 khả nghịch trên $\mathbb{R}$ sinh bởi $a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ và cho $S = \mathbb{R}^2$.

a) Chứng minh rằng G tác động lên S bởi tác động

$$(x, y) * \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ax + cy, bx + dy).$$

b) Xác định các quỹ đạo của $u_1, u_2, u_3, u_4 \in S$. Trong đó $u_1 = (0, 0)$; $u_2 = (x, x)$, với $x \neq 0$; $u_3 = (x, 0)$, với $x \neq 0$; $u_4 = (x, y)$, với $x \neq 0, y \neq 0, x \neq y$.

c) Mô tả các nhóm con đẳng hướng G_u, với $u \in \{u_1, u_2, u_3, u_4\}$.

BÀI TẬP

Bài 2.4

Xét G là một nhóm bất kỳ và xét $S = G$ với tác động liên hợp $x * g = g^{-1}xg$. Chứng minh rằng các điều sau tương đương:

i) $x \in Z(G)$.

ii) $G_x = G$.

iii) $x * G = \{x\}$.

iv) $|x * G| = 1$.

Bài 2.5

Cho G là một nhóm tác động lên tập hợp $S \neq \emptyset$ và H là một nhóm con chuẩn tắc của G. Đặt $S^H = \{x \in S \mid x * h = x, \forall h \in H\}$. Chứng minh $(S^H) * g = S^H$ với mọi $g \in G$.

BÀI TẬP

Bài 2.6

Xét nhóm $G = S_3$ với tác động liên hợp.
a) Xác định các quỹ đạo của các phần tử $x \in G$.
b) Mô tả các nhóm con đẳng hướng G_x, với $x \in G$.
c) Kiểm tra công thức lớp tương ứng với nhóm G.

Bài 2.7

Cho S là một G-tập và $r, s \in S$. Chứng minh rằng, nếu r và s thuộc cùng một quỹ đạo thì các nhóm con đẳng hướng G_r và G_s là các nhóm con liên hợp.

BÀI TẬP

Bài 2.8

Cho X là một G-tập. Giả sử $|G| = 15, |X| = 17$ và mọi quỹ đạo của X đều chứa ít nhất 2 phần tử. Hãy tìm số quỹ đạo và số phần tử của mỗi quỹ đạo.

Bài 2.9

Cho X là một G-tập. Giả sử $|G| = 33, |X| = 19$. Chứng minh rằng tồn tại ít nhất một quỹ đạo chỉ chứa một phần tử.

Bài 2.10

Cho G là một nhóm hữu hạn và H là nhóm con chuẩn tắc của G sao cho $|H| = p$, với p là ước nguyên tố nhỏ nhất của $|G|$. Chứng minh rằng mọi quỹ đạo của H dưới tác động của G đều có đúng 1 phần tử. Suy ra $H \subseteq Z(G)$.

p-nhóm

Cho G là một nhóm và p là một số nguyên tố. Ta nói G là một *p-nhóm* nếu mọi phần tử của G đều có cấp là lũy thừa của p.

p-nhóm con

Cho G là một nhóm và $H \leq G$. Nếu H là một p-nhóm thì ta nói H là *p-nhóm con* của G.

Mệnh đề 1 (Bổ đề Cauchy)

Nếu G là một nhóm hữu hạn có cấp chia hết cho một số nguyên tố p thì G chứa một nhóm con cấp p.

Chứng minh

Ta sẽ chứng minh bằng qui nạp theo cấp của nhóm G. Hiển nhiên điều khẳng định là đúng nếu $|G| = p$. Giả sử điều khẳng định là đúng đối với những nhóm hữu hạn có cấp bé hơn cấp của G. Xét công thức lớp

$$|G| = |Z(G)| + \sum_{a \in \Gamma} [G : C(a)],$$

trong đó Γ là tập hợp đầy đủ các phần tử của G đôi một không liên hợp nhau và không nằm trong tâm.

Chứng minh (tiếp theo)

Trường hợp 1: $\Gamma \neq \emptyset$.
Nếu tồn tại $a \in \Gamma$ sao cho $p \mid |C(a)|$ thì, theo qui nạp, $C(a)$ chứa một nhóm con cấp p; nếu $p \nmid |C(a)|, \forall a \in \Gamma$ thì với mọi $a \in \Gamma$, $p \mid [G : C(a)]$, kéo theo $p \mid |Z(G)|$. Do đó, theo qui nạp, $Z(G)$ chứa một nhóm con cấp p.
Trường hợp 2: $\Gamma = \emptyset$.
Khi đó, $G = Z(G)$, nên G aben. Nếu tồn tại $a \in G$ sao cho $|a| = |G|$ thì $G = \langle a \rangle$, nên G chứa nhóm con cấp p; nếu G không có phần tử nào có cấp $n = |G|$ thì lấy $a \in G$. Đặt $H = \langle a \rangle$ và $k = |a|$, suy ra $|H| = k < n$. Nếu $p \mid k$ thì, theo qui nạp, H chứa một nhóm con cấp p; nếu $p \nmid k$ thì, theo qui nạp, nhóm thương G/H chứa một phần tử cấp p, gọi nó là yH chẳng hạn $(y \in G)$. Vậy, $y^p \in H$, kéo theo $(y^p)^k = 1$. Nếu $y^k = 1$ thì $(yH)^k = H$, kéo theo $p \mid k$, là điều mâu thuẫn với giả thiết ở trên. Do đó, $b = y^k \neq 1$ và b có cấp là p.

Định lý 2

Nếu $G \neq 1$ là một p-nhóm hữu hạn thì $Z(G) \neq 1$.

Chứng minh

Xét công thức lớp $|G| = |Z(G)| + \sum_{a \in \Gamma} [G : C(a)]$.
- Nếu $\Gamma = \emptyset$ thì $Z(G) = G \neq 1$.
- Nếu $\Gamma \neq \emptyset$ thì $p \mid [G : C(a)], \forall a \in \Gamma$, kéo theo $p \mid |Z(G)|$.

Mệnh đề 3

Nhóm G hữu hạn là một p-nhóm khi và chỉ khi G có cấp là lũy thừa của p.

Chứng minh

Chiều đảo là hiển nhiên.
Chiều thuận, nếu tồn tại q nguyên tố và $q \neq p$ sao cho $q \mid |G|$ thì q phải chứa phần tử cấp q. Điều này mâu thuẫn với Bổ đề Cauchy, nên ta được kết quả.

Nhóm con p-Sylow

Một p-nhóm con P của nhóm G được gọi là *nhóm con p-Sylow* của G nếu không tồn tại một p-nhóm con nào của G thực sự chứa P.
Tập tất cả các nhóm con p-Sylow của G được ký hiệu là $Syl_p(G)$.

Định lý 4 (Sylow 1)

Cho G là nhóm hữu hạn cấp n và p là một ước nguyên tố của n. Khi đó:
i) Với mọi số tự nhiên r thỏa mãn $p^r \mid n$, tồn tại nhóm con H của G có cấp là p^r.
ii) Nếu $p^{r+1} \mid n$ thì mọi nhóm con cấp p^r của G đều nằm trong một nhóm con cấp p^{r+1} nào đó của G.
iii) Các nhóm con p-Sylow của G chính là các nhóm con của G cấp p^m sao cho $p^m \mid n$ nhưng $p^{m+1} \nmid n$.

Chứng minh

i) Ta chứng minh bằng quy nạp theo cấp của G. Hiển nhiên điều khẳng định là đúng đối với những nhóm cấp nguyên tố. Vậy, giả sử $n = |G|$ không là số nguyên tố và điều khẳng định đúng đối với những nhóm có cấp bé hơn n.
Xét công thức lớp $|G| = |Z(G)| + \sum_{a\in\Gamma}[G : C(a)]$.
- Nếu tồn tại $a \in \Gamma$ sao cho p^r là ước của $|C(a)|$ thì, theo quy nạp, tồn tại một nhóm con của $C(a)$ có cấp là p^r.
- Nếu với mọi $a \in \Gamma$, p^r không là ước của $|C(a)|$ thì p là ước của $[G : C(a)], \forall a \in \Gamma$, kéo theo $p \mid |Z(G)|$. Do đó, theo Bổ đề Cauchy, tồn tại nhóm con $K \leq Z(G)$ sao cho $|K| = p$. Hiển nhiên $K \trianglelefteq G$. Vì $p^{r-1} \mid |G/K|$ nên theo giả thiết qui nạp G/K chứa nhóm con cấp p^{r-1}, gọi là $\mathcal{H}$ chẳng hạn. Áp dụng Định lý về sự tương ứng, ta tìm được nhóm con H của G chứa K sao cho $H/K = \mathcal{H}$. Suy ra $|H| = p^r$.

Chứng minh (tiếp theo)

ii) Bây giờ giả sử $p^{r+1} \mid n$ và H là một nhóm con cấp p^r của G. Ký hiệu $\mathcal{O}(H)$ là quĩ đạo của H bởi tác động liên hợp của G lên tập hợp tất cả các nhóm con của G. Khi đó, rõ ràng $\mathcal{O}(H)$ là tập hợp tất cả các nhóm con của G liên hợp với H. Theo Hệ quả 6(§2), ta có $|\mathcal{O}(H)| = [G : N_G(H)]$.
Nếu $|\mathcal{O}(H)| \not\vdots p$ thì $|N_G(H)| \vdots p^{r+1}$. Do đó theo Bổ đề Cauchy $N_G(H)/H$ chứa nhóm con cấp p. Vậy, ta có thể tìm được trong $N_G(H)$ một nhóm con H^* chứa H sao cho H^*/H là nhóm con cấp p, dẫn đến H^* là nhóm con cấp p^{r+1}.
Vậy, giả sử $|\mathcal{O}(H)| \vdots p$. Xét tác động liên hợp của H lên tập hợp $\mathcal{O}(H)$. Khi đó $\mathcal{O}(H)$ phân hoạch thành các quĩ đạo theo tác động này, mà để cho tiện phân biệt, ta sẽ gọi chúng là các H-quĩ đạo. Do độ dài của các H-quĩ đạo đều là ước của $|H|$ nên chúng phải có dạng $p^{r_i}, r_i \geq 0$.

Chứng minh (tiếp theo)

Vì $\{H\}$ là một H-quĩ đạo độ dài 1 và $|\mathcal{O}(H)|$ chia hết cho p nên phải tồn tại ít nhất một H-quĩ đạo khác nữa, ta gọi là $\{K\}$ chẳng hạn. Khi đó $hKh^{-1} = K, \forall h \in H$. Điều này chứng tỏ $H \leq N_G(K)$, dẫn đến HK là nhóm con của $N_G(K)$ và K là nhóm con chuẩn tắc của HK. Từ Định lý đẳng cấu 2 ta có $HK/K \cong H/H \cap K$, kéo theo HK là một p-nhóm con của G. Do H và K là các nhóm con liên hợp với nhau trong G nên ta có thể tìm được phần tử $a \in G$ sao cho $H = aKa^{-1}$. Từ đó K là nhóm con chuẩn tắc thực sự của HK. Gọi σ_a là tự đẳng cấu trong của nhóm G, nghĩa là $\sigma_a(x) = axa^{-1}, \forall x \in G$. Ta có $\sigma_a(K) = H \trianglelefteq \sigma_a(HK) = (aHa^{-1})(aKa^{-1}) = H'H$. Vậy H là nhóm con chuẩn tắc thực sự của $H'H$. Áp dụng Bổ đề Cauchy suy ra $H'H/H$ có một nhóm con cấp p. Từ đó suy ra $H'H$ có một nhóm con chứa H, gọi là S chẳng hạn, sao cho $|S/H| = p$. Vậy S là nhóm con của G có cấp là p^{r+1}.

Chứng minh (tiếp theo)

iii) Giả sử m là một số nguyên dương sao cho p^m là ước của n và p^{m+1} không là ước của n. Theo chứng minh ở phần đầu của định lý ta thấy rằng luôn tồn tại các nhóm con cấp p^m trong G. Hiển nhiên các nhóm con này là các nhóm con p-Sylow của G. Ngược lại, nếu P là một nhóm con p-Sylow của G thì theo chứng minh ở phần cuối ta thấy ngay rằng cấp của P phải là p^m. Vậy, P là nhóm con p-Sylow của G khi và chỉ khi P có cấp là p^m.

Định lý 5 (Sylow 2)

Cho G là một nhóm hữu hạn cấp n và p là ước nguyên tố của n. Khi đó:
i) Mọi p-nhóm con của G đều nằm trong một nhóm con p-Sylow nào đó của G.
ii) Tất cả các nhóm con p-Sylow của G đều liên hợp với nhau.
iii) Số các nhóm con p-Sylow của G là ước của n và $\equiv 1 \pmod{p}$.

Chứng minh

i) Hiển nhiên do tính hữu hạn của nhóm G.
ii) Giả sử P và H là hai nhóm con p-Sylow bất kỳ của G và $\mathcal{O}(P) = \{P^x \mid x \in G\}$ là tập tất cả các nhóm con của G liên hợp với P. Từ chứng minh Định lý Sylow 1, ta có $|\mathcal{O}(P)| = [G : N_G(P)]$. Mà P là nhóm con p-Sylow của G và $P \leq N_G(P)$ nên $|\mathcal{O}(P)|$ không chia hết cho p.
Xét tác động liên hợp của H lên tập hợp $\mathcal{O}(P)$. Các H-quĩ đạo theo nghĩa đã nói tới trong chứng minh Định lý Sylow 1 có độ dài là p^r, với $r \geq 0$. Do $|\mathcal{O}(P)|$ là một số không chia hết cho p, nên trong số các H-quỹ đạo nói trên phải có ít nhất một quỹ đạo có độ dài 1 (ứng với $\alpha = 0$). Gọi quỹ đạo đó là $\{Q\}$. Khi đó $Q^h = Q, \forall h \in H$ hay $H \leq N_G(Q)$, dẫn đến HQ là nhóm con của $N_G(Q)$ và Q là nhóm con chuẩn tắc của HQ.

Chứng minh (tiếp theo)

Áp dụng Định lý đẳng cấu 2, ta có $HQ/Q \cong H/H \cap Q$, kéo theo HQ là một p-nhóm con của G chứa Q. Do Q là một nhóm con p-Sylow của G nên từ đó suy ra $Q = HQ$, dẫn đến $H \leq Q$. Tuy nhiên, do H cũng là nhóm con p-Sylow của G nên $H = Q$. Do $Q \in \mathcal{O}(P)$ nên ta có $H = Q$ liên hợp với P.
iii) Cũng với các ký hiệu đã dùng trong chứng minh ii), ta thấy rằng, nếu $\{Q\}$ là một H-quỹ đạo độ dài 1 thì $Q = H$. Vậy chỉ có duy nhất một H-quỹ đạo có độ dài 1. Do đó $|\mathcal{O}(P)| \equiv 1 \pmod{p}$. Theo chứng minh ii) ta có $|\mathcal{O}(P)| = [G : N_G(P)]$ chính là số các nhóm con p-Sylow của G. Do đó số các nhóm con p-Sylow của G là ước của n và $\equiv 1 \pmod{p}$.

BÀI TẬP

Bài 3.1

Chứng minh rằng, nếu $|G| = p^n$ với p nguyên tố và k là một số nguyên sao cho $0 \leq k \leq n$ thì G chứa một nhóm con chuẩn tắc cấp p^k.

Bài 3.2

Chứng minh rằng, nếu G là một p-nhóm và H là một nhóm con chuẩn tắc không tầm thường của G thì $H \cap Z(G) \neq 1$.

Bài 3.3

Chứng minh rằng, nếu G là một p-nhóm và H là một nhóm con chuẩn tắc có cấp p của G thì $H \leq Z(G)$.

BÀI TẬP

Bài 3.4

Chứng minh rằng, nếu G là một p-nhóm và H là một nhóm con thực sự của G và có cấp là p^s thì H chứa trong một nhóm con của G có cấp p^{s+1}.

Bài 3.5

Chứng minh rằng, nếu p nguyên tố và G là một nhóm không aben có cấp p^3 thì các tính chất sau được thỏa mãn:
a) $|Z(G)| = p$;
b) $G/Z(G) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$;
c) $Z(G) = [G, G]$.

BÀI TẬP

Bài 3.6

Cho $H \trianglelefteq G$. Chứng minh rằng, nếu H và G/H là các p-nhóm thì G là một p-nhóm.

Bài 3.7

Cho G là một nhóm. Chứng minh rằng, nếu H là một nhóm con duy nhất có cấp bằng k của G thì H là nhóm con chuẩn tắc của G.

Bài 3.8

Giả sử G là một nhóm hữu hạn và P là một nhóm con p-Sylow của G. Chứng minh rằng, P là nhóm con p-Sylow duy nhất của G nếu và chỉ nếu $P \trianglelefteq G$.

BÀI TẬP

Bài 3.9

Một nhóm G được gọi là *nhóm đơn* nếu G không chứa các nhóm con chuẩn tắc thực sự. Chứng minh rằng, các nhóm có cấp $30, 36, 56, 196, 200$ không là các nhóm đơn.

Bài 3.10

Cho G là một nhóm hữu hạn. Chứng minh rằng một p-nhóm con chuẩn tắc bất kỳ của G luôn chứa trong tất cả các nhóm con p-Sylow của G.

Bài 3.11

Chứng minh rằng, các nhóm con p-Sylow của một nhóm có cấp vô hạn không nhất thiết liên hợp với nhau. (*Hướng dẫn*: Xét tổng trực tiếp vô hạn của S_3).

BÀI TẬP

Bài 3.12

Cho G là một nhóm hữu hạn. Chứng minh rằng, nếu với mỗi ước nguyên tố p của $|G|$ đều tồn tại duy nhất một nhóm con p-Sylow của G thì G là tích trực tiếp (trong) của các nhóm con Sylow của nó.

Bài 3.13

Cho G là một nhóm có cấp $5^2.7^2$. Chứng minh rằng, G phân tích được thành tích trực tiếp của hai nhóm con p-Sylow của G.

BÀI TẬP

Bài 3.14

Cho p, q nguyên tố với $p > q$. Chứng minh rằng, nếu $|G| = pq$ thì G có duy nhất một nhóm con p-Sylow và do đó nhóm con này chuẩn tắc trong G.

Bài 3.15

Cho $G = \langle \{a, b\} \rangle$ là nhóm con của $GL_2(\mathbb{C})$ sinh bởi: $a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

Chứng minh rằng:
a) G là nhóm không aben cấp 8.
b) G chỉ có duy nhất một nhóm con cấp 2.

BÀI TẬP

Bài 3.16

Nếu G là một nhóm aben thì mọi nhóm con của G đều chuẩn tắc. Hãy cho một ví dụ chứng tỏ điều ngược lại không đúng.

Bài 3.17

Hãy tìm tất cả các nhóm con 2-Sylow của S_4.

Bài 3.18

Hãy tìm tất cả các nhóm con cấp 3 của S_4.

BÀI TẬP

Bài 3.19

Chứng minh rằng S_5 không có nhóm con cấp 15.

Bài 3.20

Cho $P \in Syl_p(H)$ và $N \trianglelefteq H$. Chứng minh rằng $P \cap N \in Syl_p(N)$. Suy ra, nếu N và H/N là p-nhóm thì $H = PN$.

§4. Nhóm giải được

Nhóm tự đẳng cấu

Cho G là một nhóm. Một đẳng cấu $\varphi : G \to G$ được gọi là một *tự đẳng cấu* của G. Tập tất cả các tự đẳng cấu của G là một nhóm với phép nhân đồng cấu, gọi là *nhóm các tự đẳng cấu* của G, ký hiệu bởi $Aut(G)$.

Nhóm con đặc trưng

Một nhóm con H của nhóm G được gọi là *nhóm con đặc trưng* của G, ký hiệu $H \operatorname{char} G$, nếu với mọi $\varphi \in Aut(G), \varphi(H) = H$.

§4. Nhóm giải được

Mệnh đề 1

Nếu với mọi $\varphi \in Aut(G), \varphi(H) \leq H$ thì $H \operatorname{char} G$.

Chứng minh

Nếu φ là tự đẳng cấu của G thì φ^{-1} cũng là tự đẳng cấu của G.
Theo giả thiết $\varphi(H) \leq H$ và $\varphi^{-1}(H) \leq H$. Suy ra, $\varphi(H) = H$.

§4. Nhóm giải được

Mệnh đề 2

Nếu $H \operatorname{char} G$ thì $H \trianglelefteq G$.

Chứng minh

Giả sử $H \operatorname{char} G$ và a là phần tử bất kỳ trong G. Ánh xạ $\varphi_a : G \to G; x \mapsto x^a$ là một tự đẳng cấu của G, gọi là *tự đẳng cấu trong* của G. Do $H \operatorname{char} G$ nên $H = \varphi_a(H) = H^a$. Mà a là phần tử bất kỳ trong G nên $H \trianglelefteq G$.

§4. Nhóm giải được

Mệnh đề 3

Nếu H char K và K char G thì H char G.

Chứng minh

Cho φ là một tự đẳng cấu bất kỳ của G.
Do K char G nên $\varphi(K) = K$, do đó $\varphi|_K : K \to K$ là một tự đẳng cấu của K.
Mà H char K nên $H = \varphi|_K(H) = \varphi(H)$. Vậy H char G.

§4. Nhóm giải được

Mệnh đề 4

Nếu H char K và $K \trianglelefteq G$ thì $H \trianglelefteq G$.

Chứng minh

Cho a là phần tử bất kỳ trong G.
Gọi φ_K là hạn chế của tự đẳng cấu trong φ_a lên K. Vì $K \trianglelefteq G$ nên φ_K là tự đẳng cấu của K. Mà H char K nên $H = \varphi_K(H) = \varphi(H) = H^a$. Vậy $H \trianglelefteq G$.

§4. Nhóm giải được

Mệnh đề 5

Nếu $H \leq K \leq G$ và $H \operatorname{char} G$, $K/H \operatorname{char} G/H$ thì $K \operatorname{char} G$.

Chứng minh

Với mọi $\varphi \in Aut(G)$ ta có $\varphi(H) = H$. Do đó ta có thể định nghĩa ánh xạ φ' trên G/H như sau: $\varphi' : G/H \to G/H; xH \mapsto \varphi(x)H$.
Nếu $xH = yH$ thì $x^{-1}y \in H$. Nhưng $H \operatorname{char} G$ nên $\varphi(x^{-1}y) \in H$, kéo theo $\varphi(x)H = \varphi(y)H$. Vậy, φ' là ánh xạ. Dễ thấy φ' là tự đẳng cấu của G/H. Do đó, từ $K/H \operatorname{char} G/H$ suy ra $\varphi'(K/H) = K/H$.
Do $H \leq K$ nên $H = \varphi(H) \leq \varphi(K)$. Do đó $\varphi'(K/H) = \varphi(K)/H = K/H$, kéo theo $\varphi(K) = K$. Vậy $K \operatorname{char} G$.

§4. Nhóm giải được

Dãy aben

Cho dãy các nhóm con $G = G_0 \geq G_1 \geq \ldots \geq G_n = 1$ trong nhóm G là một *dãy aben* nếu với mọi i, $G_i \trianglelefteq G_{i-1}$ và G_{i-1}/G_i là nhóm aben.

Nhóm giải được

Ta nói nhóm G là *nhóm giải được* nếu tồn tại trong G một dãy aben.

§4. Nhóm giải được

Đạo nhóm

Cho G là một nhóm, đặt $G^{(0)} = G$ và với mọi $i \geq 0$, $G^{(i+1)} = [G^{(i)}, G^{(i)}]$.
Ta gọi nhóm con $G^{(i)}$ là *nhóm con hoán tử bậc i* hoặc *đạo nhóm bậc i* của G.

Dãy dẫn xuất

Dãy các nhóm con hoán tử $G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \dots$ được gọi là *dãy dẫn xuất* của G.

§4. Nhóm giải được

Định lý 6

Cho G là một nhóm. Khi đó $G^{(i)} \operatorname{char} G$ với mọi i.

Chứng minh

Hiển nhiên $G^{(0)} \operatorname{char} G$. Giả sử φ là một tự đẳng cấu bất kỳ của G. Khi đó, với mọi $a, b \in G$, $\varphi([a,b]) = [\varphi(a), \varphi(b)] \in [G,G]$, nên $\varphi([G,G]) \leq [G,G]$. Vậy $[G,G] \operatorname{char} G$. Nói riêng, với mọi i, $G^{(i+1)} = [G^{(i)}, G^{(i)}] \operatorname{char} G^{(i)}$. Bằng quy nạp theo bậc i của các hoán tử, giả sử $G^{(i)} \operatorname{char} G$. Khi đó, $G^{(i+1)} \operatorname{char} G$. Vậy, $G^{(i)} \operatorname{char} G$ với mọi i.

§4. Nhóm giải được

Định lý 7

Cho G là một nhóm. Khi đó $G^{(i+j)} = (G^{(i)})^{(j)}$ với mọi i, j.

Chứng minh

Bằng quy nạp theo j, giả sử $G^{(i+j)} = (G^{(i)})^{(j)}$.
Khi đó $G^{(i+j+1)} = [G^{(i+j)}, G^{(i+j)}] = [(G^{(i)})^{(j)}, (G^{(i)})^{(j)}] = (G^{(i)})^{(j+1)}$.

§4. Nhóm giải được

Mệnh đề 8

Giả sử $G = G_0 \geq G_1 \geq \ldots \geq G_n = 1$ là một dãy aben. Khi đó, với mọi $i \in \mathbb{Z}^+$, $G_i \geq G^{(i)}$.

Chứng minh

Rõ ràng $G_0 = G = G^{(0)}$. Bằng quy nạp theo i, giả sử $G_i \geq G^{(i)}$. Khi đó, $[G_i, G_i] \geq [G^{(i)}, G^{(i)}] = G^{(i+1)}$. Mặt khác, nhóm thương G_i/G_{i+1} là nhóm aben, nên $[G_i, G_i] \leq G_{i+1}$. Do đó $G_{i+1} \geq G^{(i+1)}$.

§4. Nhóm giải được

Định lý 9

Cho G là một nhóm không tầm thường. Khi đó, G giải được nếu và chỉ nếu tồn tại $n \in \mathbb{N}$ sao cho $G^{(n)} = 1$.

Chứng minh

Giả sử G giải được, nghĩa là có một dãy aben $G = G_0 \geq G_1 \geq \ldots \geq G_n = 1$. Do đó $1 = G_n \geq G^{(n)}$, nên $G^{(n)} = 1$.
Ngược lại, giả sử $G^{(n)} = 1$. Với mọi i, do $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ nên $G^{(i+1)} \trianglelefteq G^{(i)}$ và $G^{(i)}/G^{(i+1)}$ aben. Do đó dãy dẫn xuất $G = G^{(0)} \geq G^{(1)} \geq \ldots \geq G^{(n)} = 1$ là dãy aben, nghĩa là G giải được.

§4. Nhóm giải được

Hệ quả 10

Nếu tồn tại một nhóm con $H \neq 1$ của G sao cho $[H, H] = H$ thì G không giải được.

Bậc giải được

Nếu G là nhóm giải được thì số n nhỏ nhất sao cho $G^{(n)} = 1$ được gọi là *bậc giải được* của G.

§4. Nhóm giải được

Định lý 11

Mọi nhóm con của một nhóm giải được bậc n đều là nhóm giải được với bậc $\leq n$.

Chứng minh

Giả sử G là nhóm giải được bậc n. Khi đó $G^{(n)} = 1$. Nếu $H \leq G$ thì với mọi $i \in \mathbb{N}$, $H^{(i)} \leq G^{(i)}$. Do đó $H^{(n)} \leq G^{(n)} = 1$, suy ra $H^{(n)} = 1$. Vậy H là nhóm giải được với bậc $\leq n$.

§4. Nhóm giải được

Định lý 12

Nếu G là nhóm giải được bậc n và $f : G \to H$ là một toàn cấu thì H là nhóm giải được với bậc $\leq n$.

Chứng minh

Giả sử G là nhóm giải được bậc n. Khi đó $G^{(n)} = 1$. Nếu $H = f(G)$ thì dễ dàng chứng minh bằng quy nạp theo $i \in \mathbb{N}$ rằng $H^{(i)} = f(G^{(i)})$. Nói riêng, $H^{(n)} = f(G^{(n)}) = f(1) = 1$. Do đó H là nhóm giải được bậc không vượt quá n.

§4. Nhóm giải được

Định lý 13

Nếu $H \trianglelefteq G$ sao cho H và G/H giải được thì G giải được.

Chứng minh

Đặt $K = G/H$. Do H và K giải được nên tồn tại $m, n \in \mathbb{N}$ sao cho $H^{(m)} = 1$ và $K^{(n)} = 1$. Xét đồng cấu tự nhiên $f : G \to K$. Do $K^{(n)} = 1$ nên $f(G^{(n)}) = 1$, nghĩa là $G^{(n)} \leq H$. Suy ra, $(G^{(n)})^{(m)} \leq H^{(m)} = 1$. Do đó, $G^{(m+n)} = (G^{(n)})^{(m)} = 1$. Vậy G giải được.

§4. Nhóm giải được

Hệ quả 14

Hai nhóm H và K đều giải được khi và chỉ khi $H \times K$ giải được.

Chứng minh

Đặt $G = H \times K$. Khi đó $H \trianglelefteq G$ và $K \simeq G/H$. Nếu H và K giải được thì G/H giải được. Do đó G giải được. Chiều ngược lại là hiển nhiên.

§4. Nhóm giải được

Định lý 15

Mọi p-nhóm G hữu hạn đều giải được.

Chứng minh

Vì G là một p-nhóm nên $Z(G) \neq 1$, suy ra $G/Z(G)$ là một p-nhóm có cấp nhỏ hơn $|G|$. Do đó, bằng quy nạp theo cấp của G suy ra $G/Z(G)$ giải được, mà $Z(G)$ là nhóm aben nên $Z(G)$ giải được. Do đó G giải được.

BÀI TẬP

Bài 4.1

Cho G là một nhóm. Chứng minh rằng, $Z(G)\,\mathrm{char}\,G$.

Bài 4.2

Chứng minh rằng, nếu $H \trianglelefteq G$ và $(|H|, |G/H|) = 1$ thì $H\,\mathrm{char}\,G$.

Bài 4.3

Cho một ví dụ chứng tỏ một nhóm G chứa một nhóm con chuẩn tắc H nhưng H không là nhóm con đặc trưng của G.

BÀI TẬP

Bài 4.4

Chứng minh rằng:
a) Nếu S và T là hai nhóm con giải được của G và $S \trianglelefteq G$ thì ST giải được.
b) Mọi nhóm G hữu hạn đều có duy nhất một nhóm con chuẩn tắc giải được tối đại $\mathcal{S}(G)$. Hơn nữa $G/\mathcal{S}(G)$ không có nhóm con chuẩn tắc giải được không tầm thường.

Bài 4.5

Cho G là một nhóm hữu hạn có cấp lớn hơn 1. Chứng minh rằng:
a) Nếu G giải được với bậc giải được n thì G chứa một nhóm con H aben, chuẩn tắc, với G/H có bậc giải được là $n-1$.
b) Nếu G không giải được thì G chứa một nhóm con $H \neq 1$ với $[H,H] = H$.

BÀI TẬP

Bài 4.6

Chứng minh rằng S_n giải được khi và chỉ khi $n < 5$.

Bài 4.7

Cho p, q nguyên tố. Chứng minh rằng:
a) Mọi nhóm có cấp pq và p^2q đều giải được.
b) Nếu $p < q$ thì mọi nhóm cấp pq^n đều giải được.

Dãy tâm trên

Xét nhóm G. Ta đặt $\zeta_0(G) := 1$ và với mỗi i,

$$\zeta_{i+1}(G) := \{x \in G \mid [x, y] \in \zeta_i(G), \forall y \in G\}.$$

Khi đó ta gọi dãy $\zeta_0(G) = 1 \leq \zeta_1(G) \leq \zeta_2(G) \leq \ldots$ là *dãy tâm trên* của G.

Bổ đề 1

Ta có $\zeta_i(G)\,\mathrm{char}\,G$ với mọi i

Chứng minh

Dễ thấy $\zeta_i(G) \leq G$ với mọi i. Ta có $\zeta_0(G) = 1\,\mathrm{char}\,G$. Bằng quy nạp, giả sử $\zeta_i(G)\,\mathrm{char}\,G$ và $\varphi \in Aut(G)$, $x \in \zeta_{i+1}(G)$, $y \in G$. Khi đó tồn tại $z \in G$ sao cho $y = \varphi(z)$. Ta có $[\varphi(x), y] = [\varphi(x), \varphi(z)] = \varphi([x, z])$. Nhưng $[x, z] \in \zeta_i(G)$ và theo quy nạp, $\zeta_i(G)\,\mathrm{char}\,G$, nên $\varphi([x, z]) \in \zeta_i(G)$. Vậy $[\varphi(x), y] \in \zeta_i(G)$. Do y bất kỳ trong G nên $\varphi(x) \in \zeta_{i+1}(G)$. Vậy $\zeta_{i+1}(G)\,\mathrm{char}\,G$.

Từ định nghĩa ta được $\zeta_{i+1}(G)/\zeta_i(G) = Z(G/\zeta_i(G))$.

§5. Nhóm lũy linh

Dãy tâm tăng

Cho dãy $1 = G_0 \leq G_1 \leq \ldots$ các nhóm con của nhóm G.
Ta gọi dãy trên là *dãy tâm tăng* nếu với mọi i, $G_i \trianglelefteq G$ và $G_{i+1}/G_i \leq Z(G/G_i)$.

Nhận xét

Rõ ràng dãy tâm trên là một dãy tâm tăng.

§5. Nhóm lũy linh

Mệnh đề 2

Nếu $1 = G_0 \leq G_1 \leq \ldots$ là một dãy tâm tăng của G thì với mọi i, $G_i \leq \zeta_i(G)$.

Chứng minh

Ta có $G_0 = 1 = \zeta_0(G)$. Bằng quy nạp, giả sử $G_i \leq \zeta_i(G)$.
Khi đó, $[G_{i+1}, G] \leq G_i \leq \zeta_i(G)$, kéo theo $G_{i+1} \leq \zeta_{i+1}(G)$.

§5. Nhóm lũy linh

Nhóm lũy linh

Ta nói nhóm G là *nhóm lũy linh* nếu tồn tại $n \geq 0$ sao cho $\zeta_n(G) = G$.

Mệnh đề 3

Mọi nhóm aben đều lũy linh.

Chứng minh

Nếu G là nhóm aben thì $\zeta_1(G) = Z(G) = G$, do đó G lũy linh.

§5. Nhóm lũy linh

Mệnh đề 4

Mọi p-nhóm hữu hạn đều lũy linh.

Chứng minh

Giả sử G là một p-nhóm hữu hạn. Nếu $\zeta_i(G) \neq G$ thì $G/\zeta_i(G)$ là p-nhóm không tầm thường, do đó $Z(G/\zeta_i(G)) = \zeta_{i+1}(G)/\zeta_i(G)$ là nhóm không tầm thường, kéo theo $\zeta_{i+1}(G) \neq \zeta_i(G)$. Do nhóm G hữu hạn nên tồn tại n sao cho $\zeta_n(G) = G$.

§5. Nhóm lũy linh

Dãy tâm dưới

Cho G là một nhóm. Đặt $\gamma_1(G) := G$ và với mọi i, $\gamma_{i+1}(G) := [\gamma_i(G), G]$.
Ta gọi dãy $\gamma_1(G) = G \geq \gamma_2(G) \geq \ldots$ là *dãy tâm dưới* của G.

Bổ đề 5

Ta có $\gamma_i(G)$ char G với mọi i.

Chứng minh

Ta có $\gamma_1(G) = G$ char G. Bằng quy nạp, giả sử $\gamma_i(G)$ char G. Xét $\varphi \in Aut(G)$.
Ta có $\varphi(\gamma_{i+1}(G)) = \varphi[\gamma_i(G), G] = [\varphi(\gamma_i(G)), \varphi(G)] = [\gamma_i(G), G] = \gamma_{i+1}(G)$.
Do đó $\gamma_{i+1}(G)$ char G.

§5. Nhóm lũy linh

Dãy tâm giảm

Cho dãy $G_1 = G \geq G_2 \geq \ldots$ các nhóm con của nhóm G.
Ta gọi dãy trên là *dãy tâm giảm* nếu với mọi i, $G_i \trianglelefteq G$ và $G_i/G_{i+1} \leq Z(G/G_{i+1})$.

Nhận xét

Dãy tâm dưới là dãy tâm giảm.

§5. Nhóm lũy linh

Mệnh đề 6

Nếu $G_1 = G \geq G_2 \geq \ldots$ là một dãy tâm giảm thì $\gamma_i(G) \leq G_i$ với mọi i.

Chứng minh

Ta có $\gamma_1(G) = G = G_1$. Bằng quy nạp, giả sử $\gamma_i(G) \leq G_i$.
Khi đó $\gamma_{i+1}(G) = [\gamma_i(G), G] \leq [G_i, G] \leq G_{i+1}$.
Do đó ta được kết quả cần chứng minh.

§5. Nhóm lũy linh

Lớp lũy linh

Nếu G là nhóm lũy linh thì số tự nhiên n nhỏ nhất thỏa mãn $\zeta_n(G) = G$ được gọi là *lớp lũy linh* của G. Khi đó G gọi là *nhóm lũy linh lớp n*.

Mọi nhóm aben không tầm thường đều là nhóm lũy linh lớp 1.

Lớp của một nhóm lũy linh chính là độ dài của dãy tâm trên.

Định lý 7

Cho G là một nhóm. Khi đó, G là nhóm lũy linh lớp n khi và chỉ khi $\gamma_n(G) \neq 1$ và $\gamma_{n+1}(G) = 1$.

Chứng minh

Chiều thuận: Giả sử G là nhóm lũy linh lớp n.
- Nếu $n = 1$ thì G là nhóm aben, suy ra $\gamma_2(G) = [G, G] = 1$.
- Nếu $n > 1$, xét hai dãy tâm giảm

$$\zeta_n(G) \geq \zeta_{n-1}(G) \geq \ldots \geq \zeta_0(G) \text{ và } \gamma_1(G) \geq \gamma_2(G) \ldots.$$

Từ Mệnh đề 6 suy ra $\gamma_{n+1}(G) \leq \zeta_0(G) = 1$, kéo theo $\gamma_{n+1}(G) = 1$.
Giả sử $\gamma_n(G) = 1$. Xét hai dãy tâm tăng

$$\zeta_0(G) \leq \zeta_1(G) \leq \ldots \leq \zeta_n(G) \text{ và } \gamma_n(G) \leq \ldots \leq \gamma_1(G) = G.$$

Từ Mệnh đề 2 suy ra $\gamma_1(G) = G \leq \zeta_{n-1}(G) \neq G$, mâu thuẫn. Do đó $\gamma_n(G) \neq 1$.

Chứng minh (tiếp theo)

Chiều đảo: Giả sử $\gamma_{n+1}(G) = 1$ và $\gamma_n(G) \neq 1$.
Ta chứng minh G là nhóm lũy linh lớp n.
- Nếu $n = 1$ thì $\gamma_2(G) = 1$, nghĩa là G aben, suy ra G là nhóm lũy linh lớp 1.

Nếu $n \geq 1$, xét hai dãy tâm tăng

$$\gamma_{n+1}(G) = 1 \leq \gamma_n(G) \leq \ldots \leq \gamma_1(G) = G \text{ và } \zeta_0(G) = 1 \leq \zeta_1(G) \leq \ldots$$

Từ Mệnh đề 2 ta có $\gamma_1(G) = G \leq \zeta_n(G)$, kéo theo $\zeta_n(G) = G$.
Giả sử $\zeta_{n-1}(G) = G$. Xét hai dãy tâm giảm
$\zeta_{n-1}(G) = G \geq \ldots \geq \zeta_0(G) = 1$ và $\gamma_1(G) = G \geq \gamma_2(G) \ldots \geq \gamma_{n+1}(G) = 1$.
Từ Mệnh đề 6 ta có $\zeta_0(G) \geq \gamma_n(G) \neq 1$, kéo theo $\zeta_0(G) \neq 1$, mâu thuẫn.
Vậy, độ dài của dãy tâm trên của G là n, hay G là nhóm lũy linh lớp n.

§5. Nhóm lũy linh

Mệnh đề 8

Nhóm con của nhóm lũy linh lớp n là một nhóm lũy linh lớp $\leq n$.

Chứng minh

Giả sử G là nhóm lũy linh lớp n và $H \leq G$. Ta có $\gamma_1(H) = H \leq G = \gamma_1(G)$. Nếu $\gamma_i(H) \leq \gamma_i(G)$ thì $\gamma_{i+1}(H) = [\gamma_i(H), H] \leq [\gamma_i(G), G] = \gamma_{i+1}(G)$. Vậy, với mọi i, $\gamma_i(H) \leq \gamma_i(G)$. Nói riêng, $\gamma_{n+1}(H) = 1$, kéo theo H là nhóm lũy linh lớp $\leq n$.

§5. Nhóm lũy linh

Mệnh đề 9

Ảnh đồng cấu của một nhóm lũy linh lớp n là một nhóm lũy linh lớp $\leq n$.

Chứng minh

Giả sử G là nhóm lũy linh lớp n và $f : G \to H$ là một toàn cấu.
Dễ dàng chứng minh bằng quy nạp rằng $f(\gamma_i(G)) = \gamma_i(H)$.
Do đó $\gamma_{n+1}(H) = f(\gamma_{n+1}(G)) = f(1) = 1$.
Suy ra H là nhóm lũy linh lớp không vượt quá n.

Mệnh đề 10

Mọi nhóm lũy linh đều giải được.

Chứng minh

Giả sử G là nhóm lũy linh lớp n. Khi đó dãy $\zeta_0 = 1 \leq \zeta_1 \leq \ldots \leq \zeta_n = G$ là một dãy chuẩn tắc. Hơn nữa, $\zeta_{i+1}(G)/\zeta_i(G) = Z(G/\zeta_i(G))$ là nhóm aben. Vậy G là nhóm giải được.

Điều kiện chuẩn hóa

Ta nói nhóm G thỏa mãn *điều kiện chuẩn hóa* nếu mọi nhóm con thực sự của G đều thực sự nằm trong chuẩn hóa tử của nó.

Định lý 11

Mọi nhóm lũy linh đều thỏa mãn điều kiện chuẩn hóa.

Chứng minh

Giả sử G là nhóm lũy linh lớp n và H là một nhóm con thực sự của G. Ta có $\zeta_0(G) = 1 \leq H$. Gọi k là số tự nhiên lớn nhất thỏa mãn $\zeta_k(G) \leq H$. Khi đó tồn tại $x \in \zeta_{k+1}(G) \setminus H$. Ta chứng minh $x \in N_G(H)$. Thật vậy, với mọi $h \in H$, ta có $x^{-1}hx = hh^{-1}x^{-1}hx = h[h,x] \in H\zeta_k = H$. Do đó $H^x \leq H$. Thay x bởi x^{-1}, ta có $H^{x^{-1}} \leq H$ hay $H \leq H^x$. Suy ra $H^x = H$, hay $x \in N_G(H)$.
Vậy $H \lneqq N_G(H)$.

Hệ quả 12

Nếu G là nhóm lũy linh và H là nhóm con tối đại của G thì $H \trianglelefteq G$.

Chứng minh

Theo Định lý 11, $H \lneqq N_G(H)$. Do H là nhóm con tối đại của G nên $N_G(H) = G$, nghĩa là $H \trianglelefteq G$.

Từ những kết quả vừa nêu, ta có mối liên hệ sau đây giữa các lớp nhóm:

aben $\subseteq$ lũy linh $\subseteq$ giải được.

Tồn tại những nhóm lũy linh không aben, chẳng hạn:

- Nhóm Q các quaternions: $Q = \left\langle a, b \,\middle|\, a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\rangle$.
- Nhóm con cấp 8 trong nhóm đối xứng S_4 sinh ra bởi các chu trình $(12), (1324)$.

Nhóm đối xứng S_3 giải được nhưng không lũy linh. Thật vậy, $1 \leq \langle (123) \rangle \leq S_3$ là dãy aben của S_3. Mặt khác, $Z(S_3) = 1$ nên S_3 không lũy linh.

Nhóm con á chuẩn tắc

Ta nói nhóm con H là *á chuẩn tắc* trong nhóm G nếu tồn tại dãy các nhóm con $H_0 = H \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_n = G$.

Mệnh đề 13

Mọi nhóm con của nhóm lũy linh đều á chuẩn tắc.

Chứng minh

Giả sử G là nhóm lũy linh lớp n. Ta chứng minh $H\zeta_i(G) \trianglelefteq H\zeta_{i+1}(G)$.
Trước hết, ta có nhận xét rằng, với mọi $h \in H$ và với mọi $x \in \zeta_{i+1}(G)$, ta có $x^{-1}hx = hh^{-1}x^{-1}hx = h[h,x] \in H\zeta_i(G)$.
Bây giờ xét các phần tử bất kỳ $h,k \in H, x \in \zeta_{i+1}$ và $y \in \zeta_i(G)$. Theo chứng minh trên, ta có $(hx)^{-1}(ky)(hx) = [x^{-1}(h^{-1}k)x](x^{-1}yx)(x^{-1}hx) \in H\zeta_i(G)$. Vậy $H\zeta_i(G) \trianglelefteq H\zeta_{i+1}(G)$ và ta có dãy $H = H\zeta_0 \trianglelefteq H\zeta_1 \trianglelefteq \ldots \trianglelefteq H\zeta_n = G$. Do đó H là nhóm con á chuẩn tắc của G.

Mệnh đề 14

Tích trực tiếp của hai nhóm lũy linh là nhóm lũy linh.

Chứng minh

Giả sử $G = HK$ là một tích trực tiếp, trong đó H là nhóm lũy linh lớp n và K là nhóm lũy linh lớp m. Ta chứng minh $\gamma_i(G) \leq \gamma_i(H)\gamma_i(K)$ (1) bằng quy nạp theo i. Thật vậy, (1) hiển nhiên đúng với $i = 1$. Giả sử (1) đúng với $i \geq 1$. Khi đó $\gamma_{i+1}(G) = [\gamma_i(G), G] \leq [\gamma_i(H)\gamma_i(K), HK]$. Lấy $h \in \gamma_i(H), h_1 \in H, k \in \gamma_i(K)$ và $k_1 \in K$. Khi đó, do HK là tích trực tiếp nên $[hk, h_1k_1] = k^{-1}h^{-1}k_1^{-1}h_1^{-1}hkh_1k_1 = [h,h_1][k,k_1] \in [\gamma_i(H), H][\gamma_i(K), K] = \gamma_{i+1}(H)\gamma_{i+1}(K)$. Do đó $\gamma_{i+1}(G) \leq \gamma_{i+1}(H)\gamma_{i+1}(K)$. Vậy (1) đúng với mọi $i \geq 1$. Bây giờ lấy $k = \max\{n,m\}$, suy ra $\gamma_k(G) = 1$. Do đó G là nhóm lũy linh.

§5. Nhóm lũy linh

Bổ đề 15

Cho P là một nhóm con p-Sylow của nhóm hữu hạn G và H là một nhóm con của G chứa $N_G(P)$. Khi đó, H là một nhóm con tự chuẩn hóa, nghĩa là $N_G(H) = H$.

Chứng minh

Với mọi $x \in N_G(H), H^x = H$, do đó P và các nhóm P^x là các nhóm con p-Sylow của H. Vì vậy, tồn tại $u \in H$ sao cho $P^x = P^u$ hay $xu^{-1} \in N_G(P) \leq H$, kéo theo $x \in H$.

§5. Nhóm lũy linh

Định lý 16

Nhóm hữu hạn G là lũy linh khi và chỉ khi G là tích trực tiếp của các nhóm con Sylow của nó.

Chứng minh

Nếu G là tích trực tiếp của các nhóm con Sylow của nó thì theo các Mệnh đề 4 và 14 ta được G là nhóm lũy linh. Ngược lại, giả sử G là nhóm lũy linh. Khi đó, ta chỉ cần chứng minh mọi nhóm con Sylow của G đều chuẩn tắc. Vậy, giả sử P là một nhóm con Sylow bất kỳ của G. Đặt $H = N_G(P)$. Nếu $H \neq G$ thì $H \lneqq N_G(H)$. Nhưng điều này mâu thuẫn với Bổ đề 15. Vậy $H = G$, nghĩa là $P \trianglelefteq G$.

Mệnh đề 17

Nếu G là nhóm lũy linh và N là nhóm con chuẩn tắc không tầm thường của G thì $N \cap Z(G)$ cũng là nhóm con chuẩn tắc không tầm thường của G.

Chứng minh

Do G lũy linh nên tồn tại $n \in \mathbb{N}$ sao cho $\zeta_n(G) = G$. Do đó tồn tại số tự nhiên i nhỏ nhất sao cho $N \cap \zeta_i(G) \neq 1$. Do $N \trianglelefteq G$ nên $[N \cap \zeta_i(G), G] \leq N \cap \zeta_{i-1}(G) = 1$. Suy ra $N \cap \zeta_i(G) \leq N \cap Z(G)$, kéo theo $N \cap Z(G) = N \cap \zeta_i(G) \neq 1$. Để ý rằng $\zeta_1(G) = Z(G)$ nên chứng minh vừa rồi chứng tỏ $i = 1$.

Hệ quả 18

Nhóm con chuẩn tắc tối tiểu của nhóm lũy linh G nằm trong $Z(G)$.

Mệnh đề 19

Nếu G lũy linh và A là nhóm con aben chuẩn tắc tối đại của G thì $A = C_G(A)$.

Chứng minh

Đặt $C := C_G(A)$. Do A là nhóm con aben của G nên $A \leq C$. Giả sử $A \neq C$. Khi đó, do $A \trianglelefteq G$ nên với mọi $x \in G$, với mọi $c \in C$ và với mọi $a \in A$ ta có $(x^{-1}cx)a(x^{-1}cx)^{-1}a^{-1} = x^{-1}[c(xax^{-1})]c^{-1}xa^{-1} = x^{-1}[(xax^{-1})c]c^{-1}xa^{-1} = 1$. Suy ra C/A là nhóm con chuẩn tắc không tầm thường của nhóm lũy linh G/A. Do đó, theo Mệnh đề 17, tồn tại $x \in C \setminus A$ sao cho $xA \in (C/A) \cap Z(G/A)$. Vì $\langle x, A\rangle/A \leq Z(G/A)$ nên theo Định lý về sự tương ứng ta được $\langle x, A\rangle \trianglelefteq G$. Hơn nữa, $\langle x, A\rangle$ là nhóm con aben của G, do đó từ tính tối đại của A suy ra $x \in A$ và ta có một mâu thuẫn. Vậy $A = C_G(A)$.

§5. Nhóm lũy linh

Định lý 20

Cho G là nhóm hữu hạn. Khi đó các điều sau tương đương:
i) G lũy linh.
ii) Mọi nhóm con của G đều á chuẩn tắc.
iii) G thỏa điều kiện chuẩn hóa.
iv) Mọi nhóm con tối đại của G đều chuẩn tắc.
v) G là tích trực tiếp của những nhóm con Sylow của nó.

§5. Nhóm lũy linh

Chứng minh

i) $\Rightarrow$ ii). Do Mệnh đề 13.
ii) $\Rightarrow$ iii). Giả sử $H \lneqq G$. Do H á chuẩn tắc trong G nên tồn tại dãy $H = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_n = G$. Gọi i là số nhỏ nhất sao cho $H \neq H_i$. Khi đó, $H = H_{i-1} \lhd H_i$ và $H_i \leq N_G(H)$. Vậy, $H \lneqq H_i \leq N_G(H)$.
iii) $\Rightarrow$ iv). Do Hệ quả 12.
iv) $\Rightarrow$ v). Giả sử P là một nhóm con Sylow của G. Nếu P không chuẩn tắc trong G thì $N_G(P)$ nằm trong một nhóm con tối đại M nào đó của G. Theo giả thiết $M \trianglelefteq G$, trái với kết luận của Bổ đề 15. Vậy mọi nhóm con Sylow của G đều chuẩn tắc trong G.
v) $\Rightarrow$ i). Do Định lý 14.

BÀI TẬP

Bài 5.1

Cho G là một nhóm không tầm thường. Chứng minh rằng, G lũy linh lớp 1 khi và chỉ khi G aben.

Bài 5.2

Chứng minh rằng, nếu $G \neq 1$ và G lũy linh thì $Z(G) \neq 1$.

Bài 5.3

Chứng minh rằng, nếu $H \leq Z(G)$ và G/H lũy linh thì G lũy linh.

BÀI TẬP

Bài 5.4

Chứng minh rằng, nếu G lũy linh và H là nhóm con chuẩn tắc tối tiểu của G thì $H \leq Z(G)$.

Bài 5.5

Chứng minh rằng, S_3 giải được nhưng không lũy linh.

Bài 5.6

Chứng minh rằng, nếu G lũy linh lớp $n \geq 1$ thì $G/Z(G)$ lũy linh lớp $n-1$.

BÀI TẬP

Bài 5.7

Chứng minh rằng, nếu G thỏa điều kiện chuẩn hóa thì mọi nhóm con tối đại của G đều chuẩn tắc trong G và có chỉ số là một số nguyên tố.

Bài 5.8

a) Chứng minh rằng, nếu H, K là hai nhóm con lũy linh, chuẩn tắc của G thì HK là nhóm con lũy linh, chuẩn tắc của G.
b) Suy ra, mọi nhóm G hữu hạn đều có nhóm con lũy linh chuẩn tắc lớn nhất, ký hiệu bởi $\mathcal{F}(G)$.
c) Chứng tỏ rằng, nếu G hữu hạn thì $\mathcal{F}(G)\,\mathrm{char}\,G$.

§6. Nhóm aben hữu hạn sinh

Bổ đề 1

Mọi nhóm con của $\mathbb{Z}^n$ đều hữu hạn sinh.

Chứng minh

Ta chứng minh bằng quy nạp theo n. Xét K là một nhóm con của $\mathbb{Z}^n$. Đặt $F = \{f \mid (f, a_2, \ldots, a_n) \in K\}$. Dễ thấy F là một nhóm con của $\mathbb{Z}$ nên F có dạng $f_0\mathbb{Z}$, với f_0 nguyên không âm. Cố định $x_0 = (f_0, a_2, \ldots, a_n) \in K$. Khi đó, với mọi $x = (k_1, k_2, \ldots, k_n) \in K$, tồn tại s sao cho $k_1 = sf_0$. Do đó $x = sx_0 + (0, k_2 - sa_2, \ldots, k_n - sa_n)$. Tập tất cả các phần tử dạng $(k_2 - sa_2, \ldots, k_n - sa_n)$ tạo thành một nhóm con K' của $\mathbb{Z}^{n-1}$ nên theo quy nạp ta được K' hữu hạn sinh. Vậy K hữu hạn sinh.

Định lý 2

Cho K là một nhóm con của $\mathbb{Z}^n$. Khi đó, tồn tại $d_1, d_2, \ldots, d_r$ nguyên dương sao cho $d_1 \mid d_2 \mid \ldots \mid d_r$ và $K \cong d_1\mathbb{Z} \times d_2\mathbb{Z} \times \ldots \times d_r\mathbb{Z}$.

Chứng minh

Từ Bổ đề 1 ta được K hữu hạn sinh. Giả sử $k_1, k_2, \ldots, k_m$ là tập hợp các phần tử sinh của K và xem $k_i = (k_{i1}, k_{i2}, \ldots, k_{in})$.

Đặt $A = \begin{pmatrix} k_{11} & k_{12} & \ldots & k_{1n} \\ k_{21} & k_{22} & \ldots & k_{2n} \\ & \ldots\ldots\ldots & & \\ k_{m1} & k_{m2} & \ldots & k_{mn} \end{pmatrix}$.

Chứng minh (tiếp theo)

Nhận xét rằng:
- Đổi thứ tự hai dòng của A, hoặc đổi dấu một dòng của A, hoặc cộng dòng thứ i của A với k lần dòng thứ j của A ($k \in \mathbb{Z}$) ta sẽ được một ma trận có các dòng là các phần tử sinh của K.
- Đổi thứ tự hai cột của A, hoặc đổi dấu một cột của A, hoặc cộng cột thứ i của A với k lần cột thứ j của A ($k \in \mathbb{Z}$) ta sẽ được một ma trận có các dòng là các phần tử sinh của một nhóm đẳng cấu với K.

Đặt d_1 là ước số chung lớn nhất của tất cả các k_{ij}. Áp dụng các phép biến đổi dòng và cột như trên ta đưa được A về dạng $A' = \left(\begin{array}{c|ccc} d_1 & 0 & \ldots & 0 \\ \hline 0 & k'_{22} & \ldots & k'_{2n} \\ \ldots & & \ldots\ldots & \\ 0 & k'_{m2} & \ldots & k'_{mn} \end{array}\right)$,

trong đó các k'_{ij} chia hết cho d_1.

Chứng minh (tiếp theo)

Do nhận xét trên ta được tập các dòng của A' là các phần tử sinh của một nhóm đẳng cấu với K. Cứ tiếp tục như trên, cuối cùng ta được K đẳng cấu với nhóm sinh bởi các dòng của ma trận

$$S = \left(\begin{array}{cccc|c} d_1 & 0 & \dots & 0 & \\ 0 & d_2 & \dots & 0 & 0 \\ & \dots\dots\dots & & & \\ 0 & 0 & \dots & d_r & \\ \hline & 0 & & & 0 \end{array}\right), \quad \text{với } 1 \le d_1 \mid d_2 \mid \dots \mid d_r.$$

Từ đó ta được kết quả cần chứng minh.

Định lý 3 (Định lý cơ bản của nhóm aben hữu hạn sinh)

Cho G là một nhóm aben hữu hạn sinh. Khi đó: $G \cong \mathbb{Z}^r \times \mathbb{Z}_{d_1} \times ... \times \mathbb{Z}_{d_s}$, trong đó $r, d_1, ..., d_s$ là các số tự nhiên thỏa mãn $r \ge 0$, $n_j \ge 2$ với mọi j, và $d_{i+1} \mid d_i$, $1 \le i \le s-1$.

Chứng minh

Giả sử $G = \langle g_1, ..., g_n \rangle$. Xét phép tương ứng $\varphi : \mathbb{Z}^n \to G$ xác định bởi $\varphi(i_1, ..., i_n) = i_1 g_1 + ... + i_n g_n$. Dễ dàng chứng minh rằng φ là toàn cấu. Do đó $G \cong \mathbb{Z}^n / \ker\varphi$. Mặt khác, $\ker\varphi$ là nhóm con của $\mathbb{Z}^n$ nên theo Định lý 2, tồn tại $d_1, ..., d_s$ nguyên dương sao cho $d_1 \mid ... \mid d_s$ và $\ker\varphi \cong d_1\mathbb{Z} \times ... \times d_s\mathbb{Z}$. Do đó $G \cong \mathbb{Z}^n / \ker\varphi \cong \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_s\mathbb{Z} \times \mathbb{Z} \times ... \times \mathbb{Z} \cong \mathbb{Z}_{d_1} \times ... \times \mathbb{Z}_{d_s} \times \mathbb{Z} \times ... \times \mathbb{Z}$. Do $\mathbb{Z}_1$ là tầm thường nên ta có thể xem $d_i > 1$ với mọi i. Bằng cách sắp xếp lại các d_i sao cho $d_{i+1} \mid d_i$ ta được kết quả cần chứng minh.

§6. Nhóm aben hữu hạn sinh

Hạng tự do

Số r trong Định lý 3 được gọi là *hạng tự do* hoặc *số Betti* của G và các số $d_1, d_2, \ldots, d_s$ được gọi là các *nhân tử bất biến* của G. Dạng biểu diễn của G trong Định lý 3 được gọi là *sự phân tích nhân tử bất biến* của G.

Hệ quả 4

Cho G là nhóm aben hữu hạn sinh G. Khi đó G hữu hạn khi và chỉ khi G có hạng tự do bằng 0.

Hệ quả 5

Nếu G là nhóm aben hữu hạn thì cấp của G bằng tích của tất cả các nhân tử bất biến của nó.

§6. Nhóm aben hữu hạn sinh

Nếu G là nhóm aben hữu hạn với các nhân tử bất biến là $d_1, d_2, \ldots, d_s$, với $d_{i+1} \mid d_i$, thì G được gọi là *kiểu* $(d_1, d_2, \ldots, d_s)$.

Phương pháp liệt kê các nhóm aben hữu hạn có cấp cho trước

Để tìm tất cả (sai khác một đẳng cấu) các nhóm aben hữu hạn cấp n cho trước, ta tìm tất cả các dãy hữu hạn số tự nhiên $d_1, d_2, \ldots, d_s$ sao cho $d_1 d_2 \ldots d_s = n$ và $d_1 \vdots d_2 \vdots \ldots \vdots d_s \geq 2$.

Chú ý rằng $d_1 \geq d_2 \geq \cdots \geq d_s$ nên d_1 là nhân tử bất biến lớn nhất của G.

§6. Nhóm aben hữu hạn sinh

Mệnh đề 6

Mọi ước nguyên tố của n đều là ước của d_1.

Chứng minh

Nếu p là một ước nguyên tố bất kỳ của n thì do $n = d_1 d_2 \dots d_s$ nên p là ước của một d_i nào đó. Khi đó, p phải là ước số của d_j với mọi $j \leq i$. Nói riêng, $p \mid d_1$.

Hệ quả 7

Nếu n là tích của các ước nguyên tố của nó thì chỉ có duy nhất một nhóm aben hữu hạn cấp n (sai khác một đẳng cấu), đó chính là $\mathbb{Z}_n$.

§6. Nhóm aben hữu hạn sinh

Ví dụ 1

Xác định tất cả các nhóm aben hữu hạn cấp $n = 180$ (sai khác một đẳng cấu).

Lời giải

Ta có $n = 180 = 2^2.3^2.5$. Như nhận xét trên, ta phải có $2.3.5|d_1$. Do đó các giá trị có thể có của d_1 là $2^2.3^2.5$ hoặc $2^2.3.5$ hoặc $2.3^2.5$, hoặc $2.3.5$.

- Nếu $d_1 = 2^2.3^2.5$ thì $d_1 = n$ nên trường hợp này chỉ có một nhóm là $\mathbb{Z}_n = \mathbb{Z}_{180}$.
- Nếu $d_1 = 2^2.3.5$ thì do $d_2|d_1$ và $d_1 d_2|n$ nên ta phải có $d_2 = 3$. Như vậy $d_1 d_2 = n$. Do đó trường hợp này chỉ có một nhóm là $\mathbb{Z}_{60} \times \mathbb{Z}_3$.
- Nếu $d_1 = 2.3^2.5$ thì, tương tự trên, chỉ có một nhóm là $\mathbb{Z}_{90} \times \mathbb{Z}_2$.
- Nếu $d_1 = 2.3.5$ thì $d_2 \in \{2, 3, 6\}$. Nếu $d_2 \in \{2, 3\}$ thì do $d_3 \mid d_2$ nên $d_3 = d_2$. Khi đó $d_1 d_2 d_3$ chia hết cho 2^3 hoặc 3^3, mâu thuẫn với (3). Do đó $d_2 = 6$, và nhóm aben tương ứng là $\mathbb{Z}_{30} \times \mathbb{Z}_6$.

Tóm lại, ta có các nhóm aben hữu hạn cấp 180 là $\mathbb{Z}_{180}$, $\mathbb{Z}_{60} \times \mathbb{Z}_3$, $\mathbb{Z}_{90} \times \mathbb{Z}_2$ và $\mathbb{Z}_{30} \times \mathbb{Z}_6$.

§6. Nhóm aben hữu hạn sinh

Nhận thấy rằng việc liệt kê như trên chỉ thực hiện được trong một số trường hợp đặc biệt. Định lý sau sẽ cho ta một phương pháp có hệ thống hơn và đưa ra phương pháp tính toán nhanh hơn để xác định tất cả các nhóm aben hữu hạn với cấp cho trước.

§6. Nhóm aben hữu hạn sinh

Định lý 8

Cho G là một nhóm aben cấp $n > 1$ và đặt sự phân tích n thành tích các lũy thừa của nguyên tố khác nhau có dạng $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Khi đó:
i) $G \cong A_1 \times A_2 \times \dots \times A_k$, với A_i là nhóm aben cấp $p_i^{\alpha_i}$,
ii) Với mỗi $A \in \{A_1, A_2, \dots, A_k\}$ sao cho $|A| = p^\alpha$, $A \cong \mathbb{Z}_{p^{\beta_1}} \times \mathbb{Z}_{p^{\beta_2}} \times \dots \times \mathbb{Z}_{p^{\beta_t}}$, với $\beta_1 \geq \beta_2 \geq \dots \geq \beta_t \geq 1$ và $\beta_1 + \beta_2 + \dots + \beta_t = \alpha$.

Chứng minh

(i) Hiển nhiên từ Định lý Sylow 1. Các nhóm con A_i chính là các nhóm con p_i-Sylow của G.
(ii) Hiển nhiên do Định lý 3.

§6. Nhóm aben hữu hạn sinh

Dựa vào Định lý 8, để tìm tất cả các nhóm aben cấp $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, ta liệt kê tất cả các nhân tử bất biến cho các nhóm con cấp p^β, với $p^\beta \in \{p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}\}$, nghĩa là tìm các bộ $\beta_j \geq 1$ sao cho $\beta_j \geq \beta_{j+1}$ và $\sum_j \beta_j = \beta$. Mỗi bộ như vậy được gọi là một *phân hoạch* của β.

Mỗi số nguyên p^{β_j} trong Định lý 8 được gọi là *ước sơ cấp* của G và sự phân tích G dưới dạng (i) được gọi là *sự phân tích ước sơ cấp* của G.

§6. Nhóm aben hữu hạn sinh

Ví dụ 2

Bảng sau liệt kê tất cả các nhóm aben cấp p^5 (với p nguyên tố) dựa vào sự phân hoạch của 5.

Các nhân tử bất biến	Nhóm aben tương ứng
5	$\mathbb{Z}_{p^5}$
4, 1	$\mathbb{Z}_{p^4} \times \mathbb{Z}_p$
3, 2	$\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2}$
3, 1, 1	$\mathbb{Z}_{p^3} \times \mathbb{Z}_p \times \mathbb{Z}_p$
2, 2, 1	$\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_p$
2, 1, 1, 1	$\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$
1, 1, 1, 1, 1	$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

Như vậy có tất cả 7 nhóm aben cấp p^5 không đẳng cấu nhau.

Mệnh đề 9

Nếu $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ và m_i là số các phân hoạch của α_i thì số các nhóm aben cấp n (không đẳng cấu nhau) là $m_1 m_2 \dots m_k$.

Ví dụ 3

Xác định tất cả các nhóm aben cấp 1800.

Lời giải

Ta có $1800 = 2^3 3^2 5^2$. Ta có bảng liệt kê các nhóm dạng p^β như sau:

Cấp p^β	**Các phân hoạch của β**	**Các nhóm aben tương ứng**
2^3	$3;\quad 2,1;\quad 1,1,1$	$\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
3^2	$2;\quad 1,1$	$\mathbb{Z}_9,\quad \mathbb{Z}_3 \times \mathbb{Z}_3$
5^2	$2;\quad 1,1$	$\mathbb{Z}_{25},\quad \mathbb{Z}_5 \times \mathbb{Z}_5$

Do đó số các nhóm aben cấp 1800 là $3.2.2 = 12$ nhóm. Đó là các tích trực tiếp của một nhóm thuộc dòng thứ nhất với một nhóm thuộc dòng thứ hai và một nhóm thuộc dòng thứ ba.

Mệnh đề 10

i) Với mọi $m, n \in \mathbb{Z}^+$, $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \Leftrightarrow (m, n) = 1$.
ii) Nếu $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ thì $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}}$.

Thuật toán xác định các ước sơ cấp từ các nhân tử bất biến

Giả sử G là nhóm aben cấp n với kiểu $(d_1, d_2, \dots, d_s)$, nghĩa là $G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_s}$. Để xác định các ước sơ cấp của G, ta thực hiện như sau:
- Phân tích n dưới dạng $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.
- Phân tích mỗi d_i dưới dạng $d_i = p_1^{\beta_{i1}} p_2^{\beta_{i2}} \dots p_k^{\beta_{ik}}$, với $\beta_{ij} \geq 0$.
- Dựa vào Mệnh đề 10, ta được $\mathbb{Z}_{d_i} \cong \mathbb{Z}_{p_1^{\beta_{i1}}} \times \mathbb{Z}_{p_2^{\beta_{i2}}} \times \dots \times \mathbb{Z}_{p_k^{\beta_{ik}}}$. Trong đó, nếu $\beta_{ij} = 0$ thì $\mathbb{Z}_{p_j^{\beta_{ij}}} = \mathbb{Z}_1$ nên ta có thể xóa bỏ trong tích trực tiếp. Khi đó, các ước sơ cấp của G chính là bộ các số nguyên $p_j^{\beta_{ij}}$, với $\beta_{ij} \neq 0$.

Ví dụ 4

Nếu nhóm G có cấp $1800 = 2^3.3^2.5^2$ với kiểu $(30, 30, 2)$, thì do $30 = 2.3.5$ nên $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_2$.

§6. Nhóm aben hữu hạn sinh

Thuật toán xác định các nhân tử bất biến từ các ước sơ cấp

Giả sử G là nhóm aben cấp $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ với sự phân tích ước sơ cấp cho trước. Để xác định các nhân tử bất biến của G, ta thực hiện như sau:
- Gọi t là số lớn nhất của số các ước sơ cấp của cùng một lũy thừa nguyên tố.
- Với mỗi $j \in \{1, 2, \dots, k\}$, sắp xếp các ước sơ cấp dạng $p_j^{\beta_{ji}}$ theo thứ tự giảm dần. Thêm vào các $\beta_{ji} = 0$ cho đủ độ dài t.
- Với mỗi $i \in \{1, 2, \dots, t\}$, đặt $d_i = p_1^{\beta_{1i}} p_2^{\beta_{2i}} \dots p_k^{\beta_{ki}}$.

Khi đó ta được kiểu của G là $(d_1, d_2, \dots, d_t)$.

Ví dụ 5

Nếu nhóm G có cấp 3600 thỏa mãn $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$ thì các bộ ước sơ cấp của G là $(4, 2, 2)$, $(3, 3, 1)$, $(25, 1, 1)$. Do đó kiểu của G là $(4.3.25, 2.3.1, 2.1.1) = (300, 6, 2)$.

BÀI TẬP

Bài 6.1

Liệt kê tất cả các nhóm aben cấp n không đẳng cấu và xác định kiểu của nhóm tương ứng trong các trường hợp sau:

a) $n = 100$.
c) $n = 1155$.
b) $n = 576$.
d) $n = 42875$.

Bài 6.2

Ký hiệu $\{n_1, n_2, \dots, n_k\}$ là nhóm aben $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$. Hãy xác định các cặp nhóm aben đẳng cấu trong các danh sách sau:

a) $\{4, 9\}$, $\{6, 6\}$, $\{8, 3\}$, $\{9, 4\}$, $\{6, 4\}$, $\{64\}$.
b) $\{4, 18\}$, $\{12, 6\}$, $\{72\}$, $\{36, 2\}$.
c) $\{5^2.7^2, 3^2.5.7\}$, $\{3^2.5^2.7, 5.7^2\}$, $\{3.5^2, 7^2, 3.5.7\}$, $\{5^2.7, 3^2.5, 7\}$.
d) $\{2^2.5.7, 2^3.5^3, 2.5^2\}$, $\{2^3.5^3.7, 2^3.5^3\}$, $\{2^2, 2.7, 2^3, 5^3, 5^3\}$, $\{2.5^3, 2^2.5^3, 2^3, 7\}$.

BÀI TẬP

Bài 6.3

Cho G là nhóm aben hữu hạn với kiểu $(n_1, n_2, \ldots, n_k)$. Chứng minh rằng G chứa một phần tử cấp m khi và chỉ khi $m|n_1$.

Bài 6.4

Cho $G = \mathbb{Z}_{60} \times \mathbb{Z}_{45} \times \mathbb{Z}_{12} \times \mathbb{Z}_{36}$. Hãy xác định số phần tử cấp 2 và số nhóm con chỉ số 2 của G.

§7. Nhóm aben tự do

Trong toàn bộ mục này, giả sử tất cả các nhóm được xét đến đều là nhóm aben với phép toán cộng.

Nhóm p-nguyên sơ

Nếu G là một p-nhóm aben thì G được gọi là một nhóm *p-nguyên sơ*.

Bổ đề 1

Cho G là một nhóm aben hữu hạn. Với mỗi ước nguyên tố p của $|G|$, đặt $G_p = \{x \in G \mid p^m x = 0, m \in \mathbb{N}\}$. Khi đó, G_p là một nhóm con p-Sylow của G.

Chứng minh

Rõ ràng $G_p \neq \emptyset$. Hơn nữa, với mọi $x, y \in G_p$, tồn tại $m, n \in \mathbb{N}$ sao cho $p^m x = 0$ và $p^n y = 0$. Do đó, $p^{m+n}(x-y) = 0$. Suy ra $x - y \in G_p$. Vậy $G_p \leq G$. Mặt khác, mọi phần tử trong G_p đều có cấp là lũy thừa của p nên G_p là một p-nhóm con của G. Do đó, tồn tại một nhóm con p-Sylow P của G sao cho $G_p \leq P$.
Ngược lại, do mọi phần tử trong P đều có cấp là một lũy thừa của p nên $P \subseteq G_p$. Vậy $G_p = P$.

Thành phần p-nguyên sơ

Nhóm con G_p xác định như trên được gọi là *thành phần p-nguyên sơ* của G.

Định lý 2 (Sự phân tích nguyên sơ)

Mọi nhóm aben hữu hạn đều là tổng trực tiếp của các thành phần p-nguyên sơ của nó.

Chứng minh

Do mọi nhóm aben đều lũy linh và mọi nhóm lũy linh hữu hạn là tích trực tiếp các nhóm con Sylow của nó nên từ Bổ đề 1 ta được kết quả.

Sự độc lập tuyến tính

Cho G là một nhóm aben và $X = \{x_1, \ldots, x_n\}$ là một tập hữu hạn các phần tử khác 0 trong G. Ta nói X là *độc lập tuyến tính* nếu với mọi $m_1, \ldots, m_n \in \mathbb{Z}$, từ điều kiện $\sum_{i=1}^{n} m_i x_i = 0$ luôn suy ra $m_i x_i = 0$ với mọi $i \in \overline{1,n}$.

Một tập hợp vô hạn trong G được gọi là *độc lập tuyến tính* nếu mọi tập con hữu hạn của nó đều độc lập tuyến tính.

Mệnh đề 3

Tập hợp $\{x_1, \ldots, x_r\} \subseteq G$ gồm các phần tử khác 0 là độc lập tuyến tính khi và chỉ khi $\langle x_1, \ldots, x_r \rangle = \langle x_1 \rangle \oplus \cdots \oplus \langle x_r \rangle$.

Chứng minh

Giả sử $\{x_1, \ldots, x_r\}$ độc lập tuyến tính. Nếu $y \in \langle x_i \rangle \cap \langle x_j, j \neq i \rangle$ thì tồn tại $m_1, \ldots, m_r \in \mathbb{Z}$ sao cho $y = -m_i x_i = \sum_{j \neq i} m_j x_j$, và do đó $m_1 x_1 + \cdots + m_r x_r = 0$.

Do $\{x_1, \ldots, x_r\}$ độc lập tuyến tính, nên $m_k x_k = 0, \forall k$. Nói riêng, $m_i x_i = 0$, nghĩa là $y = 0$. Do đó $\langle x_1, \ldots, x_r \rangle = \langle x_1 \rangle \oplus \cdots \oplus \langle x_r \rangle$.

Ngược lại, giả sử $\langle x_1, \ldots, x_r \rangle = \langle x_1 \rangle \oplus \cdots \oplus \langle x_r \rangle$. Xét đẳng thức $\sum m_k x_k = 0$. Suy ra, với mỗi i, $m_i x_i = -\sum_{j \neq i} m_j x_j \in \langle x_i \rangle \cap \langle x_j, j \neq i \rangle = 0$. Do đó, $m_i x_i = 0$. Vậy $\{x_1, \ldots, x_r\}$ độc lập tuyến tính.

p-nhóm aben sơ cấp

Một p-nhóm được gọi là *p-nhóm aben sơ cấp* nếu nó là tổng trực tiếp của hữu hạn nhóm cyclic cấp p.

Hệ quả 4

Cho G là một nhóm aben hữu hạn và p nguyên tố. Khi đó, nếu mọi phần tử khác 0 trong G đều có cấp p thì G là một p-nhóm aben sơ cấp.

Chứng minh

Với mọi $x \neq 0$ trong G, nếu $mx = 0$ thì do x có cấp p nên $p \mid m$. Suy ra, $\overline{m} = \overline{0}$ trong $\mathbb{Z}_p$. Do đó, G được xem như là một không gian vectơ trên $\mathbb{Z}_p$. Do G hữu hạn nên tồn tại một cơ sở $\{x_1, \ldots, x_r\}$ (trong không gian vectơ G) mà cơ sở này là một tập sinh độc lập tuyến tính, nên theo Mệnh đề 3, $G = \langle x_1, \ldots, x_r \rangle = \langle x_1 \rangle \oplus \cdots \oplus \langle x_r \rangle$. Do đó G là p-nhóm aben sơ cấp.

Định lý 5 (Định lý cơ sở)

Mọi nhóm aben G hữu hạn đều là tổng trực tiếp của các nhóm con p-nguyên sơ cyclic.

Chứng minh

Hiển nhiên từ Định lý 8 (§6).

Mệnh đề 6

Mọi nhóm aben G hữu hạn đều là tổng trực tiếp của các nhóm cyclic $\langle x_1\rangle$, $\langle x_2\rangle$, ..., $\langle x_t\rangle$, sao cho x_i có cấp m_i và $m_1 \mid m_2 \mid \ldots \mid m_t$.

Chứng minh

Do Định lý 2, ta có thể giả sử G có sự phân tích nguyên sơ là $G = \sum_{i=1}^{r} G_{p_i}$. Do Định lý cơ sở (Định lý 5), mỗi G_{p_i} là tổng trực tiếp của các nhóm cyclic. Đặt C_i là thành phần cyclic có cấp lớn nhất trong G_{p_i} và ký hiệu $|C_i| = {p_i}^{e_i}$. Khi đó, $G = K \oplus (C_1 \oplus \cdots \oplus C_r)$, với K là tổng trực tiếp của các thành phần cyclic còn lại. Nhưng do các ${p_i}^{e_i}$ nguyên tố cùng nhau nên $C_1 \oplus \cdots \oplus C_r$ lại là một nhóm cyclic có cấp $m = {p_1}^{e_1} \ldots {p_r}^{e_r}$. Lặp lại quá trình trên bằng cách thay G bởi K đến khi nào không còn các thành phần cyclic trong các G_{p_i}. Khi đó ta được điều cần chứng minh.

§7. Nhóm aben tự do

Nhóm aben tự do

Một nhóm aben F được gọi là *nhóm aben tự do* nếu F là tổng trực tiếp của các nhóm cyclic có cấp vô hạn.
Nghĩa là tồn tại một tập hợp $X \subset F$ gồm các phần tử có cấp vô hạn (gọi là *cơ sở* của F) sao cho $F = \sum\limits_{x \in X} \langle x \rangle$, hay $F \simeq \oplus \mathbb{Z}$.

Dễ thấy rằng, nếu X là một cơ sở của nhóm aben tự do F thì với mỗi $u \in F$, tồn tại duy nhất một dạng biểu diễn

$$u = \sum_{\text{hữu hạn}} m_x x,\ x \in X,\ m_x \in \mathbb{Z}.$$

Từ Mệnh đề 3 suy ra, cơ sở của nhóm aben là một tập độc lập tuyến tính.

§7. Nhóm aben tự do

Định lý 7

Cho G là một nhóm aben bất kỳ, F là một nhóm aben tự do với cơ sở X và $f : X \to G$ là một ánh xạ. Khi đó, tồn tại duy nhất một đồng cấu $\varphi : F \to G$ sao cho $\varphi|_X = f$, nghĩa là $\forall x \in X, \varphi(x) = f(x)$.

Chứng minh

Nếu $u \in F$ thì tồn tại duy nhất dạng biểu diễn $u = \sum m_i x_i, x_i \in X$. Đặt $\varphi(u) = \sum m_i f(x_i)$. Dễ dàng chứng minh φ là một đồng cấu từ F vào G. Hiển nhiên, với mọi $x \in X, \varphi(x) = f(x)$. Tính duy nhất được suy ra từ tính chất của đồng cấu.

Hệ quả 8

Một nhóm aben G bất kỳ luôn đẳng cấu với một nhóm thương của một nhóm aben tự do.

Chứng minh

Đặt F là tổng trực tiếp của $|G|$ lần $\mathbb{Z}$ và x_g là phần tử sinh của thành phần thứ g trong tổng trực tiếp, với $g \in G$. Rõ ràng F là một nhóm aben tự do với cơ sở $X = \{x_g, g \in G\}$. Đặt $f : X \to G; x_g \mapsto g$. Do Định lý 7, tồn tại một đồng cấu $\varphi : F \to G$ là mở rộng của F. Do f là toàn ánh nên φ là một toàn cấu, như vậy $G \simeq F/\ker\varphi$.

Từ chứng minh của Hệ quả 8 nhận thấy rằng, với X là một tập hợp bất kỳ cho trước, luôn xây dựng được một nhóm aben tự do F lấy X làm cơ sở. Hệ quả này cung cấp một phương pháp mới để mô tả các nhóm aben.

Định lý 9

Cho F và F' là hai nhóm aben tự do với các cơ sở tương ứng là X và X'. Khi đó, $F \simeq F'$ khi và chỉ khi $|X| = |X'|$.

Chứng minh

Nếu $|X| = |X'|$ thì tồn tại một song ánh $f : X \to X' \subseteq F'$. Do đó F xác định một đồng cấu $\varphi : F \to F'$ sao cho $\forall x \in X, \varphi(x) = f(x)$. Tương tự, tồn tại một đồng cấu $\psi : F' \to F$ sao cho $\forall x' \in X', \varphi(x') = f^{-1}(x')$. Nhưng $\varphi\psi$ và $\psi\varphi$ là các ánh xạ đồng nhất vì chúng cố định mọi phần tử trong một cơ sở. Do đó $\psi = \varphi^{-1}$. Vậy φ là một đẳng cấu từ F vào F'.

Chứng minh (tiếp theo)

Ngược lại, cho p là một số nguyên tố. Khi đó, $V = F/pF$ là một không gian vectơ trên trường $\mathbb{Z}_p$. Đặt $\overline{X} = \{x + pF | x \in X\}$. Rõ ràng $\overline{X}$ là một tập sinh của V. Giả sử $\sum\limits_{x\in X} [m_x](x + pF) = 0, [m_x] \in \mathbb{Z}_p$. Ký hiệu $m_x \in \mathbb{Z}$ là phần tử đại diện của $[m_x]$. Khi đó, đẳng thức trên suy ra $\sum\limits_{x\in X} m_x x \in pF$. Do đó, tồn tại các $n_x \in \mathbb{Z}$ sao cho $\sum\limits_{x\in X} m_x x = \sum\limits_{x\in X} pn_x x$. Nhưng do X là cơ sở của F nên X độc lập tuyến tính và mọi phần tử trong X đều có cấp vô hạn nên với mọi $x \in X$, $m_x = pn_x$, kéo theo $[m_x] = [0]$. Do đó $\overline{X}$ độc lập tuyến tính. Vậy $\overline{X}$ là một cơ sở của V. Suy ra, $\dim V = |\overline{X}| = |X|$. Chứng minh tương tự ta được $\dim V = |X'|$. Do đó $|X| = |X'|$.

§7. Nhóm aben tự do

Hạng của nhóm aben tự do

Như vậy, với F là một nhóm aben tự do thì hai cơ sở bất kỳ của nó có cùng số phần tử. Số phần tử trong một cơ sở của F được gọi là *hạng* của F, ký hiệu là $rank(F)$.

Rõ ràng, nếu F và G là hai nhóm aben tự do thì $rank(F \oplus G) = rankF + rankG$.

§7. Nhóm aben tự do

Mệnh đề 10

Nếu $H \trianglelefteq G$ và G/H là một nhóm aben tự do thì tồn tại $K \leq G$ sao cho $G = H \oplus K$.

Chứng minh

Đặt $F = G/H$ và $X = \{x_i + H, i \in I\}$ là một cơ sở của F. Xét ánh xạ $f : X \to G; x_i + H \mapsto x_i$. Do Định lý 7, tồn tại duy nhất một đồng cấu $\psi : F \to G$ là mở rộng của f. Đặt $K = \text{Im}\psi \leq G$. Rõ ràng $G = H + K$ và $H \cap K = 0$, nên $G = H \oplus K$.

§7. Nhóm aben tự do

Định lý 11

Mọi nhóm con H của một nhóm aben tự do F có hạng hữu hạn là một nhóm aben tự do với $rank(H) \leq rank(F)$.

Chứng minh

Ta chứng minh bằng quy nạp theo $n = rank(F)$. Nếu $n = 1$ thì F là một nhóm cyclic và $F \simeq \mathbb{Z}$, nên nhóm con H của F cũng là một nhóm cyclic, do đó $H = 0$ hoặc $H \simeq \mathbb{Z}$, suy ra H là một nhóm aben tự do với $rank(H) \leq 1$. Giả sử $n > 1$ và $\{x_1, \ldots, x_n\}$ là một cơ sở của F. Đặt $F' = \langle x_1, \ldots, x_{n-1} \rangle$ và $H' = H \cap F' \leq F$. Theo quy nạp, H' là một nhóm aben tự do với hạng $\leq n-1$. Hơn nữa, $H/H' = H/(H \cap F') \simeq (H + F')/F' \leq F/F' \simeq \mathbb{Z}$. Do đó (theo bước cơ sở quy nạp), $H/H' = 0$ hoặc $H/H' \simeq \mathbb{Z}$.

§7. Nhóm aben tự do

Chứng minh (tiếp theo)

Nếu $H/H' = 0$ thì $H = H'$ nên H là nhóm aben tự do có hạng $\leq n-1$, nếu $H/H' \simeq \mathbb{Z}$ thì, từ Mệnh đề 10 suy ra, tồn tại $h \in H$ với $\langle h \rangle \simeq \mathbb{Z}$ sao cho $H = H' \oplus \langle h \rangle$. Do đó, H là nhóm aben tự do, với $rank(H) = rank(H' \oplus \mathbb{Z}) = rank(H') + 1 \leq n$.

Nhóm không xoắn

Cho G là một nhóm aben. Khi đó, G được gọi là một *nhóm không xoắn* nếu mọi phần tử khác 0 trong G đều có cấp vô hạn.

Định lý 12

Mọi nhóm G aben hữu hạn sinh không xoắn đều là nhóm aben tự do.

Chứng minh

Ta chứng minh bằng quy nạp theo số phần tử sinh n của G. Nếu $n = 1$ và $G \neq 0$ thì rõ ràng G là một nhóm cyclic cấp vô hạn (do G là nhóm không xoắn) nên $G \simeq \mathbb{Z}$, do đó G là nhóm aben tự do.
Giả sử $G = \langle x_1, \ldots, x_n \rangle$ và định lý đúng cho mọi nhóm aben không xoắn có số phần tử sinh nhỏ hơn n. Đặt $H = \{g \in G | \exists m \in \mathbb{Z}, mg \in \langle x_n \rangle\}$. Rõ ràng, H là một nhóm con của G. Hơn nữa, nếu tồn tại $k \in \mathbb{Z}$ sao cho $k(x + H) = 0$ thì $kx \in H$ nên tồn tại $m \in \mathbb{Z}$ để $m(kx) \in \langle x_n \rangle$. Suy ra $x \in H$, do đó $x + H = 0$, nên G/H là một nhóm không xoắn và G/H có thể được sinh bởi ít hơn n phần tử (chẳng hạn có tập sinh là $\{x_1 + H, \ldots, x_{n-1} + H\}$).

Chứng minh (tiếp theo)

Do đó, theo giả thiết quy nạp, G/H là một nhóm aben tự do. Do Mệnh đề 10, tồn tại $K \leq G$ sao cho $G = H \oplus K$ và $K \simeq G/H$ là nhóm aben tự do nên chỉ cần chứng minh H aben tự do là đủ.
Thật vậy, do G hữu hạn sinh nên H cũng hữu hạn sinh, giả sử $H = \langle h_1, \ldots, h_r \rangle, h_i \neq 0, \forall i$. Với mỗi i, tồn tại $0 \neq m_i \in \mathbb{Z}$ sao cho $m_i h_i = \langle x_n \rangle$. Đặt $b = m_1 m_2 \ldots m_r \neq 0$. Suy ra $bh_i \in \langle x_n \rangle, \forall i$, do đó $bH \leq \langle x_n \rangle \simeq \mathbb{Z}$. Hơn nữa, do H là nhóm không xoắn và $H \simeq bH$ nên ta suy ra H đẳng cấu với một nhóm con của $\mathbb{Z}$, do đó H là một nhóm cyclic có cấp vô hạn, hay H là một nhóm aben tự do.

BÀI TẬP

Bài 7.1

Chứng minh rằng, nhóm G aben là hữu hạn sinh nếu và chỉ nếu G là nhóm thương của một nhóm aben tự do có hạng hữu hạn.

Bài 7.2

Chứng minh rằng, mọi nhóm con H của một nhóm aben hữu hạn sinh là hữu hạn sinh. Hơn nữa, nếu G sinh bởi r phần tử thì H có thể sinh bởi một tập hợp có không quá r phần tử.

Bài 7.3

Chứng minh rằng, nhóm nhân $\mathbb{Q}^+$ là một nhóm aben tự do (với hạng vô hạn đếm được).

BÀI TẬP

Bài 7.4

Chứng minh rằng, nếu F là một nhóm tự do có hạng bằng n thì $Aut(F)$ đẳng cấu với nhóm nhân các ma trận vuông cấp n trên $\mathbb{Z}$ với định thức bằng ± 1.

Bài 7.5

Giả sử F là một nhóm aben tự do có hạng bằng n. Chứng minh rằng, nếu H là một nhóm con có chỉ số hữu hạn trong F thì $rank(H) = n$. Đồng thời, tồn tại các cơ sở $\{x_1, \ldots, x_n\}$ của F và $\{h_1, \ldots, h_n\}$ của H sao cho $h_i \in \langle x_i \rangle$ với mọi i.

BÀI TẬP

Bài 7.6

a) Chứng minh rằng, nếu F là một nhóm aben tự do có hạng bằng n và H là một nhóm con của F có hạng bằng $k < n$ thì nhóm thương F/H có ít nhất một phần tử có cấp vô hạn.
b) Cho F là một nhóm aben tự do có hạng bằng n và H là một nhóm con của F. Chứng minh rằng, H là nhóm aben tự do có hạng bằng n khi và chỉ khi H có chỉ số hữu hạn trong F.

Bài 7.7

Cho G là một nhóm aben không xoắn. Chứng minh rằng, nếu G có một nhóm con aben tự do với chỉ số hữu hạn thì G là nhóm aben tự do.

Chương 2

VÀNH VÀ MIỀN NGUYÊN

Giảng viên: **TS. TRỊNH THANH ĐÈO**

Khoa Toán - Tin học
Trường Đại học Khoa học Tự nhiên, ĐHQG-HCM

NỘI DUNG

§1. Vành và đồng cấu vành

Vành

Một *vành* $(R, +, .)$ là tập hợp R cùng với hai phép toán $+$ (cộng) và $.$ (nhân) thỏa mãn các tính chất sau đây:
(i) $(R, +)$ là nhóm aben.
(ii) $(R, .)$ là nửa nhóm.
(iii) Với mọi $a, b, c \in R$, $\begin{cases} a.(b+c) = a.b + a.c, \\ (b+c).a = b.a + c.a. \end{cases}$

Cũng như trong nhóm, ta viết ab thay cho $a.b$. Ngoài ra, ta ký hiệu 0 là phần tử trung hòa của nhóm $(R, +)$ và gọi nó là *phần tử không* của vành $(R, +, .)$. Để đơn giản, ta cũng dùng ký hiệu R để chỉ vành $(R, +, .)$ nếu như không có gì phải nhấn mạnh đến các phép toán trong R.

§1. Vành và đồng cấu vành

Vành có đơn vị

Nếu $R \neq \{0\}$ và nửa nhóm nhân $(R, .)$ có đơn vị 1 thì R được gọi là *vành có đơn vị* với đơn vị là 1 . Trong trường hợp này ta có $1 \neq 0$ (xem Mệnh đề 1).

Vành giao hoán

Nếu $(R, .)$ là nửa nhóm giao hoán, nghĩa là $\forall a, b \in R$, $ab = ba$, thì ta nói R là *vành giao hoán*.

Mệnh đề 1

Cho R là vành. Khi đó, với mọi $a, b, c \in R$ ta có:
i) $a0 = 0a = 0$.
ii) $(-a)b = a(-b) = -(ab)$ và $(-a)(-b) = ab$.
iii) $a(b-c) = ab - ac$ và $(b-c)a = ba - ca$.
iv) Nếu R có đơn vị thì $1 \neq 0$ và $(-1)a = -a$.

Chứng minh

i) Ta có $a0 = a(0+0) = a0 + a0$, suy ra $a0 = 0$.
ii) Ta có $(-a)b + ab = ((-a) + a)b = 0b = 0$, nên $(-a)b = -(ab)$.
Tương tự, $a(-b) = -(ab)$ và $(-a)(-b) = ab$.
iii) Ta có $a(b-c) = a(b + (-c)) = ab + a(-c) = ab - ac$.
Tương tự, $(b-c)a = ba - ca$.
iv) Ta có $(-1)a = 1(-a) = -a$.
Nếu $1 = 0$ thì $a = a1 = a0 = 0$, nên $R = \{0\}$, mâu thuẫn.

§1. Vành và đồng cấu vành

Ước của không

Nếu a và b là các phần tử khác 0 của vành R sao cho $ab = 0$ thì ta nói a và b tương ứng là *ước trái* và *ước phải* của không. Nếu a vừa là ước trái vừa là ước phải của không thì ta nói a là *ước của không*.

Miền nguyên

Vành giao hoán, có đơn vị và không có ước của không được gọi là *miền nguyên*.

§1. Vành và đồng cấu vành

Bổ đề 2

Cho R là vành và $a, b, c \in R$. Khi đó:
- Nếu a không là ước trái của không thì từ $ab = ac$ kéo theo $b = c$.
- Nếu a không là ước phải của không thì từ $ba = ca$ kéo theo $b = c$.

Chứng minh

Nếu $ab = ac$ thì $ab - ac = 0$. Theo Mệnh đề 1iv) ta có $a(b - c) = 0$.
Do a không là ước trái của không nên $b - c = 0$, hay $b = c$.
Điều còn lại chứng minh tương tự.

§1. Vành và đồng cấu vành

Đặc trưng của vành

Cho R là vành có đơn vị. Ta gọi *đặc trưng* của vành R là số tự nhiên n nhỏ nhất sao cho $n.1 = 0$, ký hiệu là $n = \text{char}(R)$. Nếu $n.1 \neq 0, \forall n \in \mathbb{N}$ thì ta nói vành R có *đặc trưng* 0, ký hiệu $\text{char}(R) = 0$.

Mệnh đề 3

Nếu R là một miền nguyên thì $\text{char}(R) = 0$ hoặc là một số nguyên tố.

Chứng minh

Giả sử $n = \text{char}(R) \neq 0$. Nếu n không là số nguyên tố thì $n = rs$, với $1 < r, s < n$. Từ định nghĩa suy ra $r.1 \neq 0$ và $s.1 \neq 0$. Do R là miền nguyên nên $n.1 = (r.1)(s.1) \neq 0$, mâu thuẫn. Vậy n là số nguyên tố.

§1. Vành và đồng cấu vành

Phần tử khả nghịch

Nếu R có đơn vị và $a, b \in R$ sao cho $ab = 1$ thì ta nói a và b tương ứng là *khả nghịch phải* và *khả nghịch trái*. Khi đó b là *nghịch đảo phải* của a và a là *nghịch đảo trái* của b. Phần tử $a \in R$ được gọi là *khả nghịch* nếu a vừa khả nghịch phải vừa khả nghịch trái.

Dễ thấy a khả nghịch khi và chỉ khi tồn tại duy nhất một phần tử b sao cho $ab = ba = 1$. Ta nói b là *nghịch đảo* của a và ký hiệu $b = a^{-1}$. Tập tất cả các phần tử khả nghịch của R được ký hiệu là R^*. Rõ ràng $(R^*, .)$ là một nhóm, gọi là *nhóm các phần tử khả nghịch* của R. Nếu a khả nghịch phải hoặc khả nghịch trái thì đôi khi ta sẽ nói a *khả nghịch một phía*. Một phần tử khả nghịch một phía thì chưa chắc khả nghịch.

§1. Vành và đồng cấu vành

Vành chia và trường

Một vành R có đơn vị được gọi là một *vành chia* hay một *thể*, nếu $R^* = R \setminus \{0\}$, nghĩa là mọi phần tử khác không của R đều khả nghịch. Một vành chia giao hoán được gọi là một *trường*.

§1. Vành và đồng cấu vành

Mệnh đề 4

Cho R là một vành có đơn vị. Khi đó, nếu mọi phần tử khác 0 của R đều khả nghịch phải (hoặc khả nghịch trái) thì R là vành chia.

Chứng minh

Giả sử mọi phần tử khác 0 của R đều khả nghịch phải và $0 \neq a \in R$. Khi đó tồn tại $0 \neq b \in R$ sao cho $ab = 1$. Nhưng do $b \neq 0$ nên tồn tại $0 \neq c \in R$ sao cho $bc = 1$. Suy ra $a = a.1 = a(bc) = (ab)c = 1.c = c$, dẫn đến $ab = ba = 1$, nghĩa là a khả nghịch. Trường hợp còn lại chứng minh tương tự.

§1. Vành và đồng cấu vành

Vành con

Tập con $S \neq \emptyset$ của vành R được gọi là *vành con* của R nếu S là một vành với các phép toán cộng và nhân trong R.

Nhận xét 1

Tập $S \neq \emptyset$ là vành con của R nếu và chỉ nếu S là nhóm con của nhóm $(R, +)$ và S là nửa nhóm con của nửa nhóm $(R, .)$.

§1. Vành và đồng cấu vành

Nhận xét 2

Giao của một họ bất kỳ các vành con của vành R cũng là một vành con của R.

Vành con sinh bởi tập hợp

Cho S là một tập con khác $\emptyset$ của vành R. Khi đó, giao của tất cả các vành con của R chứa S được gọi là *vành con của R sinh bởi S*.

Vành con của R sinh bởi tập S chính là vành con nhỏ nhất của R chứa S.

Mệnh đề 5

Cho S là tập con khác $\emptyset$ của vành R. Khi đó, vành con của R sinh bởi S là $\left\{ \sum_{\text{hữu hạn}} (\pm s_1 s_2 \dots s_n), s_i \in S \right\}$.

Chứng minh

Đặt T là tập tất cả các phần tử có dạng $\sum_{\text{hữu hạn}} (\pm s_1 s_2 \dots s_n),\ s_i \in S$.

Rõ ràng T là một vành con của R chứa S. Hơn nữa, mọi vành con của R chứa S đều chứa các phần tử có dạng nói trên. Do đó T chính là vành con nhỏ nhất của R chứa S.

Ideal

- Tập con $I \neq \emptyset$ của vành R được gọi là *ideal phải* (t.ư. *trái*) của R, nếu $(I, +)$ là nhóm con của $(R, +)$ và với mọi $a \in I, r \in R$ ta có $ar \in I$ (t.ư. $ra \in I$).
- Nếu I vừa là ideal phải vừa là ideal trái của R thì ta nói I là *ideal hai phía* (hay I là *ideal*) của R.
- Ideal phải (trái, hai phía) khác R gọi là *ideal phải* (*trái*, *hai phía*) *thực sự* của R.

- Nếu R là vành giao hoán thì khái niệm ideal phải trùng với khái niệm ideal trái, do đó trong trường hợp này ta chỉ cần dùng tới khái niệm ideal mà thôi.
- Nếu R là vành không giao hoán thì ta dùng thuật ngữ *ideal một phía* để chỉ các ideal phải hoặc trái nhằm phân biệt với các ideal hai phía.
- Mọi ideal một phía hoặc hai phía của vành R đều là vành con của R, nhưng điều ngược lại không đúng. Chẳng hạn trong vành $\mathbb{Q}$ các số hữu tỉ thì tập $\mathbb{Z}$ các số nguyên là vành con nhưng không là ideal của nó.

Nhận xét 3

Giao của một họ bất kỳ các ideal của vành R lại là một ideal của R.

Ideal sinh bởi tập hợp

Cho S là một tập con khác $\emptyset$ của vành R. Khi đó, giao của tất cả các ideal của R chứa S được gọi là *ideal của R sinh bởi S*, ký hiệu $\langle S\rangle$

Nhận xét 4

Ideal của R sinh bởi tập S chính là ideal nhỏ nhất của R chứa S.

Nếu $I = \langle S\rangle$ thì ta nói *I sinh bởi S*, *S là tập sinh của I*; các phần tử của S gọi là *các phần tử sinh của I*. Ideal của R sinh bởi $\{a\}$ được viết là $\langle a\rangle$, gọi là *ideal chính sinh bởi a*. Lưu ý rằng, nếu R là vành giao hoán có đơn vị thì $\langle a\rangle = Ra$.

Mệnh đề 6

Cho R là vành có đơn vị và S là một tập con khác $\emptyset$ của R. Khi đó:

- $\langle S\rangle = \left\{ \sum\limits_{\text{hữu hạn}} x_i s_i y_i \mid x_i, y_i \in R, s_i \in S \right\}$.
- Nếu R giao hoán thì $\langle S\rangle = \left\{ \sum\limits_{\text{hữu hạn}} x_i s_i \mid x_i \in R, s_i \in S \right\}$.

Chứng minh

Chứng minh tương tự Mệnh đề 5.

§1. Vành và đồng cấu vành

Tổng, tích các ideal

Cho I, J là các ideal của vành R. Đặt $I + J = \{a + b \mid a \in I, b \in J\}$ và $IJ = \{\sum a_i b_i \mid a_i \in I, b_i \in J\}$ và ta gọi $I + J, IJ$ tương ứng là *tổng* và *tích* của các ideal I và J.

Bằng quy nạp, cũng có khái niệm tổng và tích của nhiều ideal.

Mệnh đề 7

Tổng và tích các ideal là các ideal. Hơn nữa, $I + J$ là ideal của R sinh bởi $I \cup J$.

Chứng minh

Dễ dàng chứng minh

§1. Vành và đồng cấu vành

Vành thương

Nếu I là ideal (hai phía) của vành R thì trong nhóm thương $(R/I, +)$ ta định nghĩa thêm phép toán nhân bởi: $(x + I)(y + I) := xy + I, \forall x, y \in R$.
Khi đó $(R/I, +, .)$ trở thành một vành, gọi là *vành thương* của R theo I.

- Nếu R là vành có đơn vị 1 thì R/I là vành có đơn vị là $1 + I$.
- Nếu R giao hoán thì R/I cũng giao hoán, nhưng điều ngược lại không đúng.

§1. Vành và đồng cấu vành

Đồng cấu vành

Cho R và S là các vành và $f : R \to S$ là một ánh xạ. Ta nói f là một *đồng cấu vành* nếu với mọi $x, y \in R$, $f(x+y) = f(x) + f(y)$ và $f(xy) = f(x)f(y)$.

Nếu R và S có đơn vị thì ta có thêm điều kiện $f(1) = 1$.

Nhân của đồng cấu

Cho $f : R \to S$ là một đồng cấu vành. Đặt $\ker f = \{x \in R \mid f(x) = 0\}$ và ta gọi $\ker f$ là *nhân* của f.

§1. Vành và đồng cấu vành

Nhận xét 5

Dễ dàng kiểm tra rằng $\ker f$ là ideal của R.

Ảnh của đồng cấu

Cho $f : R \to S$ là một đồng cấu vành. Đặt $\mathrm{Im}f = \{f(x) \mid x \in R\}$ và ta gọi $\mathrm{Im}f$ là *ảnh* của f.

Nhận xét 6

Dễ dàng kiểm tra rằng $\mathrm{Im}f$ là vành con của S.

§1. Vành và đồng cấu vành

Đơn cấu

Nếu $\ker f = 0$ thì ta nói f là một *đơn cấu*.

Toàn cấu

Nếu $\mathrm{Im} f = S$ thì ta nói f là một *toàn cấu*.

Đẳng cấu

Nếu f vừa là đơn cấu vừa là toàn cấu thì ta nói f là *đẳng cấu*.
Trong trường hợp này ta nói R đẳng cấu với S, ký hiệu là $R \cong S$.

§1. Vành và đồng cấu vành

Định lý 8 (Định lý đẳng cấu thứ nhất)

Nếu $f : R \to S$ là một đồng cấu vành thì $R/\ker f \simeq \mathrm{Im} f$.

Chứng minh

Xét ánh xạ $\overline{f} : R/\ker f \to \mathrm{Im} f$ xác định bởi $\overline{f}(a + \ker f) = f(a)$. Tương tự kết quả ở Chương 1, ta thấy đây là định nghĩa tốt và $R/\ker f \cong \mathrm{Im} f$ như các nhóm aben đối với phép toán cộng. Với các phần tử bất kỳ a và b của R, ta có $\overline{f}((a + I)(b + I)) = \overline{f}(ab + I) = f(ab) = f(a)f(b) = \overline{f}(a + I)\overline{f}(b + I)$.
Vậy $\overline{f}$ còn là một đẳng cấu vành.

Định lý 9 (Định lý đẳng cấu thứ hai)

Cho R là vành, I là ideal và S là vành con của R. Khi đó $S+I$ là vành con của R, I là ideal của $S+I$, $S\cap I$ là ideal của S và ta có đẳng cấu $(S+I)/I \cong S/(S\cap I)$.

Chứng minh

Gọi σ_0 là hạn chế của đồng cấu tự nhiên $\sigma : R \to R/I$ lên S. Khi đó $\mathrm{Im}\sigma_0 = (S+I)/I$ và $\ker\sigma_0 = S\cap I$. Ngoại trừ công thức sau cùng, các khẳng định khác đều hiển nhiên. Bây giờ, áp dụng Định lý đẳng cấu thứ nhất, nhận được $(S+I)/I \cong S/(S\cap I)$.

Định lý 10 (Định lý đẳng cấu thứ ba)

Cho R là vành, I và J là các ideal của R thỏa $I \subseteq J$. Khi đó J/I là ideal của R/I và $R/J \cong (R/I)/(J/I)$.

Chứng minh

Định nghĩa ánh xạ $f : R/I \to R/J$ xác định bởi $f(a+I) = a+J$. Nếu $a, b \in R$ sao cho $a+I = b+I$ thì $a-b \in I \subseteq J$, suy ra $a+J = b+J$. Vậy, ánh xạ f nói trên được định nghĩa tốt. Rõ ràng f là toàn cấu và f có nhân là J/I.

Áp dụng Định lý đẳng cấu thứ nhất nhận được $R/J \cong (R/I)/(J/I)$.

Định lý 11 (Định lý về sự tương ứng

Cho R là vành, I là ideal của R và $\sigma : R \to R/I$ là đồng cấu tự nhiên. Khi đó ánh xạ $S \mapsto S/I$ xác định một song ánh giữa tập tất cả các vành con của R chứa I và tập tất cả các vành con của R/I. Với sự tương ứng này, các ideal của R chứa I ứng với các ideal của R/I.

Chứng minh

Đặt $\mathcal{L}_1$ là tập tất cả các nhóm con của $(R, +)$ chứa I và $\mathcal{L}_2$ là tập tất cả các nhóm con của $(R/I, +)$. Theo Định lý về sự tương ứng trong lý thuyết nhóm ta có song ánh $\psi : \mathcal{L}_1 \to \mathcal{L}_2; H \mapsto H/I$ biến các nhóm con của $(R, +)$ chứa I thành các nhóm con của $(R/I, +)$. Dễ thấy, nếu S là vành con của R thì $\psi(S)$ là vành con của R/I. Ngược lại, nếu S' là vành con của R/I thì $\psi^{-1}(S')$ là vành con của R. Ta cũng có kết luận tương tự cho các ideal.

Định lý 12

Cho K là một trường. Khi đó:
- Nếu $\operatorname{char} K = 0$ thì K chứa một trường con đẳng cấu với $\mathbb{Q}$.
- Nếu $\operatorname{char} K = p > 0$ thì K chứa một trường con đẳng cấu với $\mathbb{Z}_p$.

Chứng minh

Từ Mệnh đề 3 ta được $\operatorname{char} K = 0$ hoặc $\operatorname{char} K = p$, với p là số nguyên tố. Xét ánh xạ $\varphi : \mathbb{Z} \to K$ xác định bởi $\varphi(m) = m.1$. Dễ thấy φ là đồng cấu vành.
- Nếu $\operatorname{char} K = 0$ thì $\ker \varphi = 0$, nên $\mathbb{Z} = \mathbb{Z}/\ker \varphi \cong \operatorname{Im}\varphi$, nghĩa là $\mathbb{Z}$ nhúng được vào trong K. Vì K là trường nên trường các thương của $\mathbb{Z}$ (chính là $\mathbb{Q}$) cũng nhúng được vào trong K.
- Nếu $\operatorname{char} K = p > 0$ thì $\ker \varphi = p\mathbb{Z} \neq 0$, nên $\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \operatorname{Im}\varphi \subset K$. Hơn nữa, do p nguyên tố nên $\mathbb{Z}_p$ là trường.

Ví dụ 1 (Một số ví dụ mở đầu)

Với $n \in \mathbb{N}, n > 1$ ta có $n\mathbb{Z} := \{na \mid a \in \mathbb{Z}\}$ là một ideal của $\mathbb{Z}$ và $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. Hơn nữa, vành $n\mathbb{Z}$ không là miền nguyên do nó không có đơn vị.
Vành $\mathbb{Z}_n$ là vành giao hoán có đơn vị $\overline{1}$. Nếu n là hợp số thì $\mathbb{Z}_n$ có ước của không nên không là miền nguyên; nếu p là số nguyên tố thì $\mathbb{Z}_p$ không có ước của không. Hơn nữa, mọi phần tử khác 0 cuả $\mathbb{Z}_p$ đều khả nghịch, nên $\mathbb{Z}_p$ là một trường. Đây là ví dụ đầu tiên về *trường hữu hạn*.
Tồn tại rất nhiều trường hữu hạn khác với $\mathbb{Z}_p$. Trong lý thuyết trường, ta có kết quả sau: Với $n \in \mathbb{N}$ và p là một số nguyên tố, tồn tại duy nhất (sai khác một đẳng cấu) một trường hữu hạn có p^n phần tử, ký hiệu là $\mathbb{F}_{p^n}$.
Với các phép toán cộng và nhân thông thường, ta có các trường vô hạn có đặc số 0 sau đây: trường $\mathbb{Q}$ các số hữu tỷ, trường $\mathbb{R}$ các số thực và trường $\mathbb{C}$ các số phức.

Ví dụ 2 (Vành các số nguyên Gauss)

Ta có $\mathbb{Z}[i] := \{a + bi \mid \ a, b \in \mathbb{Z}\}$ là một vành con của $\mathbb{C}$, gọi là *vành các số nguyên Gauss*. Trong $\mathbb{Z}[i]$ chỉ có bốn phần tử khả nghịch là ± 1 và $\pm i$.

Ví dụ 3 (Trường quadratic)

Giả sử $d \in \mathbb{Z}, d \neq 0, 1$ và d không có thừa số chính phương (nghĩa là d không chia hết cho $n^2, \forall n \in \mathbb{N}$). Đặt $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. Khi đó $\mathbb{Q}(\sqrt{d})$ là trường con của $\mathbb{R}$, được gọi là *trường quadratic*.

Ví dụ 4 (Vành ma trận)

Cho R là vành giao hoán có đơn vị. Khi đó tập $M_n(R)$ các ma trận vuông cấp n trên R là một vành với các phép toán cộng và nhân ma trận. Ta gọi $M_n(R)$ là *vành ma trận* trên R. Dưới đây là một số vành con quan trọng của $M_n(R)$:

- Vành các ma trận đường chéo $D_n(R) = \{(a_{ij}) \in M_n(R) \mid a_{ij} = 0, \forall i \neq j\}$.
- Vành các ma trận tam giác trên $T^n(R) = \{(a_{ij}) \in M_n(R) \mid a_{ij} = 0, \forall i > j\}$.
- Vành các ma trận tam giác dưới $T_n(R) = \{(a_{ij}) \in M_n(R) \mid a_{ij} = 0, \forall i < j\}$.
- Vành các ma trận tam giác trên ngặt $ST^n(R) = \{(a_{ij}) \in M_n(R) \mid a_{ij} = 0, \forall i \geq j\}$.
- Vành các ma trận tam giác dưới ngặt $ST_n(R) = \{(a_{ij}) \in M_n(R) \mid a_{ij} = 0, \forall i \leq j\}$.

Ta có $D_n(R), T^n(R), T_n(R)$ là các vành con chứa đơn vị của $M_n(R)$ và $ST^n(R), ST_n(R)$ là các vành con không có đơn vị của $M_n(R)$.

Ví dụ 5 (Vành các tự đồng cấu)

Cho A là một nhóm aben. Khi đó tập hợp $End(A)$ tất cả các tự đồng cấu của A là một vành giao hoán có đơn vị, với các phép toán cộng và nhân như sau: $(f+g)(a) = f(a) + g(a)$ và $(fg)(a) = f(g(a))$ với mọi $f, g \in End(A)$. Ta gọi $End(A)$ là *vành các tự đồng cấu trên* A.

Ví dụ 6 (Vành đối)

Cho R là một vành, ta xây dựng vành R^o như sau: về mặt tập hợp thì R^o trùng với R; phép toán cộng trong R^o chính là phép cộng trong R; phép nhân $\circ$ trong R^o xác định bởi $a \circ b = ba$ với mọi $a, b \in R^o$. Khi đó R^o là một vành, gọi là *vành đối* của vành R. Hiển nhiên R^o có đơn vị khi và chỉ khi R có đơn vị. Nếu R là vành giao hoán thì R^o trùng với R.

Ví dụ 7 (Đại số các quaternion xác định)

Cho F là trường con của $\mathbb{R}$ và $x, y \in F$ với $x > 0, y > 0$.
Đặt $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\mathbf{i} = \sqrt{x}i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\mathbf{j} = \sqrt{y}i \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\mathbf{k} = \sqrt{xy} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
Khi đó $Q(-x, -y, F) := \{a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in F\}$ là vành con của $M_2(\mathbb{C})$. Hơn nữa, tương ứng $a \mapsto a\mathbf{1}$ xác định một phép nhúng từ F vào $Q(-x, -y, F)$. Ta đồng nhất các phần tử của F với ảnh của nó qua phép nhúng nói trên. Khi đó ta có $\mathbf{i}^2 = -x, \mathbf{j}^2 = -y, \mathbf{k}^2 = -xy$, $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$, $\mathbf{ki} = -\mathbf{ik} = x\mathbf{j}$, $\mathbf{jk} = -\mathbf{kj} = y\mathbf{i}$. Nếu $h = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in Q(-x, -y, F)$, thì với $\overline{h} = a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$, ta có $h\overline{h} = (a^2 + xb^2 + yc^2 + xyd^2)\mathbf{1}$. Do đó, nếu $h \neq 0$ thì h khả nghịch và $h^{-1} = \alpha h$, trong đó $\alpha = 1/(a^2 + xb^2 + yc^2 + xyd^2)$. Vậy $Q(-x, -y, F)$ là một vành chia, nhưng không là trường, vì dễ thấy nó không giao hoán. Ta gọi $Q(-x, -y, F)$ là một *đại số quaternion xác định*.

Ví dụ 8 (Vành chia các quaternion)

Trong Ví dụ 7, nếu $F = \mathbb{R}$ thì tất cả các đại số quaternion $Q(-x, -y, \mathbb{R})$ đều đẳng cấu với nhau và ta gọi $\mathbb{H} := Q(-1, -1, \mathbb{R})$ là một *vành chia các quaternion* (chữ $\mathbb{H}$ được dùng để tôn vinh người phát minh ra vành chia các quaternion, nhà bác học Hamilton). Lưu ý rằng tập con $\{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ của $\mathbb{H}$ lập thành một nhóm nhân.

Nếu F là trường con thực sự của $\mathbb{R}$ thì không phải tất cả các đại số quaternion xác định $Q(-x, -y, F)$ đều đẳng cấu với nhau. Các đại số này phụ thuộc vào việc chọn các phần tử x và y.

Ví dụ 9 (Vành đa thức một biến)

Cho R là một vành có đơn vị 1 (không nhất thiết giao hoán). Ký hiệu $R[x]$ là tập tất cả các biểu thức dạng $f(x) = \sum_{i=0}^{\infty} a_i x^i$, với x là một biến, $a_i \in R$ và chỉ có hữu hạn các a_i là khác 0. Với $f(x) = \sum_{i=0}^{\infty} a_i x^i, g(x) = \sum_{i=0}^{\infty} b_i x^i \in R[x]$, ta định nghĩa $(f+g)(x) = \sum_{i=0}^{\infty}(a_i + b_i)x^i$ và $(fg)(x) = \sum_{k=0}^{\infty} c_k x^k$, với $c_k = \sum_{i+j=k} a_i b_j$.
Khi đó $R[x]$ trở thành một vành có đơn vị 1, gọi là *vành đa thức một biến* theo biến x; mỗi biểu thức $f(x) = \sum_{i=0}^{\infty} a_i x^i \in R[x]$ gọi là một *đa thức theo biến* x, các a_i gọi là các *hệ số* của f.
Nếu R là vành giao hoán thì $R[x]$ cũng là vành giao hoán.

Phép cộng hai đa thức được thực hiện bằng cách cộng các hệ số tương ứng của chúng và phép nhân được thực hiện một cách tự nhiên với quy ước rằng biến x giao hoán với mọi phần tử của R.
Nếu $f(x) = \sum_{i=0}^{\infty} a_i x^i \in R[x]$ thì số nguyên n lớn nhất sao cho $a_n \neq 0$ gọi là *bậc* của f, ký hiệu $n = \deg f$. Khi đó, nếu $0 \neq a \in R$ thì $a \in R[x]$ và $\deg a = 0$. Riêng phần tử 0 được quy ước có bậc bằng $-\infty$ ($\deg 0 = -\infty$).

Ví dụ 10 (Vành đa thức nhiều biến)

Tương tự Ví dụ 9, ta có thể định nghĩa vành đa thức n biến $R[x_1, ..., x_n]$, trong đó $x_1, ..., x_n$ là các biến độc lập, giao hoán với nhau và giao hoán với mọi phần tử của R (ta gọi R là *vành cơ sở* của $R[x_1, ..., x_n]$). Các phép toán cộng và nhân được định nghĩa một cách tương tự như trong trường hợp một biến.

Ví dụ 11 (Vành các chuỗi hình thức)

Cho R là vành có đơn vị 1. Ta gọi $\sum_0^\infty a_i x^i$, với $a_i \in R$, là một *chuỗi hình thức* theo biến x trên R. Khi đó, với các phép toán cộng và nhân tương tự như trong vành đa thức một biến x, tập $R[[x]]$ các chuỗi hình thức theo biến x trên R là một vành có đơn vị 1, gọi là *vành các chuỗi hình thức* theo biến x trên R, với quy ước là biến x giao hoán với mọi phần tử của vành R.

Nhận xét 7

$f = \sum_0^\infty a_i x^i$ khả nghịch trong $R[[x]]$ khi và chỉ khi a_0 khả nghịch trong R.

Chứng minh

Nếu $a_0 \in R^*$ thì để tìm $g = \sum_0^\infty b_i x^i \in R[[x]]$ sao cho $fg = 1$, ta tìm các hệ số của g qua các đẳng thức sau: $a_0b_0 = 1, a_0b_1 + a_1b_0 = 0, a_0b_2 + a_1b_1 + a_2b_0 = 0, \ldots$ Do a_0 khả nghịch nên ta tìm được b_0 từ đẳng thức thứ nhất, sau đó tìm được b_1 từ đẳng thức thứ hai, cứ tiếp tục như vậy ta tìm được tất cả các hệ số của g. Vậy f khả nghịch nếu a_0 khả nghịch trong R. Điều ngược lại là hiển nhiên.

Ví dụ 12 (Vành các chuỗi Laurent)

Cho R là một vành có đơn vị. Ký hiệu $R((x))$ là tập tất cả các chuỗi Laurent hình thức $\sum_{-\infty}^{\infty} a_i x^i$, trong đó $a_i \in R$ và chỉ có một số hữu hạn các hệ số a_i khác 0 đối với $i < 0$ cùng với phép cộng và phép nhân được định nghĩa tương tự như trong $R[x]$, với quy ước là biến x giao hoán với mọi phần tử của R. Khi đó $R((x))$ là một vành, gọi là *vành các chuỗi Laurent* theo biến x.

Nhận xét 8

Nếu R là vành chia thì $R((x))$ cũng là vành chia.

Chứng minh

Giả sử $F = \sum_{-\infty}^{\infty} a_i x^i$ là một phần tử khác không trong $R((x))$. Khi đó với một $i \in \mathbb{Z}$ thích hợp ta có $F.x^i = b_0 + b_1 x + b_2 x^2 + \ldots$, với $b_0 \neq 0$. Nếu R là vành chia thì $F.x^i$ khả nghịch trong vành các chuỗi hình thức $R[[x]]$. Khi đó, tồn tại $g \in R[[x]]$ sao cho $F.x^i g = 1$. Vì x^i hiển nhiên là phần tử khả nghịch trong $R((x))$ nên từ đó suy ra F khả nghịch trong $R((x))$.

Ví dụ 13 (Vành nhóm)

Cho R là vành có đơn vị và G là nhóm nhân. Ký hiệu RG là tập các biểu thức hình thức hữu hạn $\sum_{\sigma\in G} a_\sigma\sigma$, với $a_\sigma \in R$ và $a_\sigma = 0$ trừ một số hữu hạn các $\sigma \in G$.

Trên RG ta định nghĩa phép cộng và nhân các biểu thức nói trên như sau: $\Big(\sum_{\sigma\in G} a_\sigma\sigma\Big) + \Big(\sum_{\sigma\in G} b_\sigma\sigma\Big) = \sum_{\sigma\in G}(a_\sigma + b_\sigma)\sigma$ và $\Big(\sum_{\sigma\in G} a_\sigma\sigma\Big)\Big(\sum_{\tau\in G} b_\tau\tau\Big) = \sum_{\mu\in G} c_\mu\mu$, trong đó $c_\mu = \sum_{\sigma\tau=\mu} a_\sigma b_\tau$.

Khi đó RG là một vành có đơn vị, gọi là một *vành nhóm* RG.

Hiển nhiên ta có thể đồng nhất phần tử $a \in R$ với $a.1 \in RG$. Tương tự, ta có thể đồng nhất phần tử $\sigma \in G$ với $1.\sigma \in RG$. Ta cũng nhận thấy rằng RG giao hoán khi và chỉ khi cả R và G đều giao hoán.

Nhận xét 9

Rõ ràng G là nhóm con của $(RG)^*$ và $R^*G \subseteq (RG)^*$. Tuy nhiên, trong trường hợp tổng quát thì $(RG)^*$ có thể thực sự chứa $R^*.G$. Ví dụ sau đây chứng tỏ điều đó. Xét vành nhóm $\mathbb{Z}G$, trong đó $G = \langle x\rangle$ là nhóm cyclic cấp 5 sinh bởi x. Với $a = 1 - x^2 - x^3$ và $b = 1 - x - x^4$, ta có $ab = 1$. Như vậy, a khả nghịch trong $\mathbb{Z}G$, nhưng a không nằm trong $\mathbb{Z}^*G = \pm G$.

Ví dụ 14 (Vành nửa nhóm)

Nếu trong Ví dụ 13 ta xét G là nửa nhóm thì vành RG nhận được bằng cách xây dựng tương tự được gọi là *vành nửa nhóm*.

BÀI TẬP

Bài 1.1

Cho R là vành có đơn vị và $a \in R$. Ta nói a *lũy linh* nếu tồn tại $n \in \mathbb{N}$ sao cho $a^n = 0$ và a *lũy đẳng* nếu $a^2 = a$. Chứng minh rằng:
a) Nếu a khả nghịch thì a không lũy linh.
b) Nếu a lũy linh thì $1 - a$ khả nghịch.
c) Nếu a lũy đẳng thì $1 - a$ cũng lũy đẳng.
d) Nếu a lũy đẳng và khả nghịch thì $a = 1$.

Bài 1.2

Cho R là vành có đơn vị. Chứng minh rằng, nếu R không có ước của không thì R chỉ có một phần tử lũy linh là 0 và hai phần tử lũy đẳng là 0 và 1.

BÀI TẬP

Bài 1.3

Cho R là vành giao hoán. Chứng minh rằng, tập tất cả các phần tử lũy linh của R tạo thành một ideal của R. Cho một ví dụ chứng tỏ kết luận trên không đúng nếu R không giao hoán.

Bài 1.4

Cho R là vành hữu hạn, giao hoán và có đơn vị. Chứng minh rằng tập các phần tử không là ước của không của R là một nhóm đối với phép nhân trong R.

Bài 1.5

Cho R là vành có đơn vị. Chứng minh rằng R là vành chia khi và chỉ khi R không có các ideal phải và trái khác 0 và khác R.

BÀI TẬP

Bài 1.6

Hãy tìm tất cả các phần tử lũy linh của vành $\mathbb{Z}_{60}$.

Bài 1.7

Cho K là trường. Tìm tất cả các phần tử lũy đẳng và tất cả các ideal trái của $M_2(K)$.

Bài 1.8

Cho R là một vành. Đặt $Z(R) = \{x \in R \mid xy = yx, \forall y \in R\}$ và ta gọi $Z(G)$ là *tâm* của R. Chứng minh rằng:
a) $Z(R)$ là vành con của R.
b) Nếu K là trường thì $Z(M_n(K)) = \{aI_n \mid a \in K\}$.

BÀI TẬP

Bài 1.9

Cho R là vành có đơn vị và M là một tập con khác rỗng của R. Đặt $Ann_L(M) = \{x \in R \mid xm = 0, \forall m \in M\}$ và ta gọi $Ann_L(M)$ là *linh hóa tử trái* của M.
a) Chứng minh rằng $Ann_L(M)$ là một ideal trái của R.
b) Chứng minh rằng, nếu M là một ideal phải khác 0 của R sinh bởi một lũy đẳng thì $Ann_L(M)$ là một ideal trái sinh bởi một lũy đẳng của R.

Bài 1.10 (Định lý dư số Trung Hoa)

Cho R là vành giao hoán có đơn vị. Chứng minh rằng:
a) Nếu I_1 và I_2 là các ideal của R thỏa mãn $I_1 + I_2 = R$ thì với mọi $x_1, x_2 \in R$, tồn tại phần tử $x \in R$ sao cho $x - x_1 \in I_1, x - x_2 \in I_2$.
b) Nếu $I_1, ..., I_n$ là các ideal của R sao cho $I_i + I_j = R, \forall i \neq j$ thì với mọi $x_1, ..., x_n \in R$, tồn tại phần tử $x \in R$ sao cho $x - x_k \in I_k, \forall k = 1, ..., n$.

BÀI TẬP

Bài 1.11

Cho X là một tập hợp và $\mathcal{P}(X)$ là tập tất cả các tập con của X. Với $A, B \in \mathcal{P}(X)$, ta định nghĩa $A\Delta B = (A \setminus B) \cup (B \setminus A)$. Chứng minh rằng:
a) $(\mathcal{P}(X), \Delta, \cap)$ là một vành giao hoán có đơn vị với Δ và $\cap$ tương ứng là phép cộng và phép nhân trong $\mathcal{P}(X)$. Trong vành này $\emptyset$ đóng vai trò phần tử không, còn X đóng vai trò phần tử đơn vị.
b) Trong vành $\mathcal{P}(X)$ mọi phần tử đều là lũy đẳng.
c) Nếu $\mathcal{P}(X)$ là miền nguyên thì $|X| = 1$.

Bài 1.12

Tìm tất cả các đồng cấu vành:
a) $\mathbb{Z} \to 2\mathbb{Z}$.
b) $2\mathbb{Z} \to 2\mathbb{Z}$.
c) $2\mathbb{Z} \to 3\mathbb{Z}$.
d) $\mathbb{Z} \to M_2(\mathbb{Z}_2)$.

BÀI TẬP

Bài 1.13

Cho R là vành có đơn vị và $I_1, ..., I_n$ là các ideal của R thỏa mãn $I_i + I_j = R$ với mọi $i \neq j$. Chứng minh rằng ánh xạ $f : R/(\bigcap_{k=1}^n I_k) \to R/I_1 \times ... \times R/I_n$ xác định bởi $f\left(a + \bigcap_{k=1}^n I_k\right) = (a + I_1, ..., a + I_n)$ là một đẳng cấu vành.

Bài 1.14

Vành R có đơn vị được gọi là *hữu hạn theo Dedekind* nếu với mọi $a \in R$, từ điều kiện a khả nghịch một phía luôn suy ra a khả nghịch.
a) Chứng minh rằng, nếu R là vành có đơn vị và không có ước của không thì R là vành hữu hạn theo Dedekind.
b) Chứng minh rằng, nếu K là trường thì vành ma trận $M_n(K)$ là vành hữu hạn theo Dedekind.

BÀI TẬP

Bài 1.15

a) Chứng minh rằng $(\mathbb{Z}[\sqrt{-1}])^* = \{\pm 1, \pm\sqrt{-1}\}$.
b) Chứng minh rằng, nếu $d < -1$ thì $(\mathbb{Z}[\sqrt{d}])^* = \{\pm 1\}$.

Bài 1.16

Chứng minh rằng $\left(\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]\right)^* = \left\{\pm 1, \pm\frac{1+\sqrt{-3}}{2}, \pm\frac{-1+\sqrt{-3}}{2}\right\}$.

Bài 1.17

a) Cho $d \in \mathbb{N}$ và d không là số chính phương. Chứng minh rằng nếu $\mathbb{Z}[\sqrt{d}]$ có một phần tử khả nghịch khác ± 1 thì nó sẽ có vô số phần tử khả nghịch.
b) Với $2 \leq d \leq 15, d \neq 4, 9$. Tìm một phần tử khả nghịch khác ± 1 của $\mathbb{Z}[\sqrt{d}]$.

§2. Đa thức trên vành giao hoán và vành Noether giao hoán

Đa thức trên vành giao hoán

Cho R là vành giao hoán có đơn vị $1 \neq 0$. Đặt $R[x]$ là tập tất cả các biểu thức có dạng $f(x) = \sum_{n=0}^{\infty} a_n x^n$, với $a_n \in R$ và $a_n = 0$ hầu khắp nơi, nghĩa là chỉ có một số hữu hạn phần tử a_n là khác 0.
Ta viết a_0 thay cho $a_0 x^0$ và gọi $f(x)$ là một *đa thức trên R theo biến x*.

Hai phần tử $\sum a_n x^n$ và $\sum b_n x^n$ gọi là bằng nhau nếu $a_n = b_n$ với mọi $n \in \mathbb{N}$.

Tập $R[x]$ như trên là một vành với các phép toán cộng và nhân như sau:
$\sum a_n x^n + \sum b_n x^n = \sum (a_n + b_n) x^n$ và $(\sum a_n x^n)(\sum b_n x^n) = \sum c_n x^n$,
trong đó $c_n = \sum_{k=0}^{n} a_k b_{n-k}$. Vành $R[x]$ gọi là *vành đa thức trên R theo biến x*.

§2. Đa thức trên vành giao hoán và vành Noether giao hoán

Lưu ý rằng $f(x) \in R[x]$ không phải là hàm số với tập xác định R do x không phải là phần tử của R mà x là một biến được ta giả thiết là giao hoán với mọi phần tử của R.

Bậc của đa thức

Nếu $f(x) = \sum_{i=0}^{\infty} a_i x^i \neq 0$ thì ta gọi *bậc của* f, ký hiệu $\deg f = \max\{i \mid a_i \neq 0\}$.

Nếu $n = \deg f$ thì $f(x) = a_0 + a_1 x + ... + a_n x^n = \sum_{i=0}^{n} a_i x^i$, với $a_n \neq 0$.

Ta gọi a_n là *hệ số cao nhất* hay *hệ số đầu* và a_0 là *hệ số tự do* của $f(x)$.
Nếu $a_n = 1$ thì ta nói $f(x)$ là *đa thức đơn khởi*.

§2. Đa thức trên vành giao hoán và vành Noether giao hoán

- Mọi phần tử khác 0 của R đều có thể xem như một đa thức bậc 0.
- Để thuận tiện, ta quy ước thêm $\deg 0 = -\infty$.

Mệnh đề 1

Cho R là vành giao hoán có đơn vị và $f(x), g(x) \in R[x]$. Khi đó:
i) $\deg(f+g) \leq \max\{\deg f, \deg g\}$.
ii) $\deg(fg) \leq \deg f + \deg g$.
Hơn nữa, nếu R là miền nguyên thì $\deg(fg) = \deg f + \deg g$.

Chứng minh

Dễ dàng chứng minh.

Hệ quả 2

Nếu R là miền nguyên thì $R[x]$ là miền nguyên và các phần tử khả nghịch của $R[x]$ chính là các phần tử khả nghịch của R.

Chứng minh

- Nếu $f(x) \neq 0$ và $g(x) \neq 0$ thì $\deg(fg) = \deg f + \deg g \geq 0 > -\infty$, do đó $f(x)g(x) \neq 0$, nên $R[x]$ là miền nguyên.
- Nếu $f(x)g(x) = 1$ thì $\deg f + \deg g = \deg(1) = 0$, nên $\deg f = \deg g = 0$. Do đó $f(x)$ và $g(x)$ đều là các phần tử của R.

Định lý 3 (Thuật chia Euclid)

Cho R là vành giao hoán có đơn vị và $f(x), g(x) \in R[x]$, trong đó $g(x)$ là đa thức đơn khởi. Khi đó, tồn tại duy nhất các đa thức $q(x), r(x) \in R[x]$ sao cho $\deg r < \deg g$ và $f(x) = g(x)q(x) + r(x)$.

Chứng minh

Sự tồn tại: Giả sử $f(x) = a_0 + a_1x + \ldots + a_nx^n$; $g(x) = b_0 + b_1x + \ldots + x^m$, trong đó $g(x)$ là đa thức đơn khởi bậc $m \geq 1$. Nếu $n < m$ thì ta viết $f(x) = g(x).0 + f(x)$; nếu $n \geq m$ thì ta đặt $q_1(x) = a_nx^{n-m}$ và $f_1(x) = f(x) - g(x)q_1(x)$. Khi đó $\deg f_1 \leq n - 1$. Lặp lại quá trình trên bằng cách thay f bởi f_1. Hiển nhiên, sau một số hữu hạn bước ta nhận được đa thức $f_s(x)$ có $\deg f_s < m$. Đặt $q(x) = q_1(x) + \ldots + q_s(x)$ và $r(x) = f(x) - g(x)q(x)$, ta có $\deg r < \deg g$ và $f(x) = g(x)q(x) + r(x)$.

Sự duy nhất: Giả sử $f(x) = g(x)q(x) + r(x)$ và $f(x) = g(x)q_1(x) + r_1(x)$, với $\deg r < \deg g$ và $\deg r_1 < \deg g$. Khi đó $g(x)(q_1(x) - q(x)) = r(x) - r_1(x)$. Mà $g(x)$ là đa thức đơn khởi nên $\deg g + \deg(q_1 - q) = \deg(r - r_1) < \deg g$. Suy ra $\deg(q_1 - q) = -\infty$, nghĩa là $q_1(x) = q(x)$, kéo theo $r_1(x) = r(x)$.

Hệ quả 4

Cho R là vành giao hoán có đơn vị và $a \in R$. Khi đó, với mọi $f(x) \in R[x]$, tồn tại $q(x) \in R[x]$ sao cho $f(x) = (x - a)q(x) + f(a)$.

Hệ quả 5

Cho R là vành giao hoán có đơn vị, $f(x) \in R[x]$ và $a \in R$. Khi đó $f(a) = 0$ nếu và chỉ nếu tồn tại $g(x) \in R[x]$ sao cho $f(x) = (x - a)g(x)$.

Hệ quả 6

Cho R là miền nguyên và $0 \neq f(x) \in R[x]$ là một đa thức bậc n. Khi đó, có không quá n phần tử $a \in R$ thỏa mãn $f(a) = 0$.

Chú ý

Kết quả trên không còn đúng nếu R không phải là miền nguyên. Ví dụ, $f(x) = x^2 - 1 \in \mathbb{Z}_{15}[x]$ là đa thức bậc hai có bốn giá trị a để $f(a) = 0$ là $1, 4, 11, 14$.

Hệ quả 7

Cho R là miền nguyên và $f(x), g(x) \in R[x]$ là các đa thức bậc n. Nếu tồn tại nhiều hơn n phần tử khác nhau $a \in R$ sao cho $f(a) = g(a)$ thì $f(x) = g(x)$.

Ideal tối đại

Ideal phải (t.ư. trái, hai phía) I của vành R được gọi là *ideal phải (t.ư. trái, hai phía) tối đại*, nếu $I \neq R$ và không tồn tại ideal phải (t.ư. trái, hai phía) J của R thỏa mãn $I \subset J \subset R$.

Định lý 8

Mọi ideal phải (t.ư. trái, hai phía) của một vành R có đơn vị đều nằm trong một ideal phải (t.ư. trái, hai phía) tối đại nào đó của R. Nói riêng, mọi vành có đơn vị đều có ideal phải (t.ư. trái, hai phía) tối đại.

Chứng minh

Ta chỉ cần chứng minh định lý đối với các ideal hai phía. Các khẳng định còn lại được chứng minh tương tự.
Đặt $\Re = \{J \mid J \text{là ideal của } R, I \subseteq J \neq R\}$. Do $I \in \Re$ nên $\Re \neq \emptyset$. Xét dây chuyền tiến các ideal $J_1 \subseteq J_2 \subseteq ...$ trong $\Re$ và đặt $A = \bigcup_{n=1}^{\infty} J_n$. Khi đó $I \subseteq A$. Nếu $A = R$ thì $1 \in A$ nên tồn tại $n_0 \in \mathbb{N}$ sao cho $1 \in J_{n_0}$, dẫn đến $J_{n_0} = R$, mâu thuẫn. Do đó $I \subseteq A \neq R$, như vậy $(\Re, \subseteq)$ thỏa mãn điều kiện của Bổ đề Zorn, nên tồn tại một phần tử tối đại M của $\Re$. Khi đó $M \neq R$ và nếu $I' \neq R$ là một ideal của R chứa M thì do tính tối đại của M trong $\Re$ ta được $I' = M$. Vậy M là ideal tối đại chứa I của R.

Hệ quả 9

Trong vành có đơn vị luôn luôn tồn tại ideal phải (t.ư. trái, hai phía) tối đại.

Định lý 10

Cho R là vành giao hoán có đơn vị. Khi đó ideal I là ideal tối đại của R nếu và chỉ nếu R/I là trường.

Chứng minh

Theo Định lý về sự tương ứng, I là ideal tối đại của R nếu và chỉ nếu R/I chỉ có hai ideal là $\overline{0}$ và R/I. Nhưng điều này xảy ra nếu và chỉ nếu R/I là trường.

Ideal nguyên tố

Cho R là vành giao hoán và P là ideal của R. Ta nói P là *ideal nguyên tố* của R nếu $P \neq R$ và với mọi $a, b \in R$, $ab \in P$ kéo theo $a \in P$ hoặc $b \in P$.

Định lý 11

Cho R là vành giao hoán có đơn vị và P là ideal của R. Khi đó P là ideal nguyên tố của R khi và chỉ khi R/P là miền nguyên.

Chứng minh

Nếu P là ideal nguyên tố của R thì $P \neq R$ nên $R/P \neq \overline{0}$. Giả sử $\overline{a} = a + P$, $\overline{b} = b + P$ và $\overline{a}\overline{b} = \overline{0}$. Khi đó $ab \in P$ và do P là ideal nguyên tố nên $a \in P$ hoặc $b \in P$, nghĩa là $\overline{a} = \overline{0}$ hoặc $\overline{b} = \overline{0}$. Vậy R/P là miền nguyên.
Ngược lại, giả sử R/P là miền nguyên và $ab \in P$. Khi đó $\overline{a}\overline{b} = \overline{0}$ nên $\overline{a} = \overline{0}$ hoặc $\overline{b} = \overline{0}$, nghĩa là $a \in P$ hoặc $b \in P$. Vậy P là ideal nguyên tố.

Hệ quả 12

Mọi ideal tối đại của vành giao hoán có đơn vị đều là ideal nguyên tố.

Chứng minh

Do mọi trường đều là miền nguyên nên ta được kết quả.

Hệ quả 13

Cho R, S là các vành giao hoán có đơn vị và $f : R \to S$ là toàn cấu. Khi đó:
i) Nếu S là trường thì $\ker f$ là ideal tối đại của R.
ii) Nếu S là miền nguyên thì $\ker f$ là ideal nguyên tố của R.

Chứng minh

Từ Định lý thứ nhất về sự đẳng cấu ta có $R/\ker f \cong \mathrm{Im} f = S$. Áp dụng các định lý 10 và 11 ta được kết quả cần chứng minh.

Ideal hữu hạn sinh

Một ideal của vành R được gọi là *hữu hạn sinh* nếu nó sinh bởi một tập hữu hạn các phần tử của R. Ideal sinh bởi một phần tử gọi là *ideal chính*.

Định lý 14

Cho R là một vành giao hoán. Khi đó, nếu mọi ideal của R đều hữu hạn sinh thì mọi ideal của vành đa thức $R[x]$ cũng hữu hạn sinh.

Chứng minh

Gọi A là một ideal của $R[x]$. Nếu $A = 0$ thì hiển nhiên A hữu hạn sinh, nếu $A \neq 0$ thì ta đặt $I_n = \{a \in R \mid f(x) \in A, \deg f = n, \mathrm{lc}(f) = a\} \cup \{0\}$, trong đó ta ký hiệu $\mathrm{lc}(f)$ là hệ số cao nhất của $f(x)$. Khi đó I_n là ideal của R.

Do $\mathrm{lc}(f) = \mathrm{lc}(xf)$, nên $I_n \subseteq I_{n+1}$. Đặt $J = \bigcup_{n=0}^{\infty} I_n$. Khi đó J là ideal của R nên J hữu hạn sinh. Giả sử $J = \langle\{a_1, ..., a_k\}\rangle$. Do cách đặt J nên tồn tại $n \in \mathbb{N}$ sao cho $a_1, ..., a_k \in I_n$. Suy ra $J \subseteq I_n$. Mà $I_n \subseteq J$ nên $J = I_n$. Với mỗi m, giả sử $I_m = \langle\{a_{m1}, ..., a_{mk_m}\}\rangle$ và với mỗi j, chọn $f_{mj}(x) \in A$ sao cho $\mathrm{lc}(f_{mj}) = a_{mj}$. Đặt $\overline{A} = \langle f_{mj}(x) \mid 0 \leq m \leq n, 1 \leq j \leq k_m\rangle$, ta chứng minh $A = \overline{A}$. Giả sử $f(x) \in A$ và đặt $r = \deg f$, ta chứng minh $f(x) \in \overline{A}$ bằng quy nạp theo r.

- Nếu $r = 0$ hoặc $r = -\infty$ thì hiển nhiên $f(x) \in \overline{A}$.
- Nếu $0 < r < n$ thì $\mathrm{lc}(f) \in I_r$ nên ta viết $\mathrm{lc}(f) = c_1 a_{r1} + ... + c_{k_r} a_{rk_r}$. Suy ra $\mathrm{lc}(f) = \mathrm{lc}(\sum c_i f_{ri})$, nên $\deg(f - \sum c_i f_{ri}) < r$. Theo quy nạp, $f(x) - \sum c_i f_{ri}(x) \in \overline{A}$, nên $f(x) \in \overline{A}$.
- Nếu $r \geq n$ thì $\mathrm{lc}(f) \in I_r = I_n$ nên $\mathrm{lc}(f) = c_1 a_{n1} + ... + c_{k_n} a_{nk_n}$. Lý luận tương tự như trên ta được $\deg(f - \sum c_i x^{r-n} f_{ni}) < r$, suy ra $f(x) \in \overline{A}$.

Vậy, $A \subseteq \overline{A}$. Hiển nhiên $\overline{A} \subseteq A$, do đó $A = \overline{A}$, nghĩa là A hữu hạn sinh.

Hệ quả 15

Cho R là vành giao hoán. Khi đó, nếu mọi ideal của R đều hữu hạn sinh thì mọi ideal của vành đa thức $R[x_1, ..., x_{n-1}, x_n]$ cũng hữu hạn sinh.

Chứng minh

Viết $R[x_1, ..., x_{n-1}, x_n] = R[x_1, ..., x_{n-1}][x_n]$, và bằng quy nạp theo n suy ra ngay điều phải chứng minh.

Hệ quả 16

Mọi ideal của vành đa thức $K[x_1, ..., x_n]$ trên trường K đều hữu hạn sinh.

Điều kiện dây chuyền tiến

Cho vành R giao hoán có đơn vị. Ta nói R thỏa mãn *điều kiện dây chuyền tiến* (hay *điều kiện ACC*) đối với các ideal nếu mọi dây chuyền tiến $I_1 \subseteq I_2 \subseteq \dots$ đều dừng, nghĩa là tồn tại $n \geq 1$ sao cho $I_k = I_n$ với mọi $k \geq n$.

Vành Noether

Nếu vành R giao hoán có đơn vị và thỏa điều kiện ACC đối với các ideal thì ta nói R là *vành Noether giao hoán*.

Định lý 17

Cho R là vành giao hoán có đơn vị. Khi các điều sau tương đương:
i) R là vành Noether.
ii) Mọi họ khác $\emptyset$ các ideal của R đều có phần tử tối đại.
iii) Mọi ideal của R đều hữu hạn sinh.

Chứng minh

i)$\Rightarrow$ ii). Giả sử $\Re = \{I_\alpha\}_{\alpha\in\Gamma}$ là một họ khác $\emptyset$ các ideal của R và $\Re$ không có phần tử tối đại. Lấy $I_1 \in \Re$. Do $\Re$ không có phần tử tối đại nên tồn tại $I_2 \in \Re$ sao cho $I_1 \subset I_2$. Tương tự, tồn tại I_3 sao cho $I_1 \subset I_2 \subset I_3$. Cứ tiếp tục như vậy ta được một dây chuyền tiến vô hạn các ideal của R: $I_1 \subset I_2 \subset I_3 \subset \ldots$ Nhưng điều này mâu thuẫn với giả thiết R là vành Noether.

ii)$\Rightarrow$iii). Xét ideal I bất kỳ của R và đặt $\Re$ là tập tất cả các ideal hữu hạn sinh của R nằm trong I. Do ii), tồn tại phần tử tối đại $J \in \Re$. Lấy $a \in I$, ta được $J \subseteq J + \langle a\rangle \in \Re$. Do J tối đại trong $\Re$ nên $J + \langle a\rangle = J$ hoặc $J + \langle a\rangle = I$. Nếu $J + \langle a\rangle = I$ thì do J hữu hạn sinh nên I hữu hạn sinh; nếu $J + \langle a\rangle = J$ thì $a \in J$ nên $I = J$, do đó I hữu hạn sinh.
iii)$\Rightarrow$i). Giả sử mọi ideal của R đều hữu hạn sinh. Xét một dây chuyền tiến các ideal của R: $I_1 \subseteq I_2 \subseteq \ldots$. Đặt $I = \bigcup_{n=1}^{\infty} I_n$. Theo giả thiết, I hữu hạn sinh, nên $I = \langle\{a_1, \ldots, a_m\}\rangle$. Do $a_i \in I$ nên tồn tại n_i sao cho $a_i \in I_{n_i}$. Đặt $n = \max\{n_1, \ldots, n_m\}$. Khi đó $a_i \in I_n$ với mọi i, nên $I \subseteq I_n$. Do đó $I = I_n$. Vậy dây chuyền nói trên dừng tại I_n.

Định lý 14 bây giờ được phát biểu lại như sau, gọi là *Định lý cơ sở Hilbert*.

Hệ quả 18 (Định lý cơ sở Hilbert)

Nếu R là vành Noether giao hoán thì vành đa thức $R[x]$ cũng là vành Noether giao hoán.

Hệ quả 15 cũng được phát biểu lại như sau.

Hệ quả 19

Nếu R là vành Noether giao hoán thì vành đa thức $R[x_1, ..., x_n]$ cũng là vành Noether giao hoán.

BÀI TẬP

Bài 2.1

Cho R là vành giao hoán có đơn vị và $f(x) = a_0 + a_1x + \ldots + a_nx^n \in R[x]$.
a) Chứng minh rằng f khả nghịch trong $R[x]$ khi và chỉ khi a_0 khả nghịch trong R và $a_1, ..., a_n$ là các phần tử lũy linh.
b) Chứng minh rằng f lũy linh khi và chỉ khi $a_0, a_1, ..., a_n$ lũy linh.
c) Chứng minh rằng f là ước của không trong $R[x]$ khi và chỉ khi tồn tại $0 \neq a \in R$ sao cho $af = 0$.

Bài 2.2

a) Chứng minh rằng vành $\mathbb{Q}[x]$ không có các phần tử lũy đẳng không tầm thường (nghĩa là những lũy đẳng khác 0 và 1).
b) Hãy tìm một phần tử lũy đẳng không tầm thường trong vành $\mathbb{Q}[x]/\langle x^4+x^2\rangle$.

BÀI TẬP

Bài 2.3

Cho $0 \neq d \in \mathbb{Z}$ không là bình phương trong $\mathbb{Z}$ (nghĩa là phương trình $x^2 = d$ không có nghiệm trong $\mathbb{Z}$). Chứng minh rằng $\mathbb{Z}[\sqrt{d}] \cong \mathbb{Z}[x]/\langle x^2 - d \rangle$.

Bài 2.4

Cho $0 \neq d, d' \in \mathbb{Z}$ và không là các bình phương trong $\mathbb{Z}$. Chứng minh rằng, nếu $d \neq d'$ thì $\mathbb{Z}[\sqrt{d}]$ không đẳng cấu với $\mathbb{Z}[\sqrt{d'}]$.

Bài 2.5

Cho $R_1 = \mathbb{Z}_p[x]/\langle x^2 - 2 \rangle$ và $R_2 = \mathbb{Z}_p[x]/\langle x^2 - 3 \rangle$. Hãy xét xem R_1 có đẳng cấu với R_2 không trong các trường hợp $p = 2, p = 5, p = 11$ hay không?

BÀI TẬP

Bài 2.6

Cho R là vành giao hoán có đơn vị. Chứng minh rằng $M_n(R[x]) \cong M_n(R)[x]$.

Bài 2.7

Hãy tìm tất cả các ideal, ideal nguyên tố, ideal tối đại của vành $\mathbb{Z}_{60}$.

Bài 2.8

Cho R là một vành Noether giao hoán và I là một ideal của R. Chứng minh rằng R/I là vành Noether giao hoán.

BÀI TẬP

Bài 2.9

Cho R là một vành Noether giao hoán và $\varphi : R \to R$ là một toàn cấu vành. Chứng minh rằng φ là một đẳng cấu.

Bài 2.10

Cho R là một vành Noether giao hoán và I là một ideal của R sao cho $R/I \cong R$. Chứng minh rằng $I = \{0\}$.

Bài 2.11

Cho R là một vành giao hoán. Chứng minh rằng R là vành Noether khi và chỉ khi mọi ideal nguyên tố của R đều hữu hạn sinh.

§3. Miền nguyên các ideal chính

Chia hết và chia hết cho

Cho R là một miền nguyên và $0 \neq a, b \in R$. Nếu tồn tại $c \in R$ sao cho $a = bc$ thì ta nói a *chia hết cho* b (ký hiệu $a \vdots b$) hay b *chia hết* a (ký hiệu $b \,|\, a$). Khi đó ta cũng nói a là *bội* của b hay b là *ước* của a.

Phần tử bất khả quy

Cho R là một miền nguyên và $0 \neq a \in R$. Ta nói a *bất khả quy* nếu $a \notin R^*$ và từ $a = bc$ (với $b, c \in R$) kéo theo $b \in R^*$ hoặc $c \in R^*$.

Phần tử nguyên tố

Cho R là một miền nguyên và $0 \neq a \in R$. Ta nói a *nguyên tố* nếu $a \notin R^*$ và từ $a \,|\, bc$ (với $b, c \in R$) kéo theo $a \,|\, b$ hoặc $a \,|\, c$.

§3. Miền nguyên các ideal chính

Mệnh đề 1

Nếu R là một miền nguyên thì mọi phần tử nguyên tố của R đều bất khả quy.

Chứng minh

Giả sử a là nguyên tố của R và $a = bc$, với $b, c \in R$. Khi đó $a \mid b$ hoặc $a \mid c$. Nếu $a \mid b$ thì tồn tại $d \in R$ sao cho $b = ad$. Khi đó $a = bc = a(dc)$. Do R là miền nguyên nên $dc = 1$, nghĩa là $c \in R^*$. Tương tự, nếu $a \mid c$ thì $b \in R^*$. Vậy a là phần tử bất khả quy.

§3. Miền nguyên các ideal chính

Điều ngược lại của mệnh đề trên không đúng

Ví dụ 1

Cho F là trường và $R = F[x^2, x^3]$. Ta có x^2 và x^3 là các phần tử bất khả quy trong R nhưng chúng không phải là các phần tử nguyên tố, vì $x^2 \mid (x^3)^2 = x^6$ nhưng $x^2 \nmid x^3$ và $x^3 \mid x^4.x^2$ nhưng $x^3 \nmid x^4$ và $x^3 \nmid x^2$.

Ví dụ 2

Trong miền nguyên $\mathbb{Z}[\sqrt{-3}]$, phần tử 2 là bất khả quy nhưng không nguyên tố.

Lời giải

Đặt $R = \mathbb{Z}[\sqrt{-3}]$. Giả sử $2 \in R^*$, nghĩa là tồn tại $a, b \in \mathbb{Z}$ sao cho $2(a + b\sqrt{-3}) = 1$. Lấy môđun hai vế, nhận được $4(a^2 + 3b^2) = 1$, mâu thuẫn. Vậy $2 \notin R^*$.
Giả sử 2 không bất khả quy, nghĩa là $2 = (a + b\sqrt{-3})(c + d\sqrt{-3})$.
Suy ra $(a^2+3b^2)(c^2+3d^2) = 4$. Do phương trình $x^2+3y^2 = 2$ không có nghiệm nguyên nên từ đẳng thức trên suy ra $a^2 + 3b^2 = 1$ hoặc $c^2 + 3d^2 = 1$. Suy ra $a = \pm 1, b = 0$ hoặc $c = \pm 1, d = 0$. Vậy 2 là bất khả quy trong R. Tuy nhiên 2 không là phần tử nguyên tố của R vì $2 \mid 4 = (1+\sqrt{-3})(1-\sqrt{-3})$, nhưng $2 \nmid (1+\sqrt{-3})$ và $2 \nmid (1-\sqrt{-3})$.

Ước chung lớn nhất

Cho R là miền nguyên, $\emptyset \neq A \subset R \setminus \{0\}$ và $d \in R$.
Ta nói d là *ước chung lớn nhất* (ƯCLN) của A nếu $d \mid a$ với mọi $a \in A$ và với mọi $e \in R$, nếu $e \mid a, \forall a \in A$ thì $e \mid d$.

Nếu ƯCLN của A là 1 thì ta nói các phần tử của A *nguyên tố cùng nhau*.

§3. Miền nguyên các ideal chính

Phần tử liên hợp

Cho R là một miền nguyên và $0 \neq a, b \in R$. Nếu tồn tại $u \in R^*$ sao cho $a = ub$ thì ta nói a *liên hợp* với b, ký hiệu $a \sim b$.

Nhận xét 1

- $a \sim b$ nếu và chỉ nếu $a \mid b$ và $b \mid a$.
- $a \sim b$ nếu và chỉ nếu $\langle a \rangle = \langle b \rangle$.
- Nếu d và d' là hai ước chung lớn nhất của tập A thì $d \sim d'$.

§3. Miền nguyên các ideal chính

Miền nguyên các ideal chính

Một miền nguyên R được gọi là một *miền nguyên các ideal chính* hay một PID nếu mọi ideal của nó đều là ideal chính.

Chẳng hạn, miền nguyên $\mathbb{Z}$ là một PID.

Nhận xét 2

Mọi PID đều là vành Noether.

Định lý 2

Cho R là một PID, $d \in R$ và $\emptyset \neq A \subseteq R \setminus \{0\}$. Khi đó, d là ước chung lớn nhất của A nếu và chỉ nếu $\langle d \rangle = \langle A \rangle$.

Chứng minh

Giả sử $\langle A \rangle = \langle d \rangle$. Khi đó $d \mid a$ với mọi $a \in A$. Do $d \in \langle A \rangle$ nên tồn tại $r_1, ..., r_n \in R$ và $a_1, ..., a_n \in A$ sao cho $d = r_1 a_1 + ... + r_n a_n$. Do đó, nếu $e \mid a$ với mọi $a \in A$ thì $e \mid d$. Vậy d là ƯCLN của A.
Ngược lại, giả sử d là ƯCLN của A. Do R là một PID nên tồn tại $c \in R$ sao cho $\langle A \rangle = \langle c \rangle$. Theo chứng minh trên, c là ƯCLN của A nên $c \sim d$, suy ra $\langle d \rangle = \langle c \rangle = \langle A \rangle$.

Hệ quả 3

Cho R là một PID và $a \in R$. Khi đó a nguyên tố khi và chỉ khi a bất khả quy.

Chứng minh

Do Mệnh đề 1 ta được chiều thuận. Ngược lại, giả sử a bất khả quy và $a \mid bc$, với $b, c \in R$. Do R là PID nên tồn tại $d \in R$ sao cho $\langle d \rangle = \langle a, b \rangle$. Do Định lý 2, d là ƯCLN của $\{a, b\}$. Đặt $a = de$. Vì a bất khả quy nên $d \in R^*$ hoặc $e \in R^*$.
- Nếu $e \in R^*$ thì $a = de \mid be$, suy ra $a \mid b$.
- Nếu $d \in R^*$ thì từ $\langle d \rangle = \langle a, b \rangle$ suy ra $d = ax + by$, với $x, y \in R$; từ $a \mid bc$ suy ra $bc = af$, với $f \in R$. Do đó $cd = acx + bcy = a(cx + fy)$, nên $a \mid cd$. Mà $d \in R^*$ nên $a \mid c$.
Vậy a là phần tử nguyên tố của R.

Hệ quả 4

Cho R là một PID và $I \neq 0$ là ideal của R. Khi đó, I nguyên tố nếu và chỉ nếu I là tối đại.

Chứng minh

Do Hệ quả 5 (§2) ta được chiều đảo. Ngược lại, giả sử $I \neq 0$ là ideal nguyên tố của R. Khi đó tồn tại phần tử nguyên tố $p \in R$ sao cho $I = \langle p \rangle$. Giả sử A là một ideal của R thỏa mãn $I \subsetneq A \subseteq R$. Do R là PID nên tồn tại $a \in R$ sao cho $A = \langle a \rangle$. Do $I \subseteq A$ nên tồn tại $b \in R$ sao cho $p = ab$. Do p nguyên tố nên theo Mệnh đề 1, p bất khả quy. Do đó $a \in R^*$ hoặc $b \in R^*$. Nhưng, do $I \neq A$ nên $b \notin R^*$. Vậy $a \in R^*$, suy ra $A = \langle a \rangle = R$.

Nếu $I = 0$ thì điều khẳng định trong hệ quả trên không còn đúng. Thực vậy, trong $\mathbb{Z}$ ta có 0 là ideal nguyên tố nhưng không tối đại.

Sự chủ yếu duy nhất

Cho R là một vành giao hoán và $0 \neq a \in R$. Nếu a phân tích được dưới dạng $a = up_1...p_n$, với $u \in R^*$ và các p_i là các phần tử nguyên số, thì sự phân tích trên gọi là *chủ yếu duy nhất* nếu với mọi sự phân tích $a = vq_1...q_m$, với $v \in R^*$ và các q_j là các phần tử nguyên tố, ta có $m = n$ và tồn tại $\sigma \in S_n$ sao cho $p_i \sim q_{\sigma(i)}$ với mọi i.

§3. Miền nguyên các ideal chính

Định lý 5 (Định lý căn bản của số học trong một PID

Cho R là một PID. Khi đó mọi phần tử $0 \neq a \in R$ đều có thể viết dưới dạng $a = up_1...p_n$, trong đó $u \in R^*$ và $p_i, i = 1, ..., n$ là những phần tử nguyên tố. Hơn nữa, sự phân tích này là chủ yếu duy nhất.

Chứng minh

Sự tồn tại. Giả sử $0 \neq a \in R$ và a không khả nghịch cũng không nguyên tố. Do R là một PID nên a không bất khả quy, nghĩa là $a = a_1b_1$, với $a_1, b_1 \notin R^*$. Vậy $\langle a \rangle \subset \langle b_1 \rangle$. Nếu b_1 là phần tử nguyên tố thì ta dừng. Nếu b_1 không nguyên tố thì lại làm như trên đối với b_1, ta tìm được $b_2 \notin R^*$ sao cho $\langle a \rangle \subset \langle b_1 \rangle \subset \langle b_2 \rangle$. Cứ tiếp tục như vậy ta được dãy $\langle a \rangle \subset \langle b_1 \rangle \subset \langle b_2 \rangle \subset ...$ Do R là PID nên R là vành Noether. Do đó dãy trên phải dừng tại $\langle b_n \rangle$, và b_n chính là một ước nguyên tố của a. Vậy a có ước nguyên tố.

§3. Miền nguyên các ideal chính

Giả sử $a = p_1c_1$, với p_1 nguyên tố. Khi đó $\langle a \rangle \subset \langle c_1 \rangle$. Nếu c_1 khả nghịch hoặc nguyên tố thì ta dừng. Nếu ngược lại, viết $c_1 = p_2c_2$, với p_2 nguyên tố và $\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle$. Cứ tiếp tục như vậy ta được dãy $\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset ...$ Dãy này phải dừng tại $\langle c_n \rangle$, với c_n khả nghịch hoặc c_n nguyên tố. Đặt $u = c_n$, ta được $a = p_1c_1 = ... = p_1p_2...p_nu$. Đây chính là sự phân tích cần tìm.

Sự chủ yếu duy nhất. Giả sử $m \neq n$. Không mất tính tổng quát, có thể giả sử $m > n$. Ta có $p_1 | q_1...q_m$, nên tồn tại j sao cho $p_1 | q_j$. Đổi chỗ các q_i nếu cần, ta giả sử $p_1 | q_1$. Suy ra $q_1 = p_1\varepsilon_1$, với $\varepsilon_1 \in R^*$. Thay $q_1 = p_1\varepsilon_1$ và khử p_1 ở hai vế, nhận được $up_2...p_n = v\varepsilon_1q_2...q_m$. Tiếp tục như vậy đến bước thứ n nhận được $u = v\varepsilon_1...\varepsilon_nq_{n+1}...q_m$, với u, v và các ε_i là các phần tử khả nghịch. Nhưng đây là một mâu thuẫn vì tất cả các q_j đều không khả nghịch. Vậy $m = n$, và từ chứng minh trên, rõ ràng tồn tại $\sigma \in S_n$ sao cho $p_i \sim q_{\sigma(i)}$.

§3. Miền nguyên các ideal chính

Hệ quả 6

Cho R là một PID và $0 \neq a \in R$. Khi đó $a = up_1^{n_1}...p_k^{n_k}$, với $u \in R^*$ và các p_i là các phần tử nguyên tố khác nhau. Sự phân tích này là chủ yếu duy nhất.

Ta gọi $a = up_1^{m_1}...p_r^{m_r}$ là sự *phân tích a thành tích các thừa số nguyên tố* p_i.

Nếu chỉ giả thiết miền nguyên R là Noether (chứ chưa là PID) thì mọi phần tử $0 \neq a \in R$ đều phân tích được thành tích của các phần tử bất khả quy (có thể không nguyên tố) và một phần tử khả nghịch. Sự phân tích này cũng không nhất thiết chủ yếu duy nhất. Nếu miền nguyên R không Noether thì một phần tử của nó có thể *không phân tích được thành tích những phần tử bất khả quy*.

§3. Miền nguyên các ideal chính

Ví dụ 1

Nếu K là trường thì, trong vành Noether $R = K[x^2, x^3]$, phần tử x^6 có hai sự phân tích thành tích các phần tử bất khả quy là $x^6 = (x^2)^3$ và $x^6 = (x^3)^2$.

Ví dụ 2

Trong vành Noether $\mathbb{Z}[\sqrt{-3}]$ có hai sự phân tích phần tử 4 thành tích các phần tử bất khả quy là $4 = 2.2$ và $4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$.

Ví dụ 3

Xét vành con $R = \{a_0 + a_1x + ... + a_nx^n \in \mathbb{Q}[x] \mid a_0 \in \mathbb{Z}\}$ của vành đa thức $\mathbb{Q}[x]$. Ta có $R^* = \{\pm 1\}$ và R không là vành Noether, vì trong R có một dây chuyền tiến vô hạn các ideal: $\langle x\rangle \subset \langle \frac{1}{2}x\rangle \subset \langle \frac{1}{4}x\rangle \subset \langle \frac{1}{8}x\rangle \subset ...$

Với mọi $k \in \mathbb{Z}$ ta có sự phân tích $x = k.\dfrac{x}{k} \in R$. Nếu $k \neq \pm 1$ thì cả k và $\dfrac{x}{k}$ đều không khả nghịch, do đó x không bất khả quy. Nếu k là một hợp số thì dễ thấy cả k và $\dfrac{x}{k}$ đều không bất khả quy. Vậy x không thể phân tích thành tích của các phần tử bất khả quy.

Định lý 7

Cho R là một miền nguyên. Khi đó, $R[x]$ là PID khi và chỉ khi R là trường.

Chứng minh

Chiều thuận. Giả sử $R[x]$ là PID. Ta có ánh xạ $\varphi : R[x] \to R, f(x) \mapsto f(0)$, là toàn cấu vành, nên $R[x]/\ker(\varphi) \cong R$. Do R là miền nguyên nên $\ker(\varphi)$ là ideal nguyên tố, mà $R[x]$ là PID nên $\ker(\varphi)$ tối đại. Do đó R là trường.

Chiều đảo. Giả sử R là trường và I là ideal của $R[x]$. Nếu $I = \{0\}$ thì $I = \langle 0\rangle$; nếu $I \neq \{0\}$ thì ta gọi $f(x)$ là đa thức khác 0 có bậc nhỏ nhất của I. Khi đó, với mọi $h(x) \in I$, chia $h(x)$ cho $f(x)$, nhận được $h(x) = f(x)q(x) + r(x)$, với $\deg r < \deg f$. Suy ra $r(x) = h(x) - f(x)q(x) \in I$. Do cách chọn của $f(x)$ ta được $r(x) = 0$, nghĩa là $h(x) = f(x)q(x) \in \langle f(x)\rangle$. Do đó $I = \langle f(x)\rangle$. Vậy $R[x]$ là một PID.

§3. Miền nguyên các ideal chính

Bội chung nhỏ nhất

Cho R là miền nguyên, $\emptyset \neq A \subset R \setminus \{0\}$ và $0 \neq m \in R$. Ta nói m là *bội chung nhỏ nhất* (BCNN) của A nếu $a \mid m, \forall a \in A$ và với mọi $e \in R$, nếu $a \mid e, \forall a \in A$ thì $m \mid e$.

§3. Miền nguyên các ideal chính

Định lý 8

Cho R là một PID, $m \in R$ và $A = \{a_1, ..., a_n\}$ là một tập hợp hữu hạn các phần tử khác 0 của R. Khi đó m là BCNN của A khi và chỉ khi $\langle m \rangle = \langle a_1 \rangle \cap ... \cap \langle a_n \rangle$.

Chứng minh

Đặt $I = \langle a_1 \rangle \cap ... \cap \langle a_n \rangle$. Nếu $I = \langle m \rangle$ thì do $0 \neq a_1...a_n \in I$, nên $m \neq 0$ và $a_i \mid m$ với mọi i. Hơn nữa, nếu $e \in R$ và $a_i \mid e$ với mọi i thì $e \in I = \langle m \rangle$. Do đó $m \mid e$. Vậy m là BCNN của A.
Ngược lại, nếu m là BCNN của A thì do R là PID nên tồn tại $c \in R$ sao cho $I = \langle c \rangle$. Theo chứng minh trên, c là BCNN của A. Do đó $c \sim m$. Suy ra $\langle m \rangle = \langle c \rangle = I$.

BÀI TẬP

Bài 3.1

Cho R là vành giao hoán có đơn vị $1 \neq 0$. Chứng minh rằng:
(a) Phần tử $p \in R$ là nguyên tố khi và chỉ khi Rp là ideal nguyên tố;
(b) Nếu phần tử $a \in R$ là bất khả qui thì Ra là ideal chính tối đại;
(c) Nếu $Ra_1 + Ra_2 + ... + Ra_n = Rd$ thì d là ƯCLN của a_1, a_2, ..., a_n.

Bài 3.2

Cho R là miền nguyên. Chứng minh rằng phần tử $a \in R \setminus \{0\}$ là bất khả qui khi và chỉ khi Ra là ideal chính tối đại.

BÀI TẬP

Bài 3.3

Cho S là một vành giao hoán có đơn vị và R là vành con của S. Giả sử $d \in R$ là một phần tử sao cho phương trình $x^2 = d$ có nghiệm trong S nhưng không có nghiệm trong R. Ký hiệu $\sqrt{d}$ là một nghiệm của phương trình nói trên trong vành S. Định nghĩa tập hợp $R[\sqrt{d}]$ bởi $R[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in R\} \subset S$.
(a) Chứng minh rằng $R[\sqrt{d}]$ là một vành giao hoán có đơn vị.
(b) Chứng minh rằng $\mathbb{Z}[\sqrt{d}]$ là miền nguyên.
(c) Nếu F là trường thì $F[\sqrt{d}]$ là một trường.

Bài 3.4

Cho ví dụ chứng tỏ vành con chứa đơn vị của một miền nguyên PID có thể không phải là một miền nguyên PID.

BÀI TẬP

Bài 3.5

a) Chứng minh rằng $\mathbb{Z}[x]$ không phải là một PID.
b) Chứng minh rằng 2 và x nguyên tố cùng nhau trong $\mathbb{Z}[x]$ nhưng không tồn tại các đa thức $f(x)$ và $g(x)$ sao cho $2f(x) + xg(x) = 1$.
c) Trong $\mathbb{Z}[x]$ chứng minh rằng ideal sinh bởi đa thức x là một ideal chính tối đại nhưng không tối đại.

§4. Miền nguyên Euclid

Miền nguyên Euclid

Cho R là một miền nguyên. Ta nói R là *miền nguyên Euclid* nếu tồn tại một ánh xạ $\delta : R \setminus \{0\} \to \mathbb{Z}^+$ sao cho:
i) Với mọi $a, b \in R \setminus \{0\}$ ta có $\delta(a) \leq \delta(ab)$;
ii) Với mọi $a \in R \setminus \{0\}$ và với mọi $b \in R$, tồn tại $q, r \in R$ sao cho
$$b = aq + r, \text{ với } r = 0 \text{ hoặc } \delta(r) < \delta(a).$$

Ví dụ 1

- Miền nguyên $\mathbb{Z}$ là miền nguyên Euclid, với $\delta(n) = |n|$.
- Nếu K là trường thì $K[x]$ là miền nguyên Euclid, với $\delta(f(x)) = \deg f$.

§4. Miền nguyên Euclid

Bổ đề 1

Cho R là miền nguyên Euclid. Khi đó, với mọi $a \in R \setminus \{0\}$ ta có $\delta(a) \geq \delta(1)$. Hơn nữa, $\delta(a) = \delta(1)$ nếu và chỉ nếu $a \in R^*$.

Chứng minh

Với mọi $a \in R \setminus \{0\}$ ta có $\delta(1) \leq \delta(1.a) = \delta(a)$.
Nếu $a \in R^*$ thì tồn tại $b \in R$ để $ab = 1$. Suy ra $\delta(1) = \delta(ab) \geq \delta(a) \geq \delta(1)$, suy ra $\delta(a) = \delta(1)$.
Ngược lại, nếu $\delta(1) = \delta(a)$ thì chia 1 cho a ta được $1 = aq + r$, với $r = 0$ hoặc $\delta(r) < \delta(a) = \delta(1)$. Nếu $r \neq 0$ thì theo chứng minh trên $\delta(r) \geq \delta(1)$, mâu thuẫn. Vậy $r = 0$, do đó $a \in R^*$.

§4. Miền nguyên Euclid

Định lý 2

Mọi miền nguyên Euclid đều là PID.

Chứng minh

Giả sử R là miền nguyên Euclid và I là ideal của R. Nếu $I = \{0\}$ thì $I = \langle 0 \rangle$, nếu $I \neq \{0\}$ thì tồn tại $0 \neq a \in I$ sao cho $\delta(a)$ nhỏ nhất. Khi đó, với mọi $x \in I$, tồn tại $q, r \in R$ sao cho $x = aq + r$, với $r = 0$ hoặc $\delta(r) < \delta(a)$. Do $a, x \in I$ nên $r = x - aq \in I$. Mà $\delta(a)$ nhỏ nhất nên $r = 0$, nghĩa là $x = aq \in \langle a \rangle$. Vậy $I = \langle a \rangle$.

Chiều đảo của định lý không đúng. Chẳng hạn, tập con $R = \left\{a + b(\frac{1+\sqrt{-19}}{2}) \mid a, b \in \mathbb{Z}\right\}$ của trường $\mathbb{C}$ là một PID nhưng không là miền nguyên Euclid (xem chứng minh trong một bài báo của Wilson).

§4. Miền nguyên Euclid

Miền nguyên $Z[\sqrt{d}]$

Giả sử d là số nguyên khác 0, khác 1 và không có thừa số chính phương.
Đặt $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.
Khi đó $\mathbb{Z}[\sqrt{d}]$ là vành con của $\mathbb{C}$, nên nó là một miền nguyên.

Nhận xét 1

Trường các thương của $\mathbb{Z}[\sqrt{d}]$ là $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$.

§4. Miền nguyên Euclid

Bổ đề 3

Cho $d \in \mathbb{Z} \setminus \{0, 1\}$ sao cho d không có thừa số chính phương và cho ánh xạ $\delta : \mathbb{Z}[\sqrt{d}] \setminus \{0\} \to \mathbb{Z}^+$ xác định bởi $\delta(a + b\sqrt{d}) = |a^2 - db^2|$. Khi đó, với mọi $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ ta có:
i) $\delta(\alpha\beta) = \delta(\alpha)\delta(\beta)$ và $\delta(\alpha\beta) \geq \delta(\alpha)$.
ii) α khả nghịch trong $\mathbb{Z}[\sqrt{d}]$ khi và chỉ khi $\delta(\alpha) = 1$.

Chứng minh

i) Dễ dàng chứng minh.
ii) Giả sử $\alpha\beta = 1$. Khi đó $1 = \delta(1) = \delta(\alpha)\delta(\beta) \geq \delta(\alpha) \geq 1$. Từ đó $\delta(\alpha) = 1$.
Ngược lại, giả sử $\alpha = a + b\sqrt{d}$ và $\delta(\alpha) = 1$.
Khi đó $|a^2 - db^2| = 1$ nên $(a + b\sqrt{d})(a - b\sqrt{d}) = \pm 1$.
Do đó $\alpha = a + b\sqrt{d}$ khả nghịch và có nghịch đảo là $\pm(a - b\sqrt{d})$.

Mệnh đề 4

Cho $d \in \{-2, -1, 2, 3\}$.
Khi đó $\mathbb{Z}[\sqrt{d}]$ là miền nguyên Euclid, với $\delta(a + b\sqrt{d}) = |a^2 - db^2|$.

Chứng minh

Từ Bổ đề 3i) ta được $\delta(\alpha\beta) \geq \delta(\alpha)$ với mọi $\alpha, \beta \in Z[\sqrt{d}]$.
Giả sử $\alpha, \beta \in \mathbb{Z}[\sqrt{d}], \beta \neq 0$. Ta viết $\dfrac{\alpha}{\beta} = x + y\sqrt{d}$, với $x, y \in \mathbb{Q}$.
Do $x \in \mathbb{Q}$ nên tồn tại $r, s \in \mathbb{Z}$ sao cho $|x - r| \leq \dfrac{1}{2}$ và $|y - s| \leq \dfrac{1}{2}$.
Đặt $\gamma = r + s\sqrt{d}$ và $\theta = \beta((x-r)+(y-s)\sqrt{d})$. Khi đó $\alpha = \beta(x+y\sqrt{d}) = \beta\gamma+\theta$.
Do $r, s \in \mathbb{Z}$ nên $\gamma \in \mathbb{Z}[\sqrt{d}]$, do đó $\theta = \alpha - \beta\gamma \in \mathbb{Z}[\sqrt{d}]$.

Ta có $\dfrac{\delta(\theta)}{\delta(\beta)} = |(x-r)^2 - d(y-s)^2| \leq |x-r|^2 + |d|\,|y-s|^2 \leq (1/2)^2 + 3(1/2)^2 = 1$.
Hơn nữa, dấu "=" xảy ra khi $|x - r| = |y - s| = \dfrac{1}{2}$ và $d = 3$.
Nhưng khi đó $\dfrac{\delta(\theta)}{\delta(\beta)} = \left||x - r|^2 - d|y - s|^2\right| = \left|\dfrac{1}{4} - \dfrac{3}{4}\right| = \dfrac{1}{2} < 1$.
Vậy không trong mọi trường hợp ta đều có $\dfrac{\delta(\theta)}{\delta(\beta)} < 1$, nghĩa là $\delta(\theta) < \delta(\beta)$.
Do đó $\mathbb{Z}[\sqrt{d}]$ là miền nguyên Euclid.

§4. Miền nguyên Euclid

Bổ đề 5

Trong miền nguyên $\mathbb{Z}[\sqrt{d}]$, phần tử 2 không là phần tử nguyên tố.

Chứng minh

Ta có $2 \mid d(d-1) = (d+\sqrt{d})(d-\sqrt{d})$. Hơn nữa, cả hai phần tử $\dfrac{d \pm \sqrt{d}}{2}$ đều không nằm trong $\mathbb{Z}[\sqrt{d}]$, nên 2 không là phần tử nguyên tố của $\mathbb{Z}[\sqrt{d}]$.

§4. Miền nguyên Euclid

Mệnh đề 6

Nếu $d < 0$ thì $\mathbb{Z}[\sqrt{d}]$ là PID khi và chỉ khi $d = -2$ hoặc $d = -1$.

Chứng minh

Chiều đảo. Từ Mệnh đề 4 và Định lý 2 ta được chiều đảo.
Chiều thuận. Từ Bổ đề 5 ta được 2 không là phần tử nguyên tố. Mà $\mathbb{Z}[\sqrt{d}]$ là PID nên từ Bổ đề 3(§3) ta được 2 không bất khả quy trong $\mathbb{Z}[\sqrt{d}]$, nghĩa là $2 = \alpha\beta$, với α, β không khả nghịch trong $\mathbb{Z}[\sqrt{d}]$. Gọi δ là ánh xạ như trong Bổ đề 3. Từ Bổ đề 3 ta được $\delta(\alpha) > 1, \delta(\beta) > 1$ và $4 = \delta(2) = \delta(\alpha\beta) = \delta(\alpha)\delta(\beta)$, do đó $\delta(\alpha) = \delta(\beta) = 2$. Vậy, tồn tại $a, b \in \mathbb{Z}, \alpha = a + b\sqrt{d}$ sao cho $\delta(\alpha) = |a^2 - db^2| = 2$. Suy ra $a^2 - db^2 = \pm 2$, và do đó $b \neq 0$.
Nếu $d \leq -3$ thì từ $b \neq 0$ suy ra $a^2 - db^2 = a^2 + (-d)b^2 \geq 0 + 3.1 = 3$, mâu thuẫn. Vậy $d > -3$, nghĩa là $d = -2$ hoặc $d = -1$.

BÀI TẬP

Bài 4.1

Cho I là một ideal của miền nguyên Euclid R. Chứng minh rằng R/I là miền nguyên Euclid khi và chỉ khi I là ideal nguyên tố của R.

Bài 4.2

Cho R là miền nguyên Euclid với ánh xạ $\delta : R \setminus \{0\} \to \mathbb{Z}^+$. Chứng minh rằng R là trường khi và chỉ khi $\exists a \in \mathbb{N}$ sao cho $\delta(x) = a, \forall x \in R \setminus \{0\}$.

Bài 4.3

Cho ví dụ chứng tỏ một vành con chứa đơn vị của một miền nguyên Euclid có thể không phải là miền nguyên Euclid.

BÀI TẬP

Bài 4.4

Trong một miền nguyên Euclid hãy tìm ƯCLN của hai phần tử a, b và viết nó dưới dạng $ra + sb$:
(a) 189 và 301 trong $\mathbb{Z}$.
(b) 1261 và 1649 trong $\mathbb{Z}$.
(c) $x^4 - x^3 + 4x^2 - x + 3$ và $x^3 - 2x^2 + x - 2$ trong $\mathbb{Q}[x]$.
(d) $x^4 + 4$ và $2x^3 + x^2 - 2x - 6$ trong $\mathbb{Z}_3[x]$.
(e) $2 + 11i$ và $1 + 3i$ trong $\mathbb{Z}[i]$.
(f) $-4 + 7i$ và $1 + 7i$ trong $\mathbb{Z}[i]$.

§5. Miền nhân tử hóa

Miền nhân tử hóa

Miền nguyên R được gọi là *miền nhân tử hóa*, viết tắt là UFD, nếu mọi phần tử $a \neq 0$ của R đều có thể viết một cách *chủ yếu duy nhất* (theo nghĩa đã nêu trong §3) dưới dạng $a = up_1 \dots p_r$, với $u \in R^*$ và các p_i bất khả quy với mọi i.

Mệnh đề 1

Mọi PID đều là UFD.

Chứng minh

Trong một PID, mọi phần tử bất khả quy đều nguyên tố, nên từ Định lý 5 (§3) ta được kết quả.

§5. Miền nhân tử hóa

Bổ đề 2

Cho R là một UFD và $a \in R$. Khi đó a bất khả quy nếu và chỉ nếu a nguyên tố.

Chứng minh

Do Mệnh đề 1 (§3), mọi phần tử nguyên tố đều bất khả quy. Ngược lại, giả sử $a \in R$ là phần tử bất khả quy và $a \mid bc$. Khi đó, tồn tại $d \in R$ sao cho $bc = ad$. Do R là UFD nên $b = ub_1 \dots b_r$, $c = vc_1 \dots c_s$, $d = wd_1 \dots d_t$, với $u, v, w \in R^*$ và b_i, c_j, d_k là các phần tử bất khả quy. Khi đó $bc = ad = (uv)b_1 \dots b_r c_1 \dots c_s = wad_1 \dots d_t$. Do tính chủ yếu duy nhất của phân tích trên nên a phải liên hợp với một phần tử b_i hoặc c_j nào đó. Suy ra $a \mid b$ hoặc $a \mid c$, nghĩa là a nguyên tố.

Bổ đề 3

Cho R là một UFD. Khi đó, mọi tập hữu hạn các phần tử khác 0 của R đều có ƯCLN.

Chứng minh

Ta chỉ cần chứng minh bổ đề cho trường hợp tập hữu hạn gồm 2 phần tử.
Giả sử $0 \neq a, b \in R$. Gọi $p_1, \ldots, p_r$ là tất cả các ước nguyên tố (mà theo Bổ đề 2, cũng là các ước bất khả quy) có mặt trong sự phân tích của a và b. Bằng cách gom các thừa số nguyên tố liên hợp lại với nhau, ta có thể viết $a = up_1^{m_1} \ldots p_r^{m_r}$, $b = vp_1^{n_1} \ldots p_r^{n_r}$, với $u, v \in R^*, m_i, n_i \geq 0$.
Đặt $d = p_1^{k_1} \ldots p_r^{k_r}$, với $k_i = \min\{m_i, n_i\}$. Hiển nhiên $d \mid a$ và $d \mid b$.

Chứng minh (tiếp theo)

Nếu $e \in R$ sao cho $e \mid a$ và $e \mid b$ thì tồn tại $g, h \in R$ sao cho $a = eg$ và $b = eh$. Phân tích a, b, e và g, h thành tích các thừa số nguyên tố, nhận thấy mỗi ước nguyên tố của e cũng chính là ước nguyên tố của a và b, lũy thừa của ước nguyên tố này đối với sự phân tích của e không thể vượt quá lũy thừa của nó đối với sự phân tích của a và của b. Do đó $e = p_1^{l_1} \ldots p_r^{l_r}$, với $l_i \leq \min\{m_i, n_i\} = k_i$. Suy ra $e \mid d$. Vậy d là ƯCLN của a và b.

Dung tích của đa thức

Cho R là một UFD và $f(x) \in R[x]$ là một đa thức khác 0. Ta gọi ƯCLN của các hệ số của $f(x)$ là *dung tích* của $f(x)$ và ký hiệu là $cont(f)$.

Nếu $cont(f) \sim 1$ (nghĩa là $cont(f) \in R^*$) thì ta nói $f(x)$ là *đa thức nguyên thủy*.

Lưu ý rằng $cont(f)$ là duy nhất sai khác một thừa số khả nghịch.
Nếu $f(x) \neq 0$ thì $f(x) = cg(x)$, với $c = cont(f)$ và $g(x)$ là đa thức nguyên thủy.

Bổ đề 4 (Gauss)

Cho R là một UFD và $0 \neq f(x), g(x) \in R[x]$. Khi đó $cont(fg) = cont(f).cont(g)$. Nói riêng, nếu $f(x), g(x)$ là các đa thức nguyên thủy thì $f(x).g(x)$ cũng là đa thức nguyên thủy.

Chứng minh

Viết $f(x) = cont(f)f_1(x)$ và $g(x) = cont(g)g_1(x)$, trong đó $f_1(x)$ và $g_1(x)$ là các đa thức nguyên thủy. Khi đó $f(x)g(x) = cont(f).cont(g)f_1(x)g_1(x)$.
Giả sử $f_1(x) = a_0 + a_1x + ... + a_mx^m$, $g_1(x) = b_0 + b_1x + ... + b_nx^n$, và giả sử $cont(f_1g_1) = d \notin R^*$. Gọi p là một ước nguyên tố của d, suy ra p là ước của mọi hệ số của $f_1(x)g_1(x)$. Nhưng $f_1(x)$ và $g_1(x)$ là các đa thức nguyên thủy nên p không phải là ước của mọi hệ số của $f_1(x)$ và $g_1(x)$. Gọi a_r là hệ số đầu tiên của $f_1(x)$ không chia hết cho p và b_s là hệ số đầu tiên của $g_1(x)$ không chia hết cho p. Khi đó hệ số của x^{r+s} trong $f_1(x).g_1(x)$ là

$$a_rb_s + (a_{r+1}b_{s-1} + a_{r+2}b_{s-2} + \ldots) + (a_{r-1}b_{s+1} + a_{r-2}b_{s+2} + \ldots).$$

Do p là ước của các phần tử nằm trong hai ngoặc đơn và p là ước của tổng trên nên p là ước của a_rb_s. Suy $p|a_r$ hoặc $p|b_s$, mâu thuẫn. Vậy $d \in R^*$. Do đó $f_1(x)g_1(x)$ là đa thức nguyên thủy.

Bổ đề 5

Cho R là một UFD và F là trường các thương của R. Khi đó, nếu $0 \neq f(x) \in F[x]$ thì tồn tại $\alpha \in F$ và tồn tại đa thức nguyên thủy $f_1(x) \in R[x]$ sao cho $f(x) = \alpha f_1(x)$. Đa thức $f_1(x)$ trong sự phân tích này là duy nhất sai khác một nhân tử khả nghịch trong R.

Chứng minh

Gọi d là mẫu số chung của các hệ số khác 0 của $f(x)$. Khi đó $f(x) = \frac{1}{d}\overline{f}(x)$, với $\overline{f}(x) \in R[x]$. Đặt $c = cont(\overline{f})$ và $\alpha = \frac{c}{d} \in F$. Khi đó $f(x) = \alpha f_1(x)$, với $f_1(x)$ là đa thức nguyên thủy trong $R[x]$. Nếu $f(x) = \beta f_2(x)$, với $f_2(x)$ là đa thức nguyên thủy trong $R[x]$ và $\beta = \frac{a}{b} \in F$ thì $adf_2(x) = bcf_1(x)$. Lấy dung tích hai vế ta được $ad = ubc$, với $u \in R^*$. Suy ra $uf_2(x) = f_1(x)$.

Bổ đề 6

Cho R là UFD, F là trường các thương của R và $f(x) \in R[x]$ sao cho $\deg f > 0$. Khi đó, nếu $f(x)$ bất khả quy trong $R[x]$ thì $f(x)$ bất khả quy trong $F[x]$.

Chứng minh

Đặt $c = cont(f)$, ta có $f(x) = cf_1(x)$, với $f_1(x)$ là đa thức nguyên thủy. Do $f(x)$ bất khả quy trong $R[x]$ và các phần tử khả nghịch trong $R[x]$ là phần tử khả nghịch trong R nên $c \in R^*$. Do đó $f(x)$ là đa thức nguyên thủy. Giả sử $f(x)$ không bất khả quy trên F, nghĩa là $f(x) = g(x)h(x)$, với $g(x), h(x) \in F[x], \deg g, \deg h > 0$. Theo Bổ đề 5, $g(x) = \alpha g_1(x)$ và $h(x) = \beta h_1(x)$, với $\alpha, \beta \in F$ và $g_1(x), h_1(x)$ là đa thức nguyên thủy. Vậy $f(x) = \alpha\beta g_1(x)h_1(x)$, trong đó $g_1(x)h_1(x)$ là đa thức nguyên thủy (theo Bổ đề Gauss). Do đó $f(x)$ không bất khả quy trên R, mâu thuẫn.

Định lý 7

Cho R là UFD, F là trường các thương của R và $f(x) \in R[x]$. Khi đó $f(x)$ bất khả quy trong $R[x]$ khi và chỉ khi $f(x)$ bất khả quy trong R hoặc $f(x)$ là vừa nguyên thủy trong $R[x]$ vừa bất khả quy trong $F[x]$.

Chứng minh

Chiều thuận. Giả sử $f(x)$ là đa thức bất khả quy trong $R[x]$.
- Nếu $\deg f = 0$ thì $f = a \in R$ nên f bất khả quy trong R.
- Nếu $\deg f > 0$ thì theo chứng minh Bổ đề 6, f là đa thức nguyên thủy trong $R[x]$ và f bất khả quy trong $F[x]$.

Chiều đảo. Giả sử $f(x) \in R[x]$ là đa thức có bậc lớn hơn 0, nguyên thủy trong $R[x]$ và bất khả quy trong $F[x]$. Giả sử f không bất khả quy trong $R[x]$, nghĩa là $f(x) = g(x)h(x)$, với $g(x), h(x) \in R[x]$. Do $f(x)$ bất khả quy trong $F[x]$ nên $g(x)$ hoặc $h(x)$ là phần tử khác không trong F. Giả sử $g(x) = d \neq 0$. Khi đó, $f(x) = dh(x)$. Do f là đa thức nguyên thủy nên $cont(f) = d.cont(h) \sim 1$, suy ra $d \in R^*$. Vậy f bất khả quy trong $R[x]$.

Định lý 8

Nếu R là một UFD thì $R[x]$ cũng là một UFD.

Chứng minh

Gọi F là trường các thương của R và xét $0 \neq f(x) \in R[x]$.
- Nếu $\deg f = 0$ thì $f = a \in R$. Do R là UFD nên a phân tích một cách chủ yếu duy nhất thành tích các phần tử bất khả quy trong R mà theo Định lý 7 cũng là các phần tử bất khả quy trong $R[x]$.
- Nếu $\deg f > 0$ thì do $F[x]$ là một PID nên ta có thể phân tích $f(x) = \varepsilon p_1(x) \dots p_r(x)$, với $\varepsilon \in F^*$ và các $p_i(x) \in F[x]$ là các đa thức bất khả quy trên F. Theo Bổ đề 5, ta có thể viết $p_i(x) = \alpha_i q_i(x)$, với $\alpha_i \in F$ và các $q_i(x) \in R[x]$ là các đa thức nguyên thủy. Suy ra $f(x) = cq_1(x) \dots q_r(x)$, với $c = \varepsilon\alpha_1 \dots \alpha_r \in F$.

Theo Bổ đề Gauss, $q_1(x) \dots q_r(x)$ là đa thức nguyên thủy, do đó $c = cont(f)$. Do R là UFD nên $c = \varepsilon a_1 \dots a_n$, với $\varepsilon \in R^*$ và a_i là các phần tử bất khả quy trong R. Vậy $f(x) = \varepsilon a_1 \dots a_n q_1(x) \dots q_r(x)$ là sự phân tích $f(x)$ thành tích các phần tử bất khả quy trong $R[x]$.
Về sự duy nhất, giả sử $f(x) = \mu b_1 \dots b_m q_1'(x) \dots q_k'(x)$, với $\mu \in R^*$, các b_i bất khả quy trong R và các $q_j'(x)$ bất khả quy trong $R[x]$. Theo Định lý 7, các $q_j'(x)$ là các đa thức nguyên thủy trong $R[x]$. Do sự phân tích này cũng có thể xem như sự phân tích trong $F[x]$ và các phần tử $\varepsilon a_1 \dots a_n$, $\mu b_1 \dots b_m$ đều khả nghịch trong F nên $r = k$, và bằng cách đánh số lại nếu cần, ta có thể giả thiết $q_i(x)$ liên hợp với $q_i'(x)$. Theo Bổ đề ... thì hai đa thức nguyên thủy trong $R[x]$ nếu liên hợp với nhau trong $F[x]$ sẽ liên hợp với nhau trong $R[x]$. Hơn nữa $cont(f) = \mu b_1 \dots b_m = \varepsilon a_1 \dots a_n$, suy ra $n = m$, và bằng cách đánh số lại nếu cần, ta có b_i liên hợp với a_i. Như vậy ta được kết quả cần chứng minh.

Định lý 9 (Tiêu chuẩn Eisenstein)

Cho R là một UFD với trường các thương F và $f(x) = a_0 + a_1x + \ldots + a_nx^n \in R[x]$, với $n > 0$ và $a_n \neq 0$. Giả sử trong R tồn tại phần tử nguyên tố p thỏa mãn các điều kiện:
i) $p \nmid a_n$;
ii) $p \mid a_i$ với mọi $i = 0, 1, \ldots, n-1$;
iii) $p^2 \nmid a_0$.
Khi đó $f(x)$ là đa thức bất khả quy trên F.

Chứng minh

Nếu viết $f(x) = cont(f)f_1(x)$ thì $f_1(x)$ là đa thức nguyên thủy và cũng thỏa mãn các điều kiện của định lý. Do đó, không mất tính tổng quát, ta có thể giả sử $f(x)$ là đa thức nguyên thủy. Giả sử $f(x)$ khả quy trên F. Khi đó, do Bổ đề 6, $f(x)$ khả quy trên R. Do đó $f(x) = g(x)h(x)$, với $g, h \in R[x], \deg(g) > 1, \deg(h) > 1$. Do $f(x)$ là đa thức nguyên thủy nên $g(x)$ và $h(x)$ cũng là các đa thức nguyên thủy. Giả sử $g(x) = b_0 + b_1x + \ldots + b_lx^l$, $h(x) = c_0 + c_1x + \ldots + c_mx^m$, với $l, m \geq 1, b_lc_m \neq 0$ và $l + m = n$. Do $p \mid a_0 = b_0c_0$ và $p^2 \nmid a_0$ nên $p \mid b_0$ hoặc $p \mid c_0$, nhưng p không đồng thời là ước của b_0 và c_0. Không mất tính tổng quát, giả sử $p \mid b_0, p \nmid c_0$. Do $g(x)$ là đa thức nguyên thủy nên tồn tại một hệ số của $g(x)$ không chia hết cho p. Gọi b_i là hệ số đầu tiên của $g(x)$ không chia hết cho p. Khi đó $1 \leq i < l < n$ và $a_i = b_ic_0 + b_{i-1}c_1 + \ldots$ Do $p \mid a_i$ và $p \mid b_j$ với mọi $j < i$ nên $p \mid b_ic_0$. Nhưng $p \nmid b_i$, nên $p \mid c_0$, mâu thuẫn. Vậy $f(x)$ bất khả quy trên F.

Hệ quả

Cho số nguyên tố p và đa thức $f_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 = \dfrac{x^p - 1}{x - 1}$. Khi

BÀI TẬP

Bài 5.1

Cho R là một UFD và $0 \neq a, b \in R$. Chứng minh rằng $ab = \{a, b\}(a, b)$, trong đó $\{a, b\}$ là BCNN và (a, b) là ƯCLN của a và b.

Bài 5.2

Cho R là một UFD và $0 \neq a, b \in R$. Chứng minh rằng $d = (a, b)$ nếu và chỉ nếu các điều sau được thỏa mãn:
i) $d|a$, $d|b$.
ii) Không tồn tại ước nguyên tố chung p của a' và b', với $a = da', b = db'$.
(Nói riêng, a và b nguyên tố cùng nhau nếu và chỉ nếu không tồn tại ước nguyên tố chung của a và b).

BÀI TẬP

Bài 5.3

Cho R là một miền nguyên. Chứng minh rằng các điều sau tương đương:
i) R là một UFD.
ii) Mọi cặp phần tử $a, b \in R$ đều có ƯCLN. Hơn nữa trong R không tồn tại một dãy vô hạn các phần tử $a_1, a_2, \ldots$ sao cho $a_{i+1} | a_i$, nhưng $a_i \nmid a_{i+1}$.
iii) Mọi phần tử bất khả quy của R đều nguyên tố. Hơn nữa tập các ideal chính của R thỏa mãn điều kiện ACC (với quan hệ bao hàm $\subseteq$).
iv) Mọi ideal chính tối đại của R là ideal nguyên tố. Hơn nữa tập các deal chính của R thỏa mãn điều kiện ACC (với quan hệ bao hàm $\subseteq$).
v) Mọi phần tử khác 0 của R đều được viết dưới dạng tích của một phần tử khả nghịch và một số hữu hạn các phần tử nguyên tố của R.

BÀI TẬP

Bài 5.4

Cho R là một UFD và $\{r_i\}_{i=1}^n$ là một tập hữu hạn các phần tử khác 0 đôi một nguyên tố cùng nhau trong R (nghĩa là $(r_i, r_j) = 1, \forall i \neq j$). Đặt $a = \prod_{i=1}^{n} r_i$ và $a = r_i a_i$. Chứng minh rằng $\{a_i\}_{i=1}^n$ là tập hợp gồm các phần tử đôi một nguyên tố cùng nhau.

Bài 5.5

Cho R là một UFD với trường các thương F. Chứng minh rằng $d \in R$ là một bình phương trong R khi và chỉ khi d là một bình phương trong F (nghĩa là, nếu phương trình $a^2 = d$ có nghiệm $a \in F$ thì $a \in R$). Cho ví dụ chứng tỏ điều này không còn đúng nếu R không là UFD.

BÀI TẬP

Bài 5.6

Cho R là một UFD với trường các thương F và $f(x)$ là một đa thức đơn khởi trong $R[x]$. Chứng minh rằng, nếu $f(x)$ có nghiệm trong F thì nghiệm này nằm trong R.

Bài 5.7

Phân tích đa thức $x^4 - x^2 - 2$ thành tích các đa thức bất khả quy trên $\mathbb{Q}$, trên $\mathbb{R}$, trên $\mathbb{C}$ và trên $\mathbb{Z}_5$.

Bài 5.8

Hãy phân tích đa thức $x^3 + 3$ thành tích các đa thức bất khả quy trong $\mathbb{Z}_5[x]$, trong $\mathbb{Z}_7[x]$.

BÀI TẬP

Bài 5.9

Xét sự phân tích của đa thức sau đây trong vành đa thức $\mathbb{Z}_5[x]$:

$$3x^3 + 4x^2 + 3 = (x+2)^2(3x+2) = (x+2)(x+4)(3x+1).$$

Hãy giải thích tại sao các sự phân tích nói trên không dẫn đến sự mâu thuẫn với việc $\mathbb{Z}_5[x]$ là một UFD.

Bài 5.10

Với các số nguyên tố p nào thì đa thức $x^3 + 2x^2 + 2x + 4$ chia hết cho đa thức $x^2 + x + 1$ trong $\mathbb{Z}_p[x]$?

BÀI TẬP

Bài 5.11

a) Chứng minh rằng đa thức $x^5 + x^3 + 1$ bất khả quy trên $\mathbb{Z}$.

b) Chứng minh rằng điều kiện cần và đủ để đa thức $x^3 + ax^2 + bx + 1$ khả quy trên $\mathbb{Z}$ là $a = b$ hoặc $a + b = -2$.

Bài 5.12

Chứng minh rằng đa thức $x^3 + 3x^2 + 6x + 6$ bất khả quy trên $\mathbb{Q}$.

Bài 5.13

Đa thức $2x^{10} - 25x^3 + 10x^2 - 30$ có bất khả quy trên $\mathbb{Q}$ hay không? Giải thích.

BÀI TẬP

Bài 5.14

Cho p là một số nguyên tố. Chứng minh rằng p là phần tử nguyên tố trong vành $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ khi và chỉ khi phương trình $x^2 + y^2 = p$ không có nghiệm nguyên.

Bài 5.15

Với $\alpha = a + b\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$, định nghĩa $N(\alpha) = a^2 - 5b^2$. Chứng minh rằng:
a) $N(\alpha\beta) = N(\alpha)N(\beta)$;
b) α khả nghịch khi và chỉ khi $N(\alpha) = \pm 1$;
c) $4 + \sqrt{5}$ là phần tử nguyên tố trong $\mathbb{Z}[\sqrt{5}]$.

BÀI TẬP

Bài 5.16

Chứng minh rằng $\mathbb{Z}_{11}[x]/\langle x^2 + 1\rangle$ là trường chứa 121 phần tử.

Bài 5.17

Cho ví dụ về một UFD nhưng không là PID.

§6. Miền nguyên Dedekind

Ideal phân thức

Cho R là miền nguyên với trường các thương F và $A \subseteq F$. Ta gọi A là một *ideal phân thức* của R nếu nó thỏa mãn các điều sau:
i) $(A, +)$ là nhóm con của $(F, +)$.
ii) Với mọi $r \in R$ và với mọi $a \in A$ ta có $ra \in A$.
iii) Tồn tại $0 \neq d \in R$ sao cho $dA \subseteq R$.

Nhận xét 1

- Nếu A là ideal phân thức của R thì dA là ideal của R, với d như trong iii).
- Mọi ideal của R cũng có thể xem như một ideal phân thức (lấy $d = 1$). Ta gọi các ideal của R là *ideal nguyên*.

§6. Miền nguyên Dedekind

Mệnh đề 1

Cho R là miền nguyên với trường các thương F và $A, B \subseteq F$ là hai ideal phân thức khác $\{0\}$ của R. Đặt $AB = \{\sum a_i b_i \mid a_i \in A, b_i \in B\}$. Khi đó AB cũng là một ideal phân thức khác $\{0\}$ của R.

Chứng minh

Hiển nhiên AB thỏa mãn i) và ii) trong Định nghĩa trên. Nếu $0 \neq d_1, d_2 \in R$ sao cho $d_1 A \subseteq R$ và $d_2 B \subseteq R$ thì với $d = d_1 d_2$ ta có $dAB \subseteq R$, nghĩa là điều kiện iii) của Định nghĩa trên cũng thỏa mãn.

Ký hiệu $\mathcal{L}(R)$ là tập tất cả các ideal nguyên khác $\{0\}$ của R và $\mathcal{L}_*(R)$ là tập tất cả các ideal phân thức khác $\{0\}$ của R. Hiển nhiên $\mathcal{L}(R) \subseteq \mathcal{L}_*(R)$.

Hệ quả 2

$\mathcal{L}_*(R)$ là một vị nhóm với phần tử đơn vị là R.

Ideal phân thức khả nghịch

Ideal phân thức A của miền nguyên R được gọi là *ideal phân thức khả nghịch* nếu A là phần tử khả nghịch trong vị nhóm $\mathcal{L}_*(R)$. Khi đó ta ký hiệu A^{-1} là nghịch đảo của A trong $\mathcal{L}_*(R)$. Vậy, $AA^{-1} = A^{-1}A = R$.

Mệnh đề 3

Cho R là miền nguyên và A là ideal phân thức khả nghịch của R.
Khi đó, tồn tại $a_1, ..., a_n \in A$ sao cho $A = a_1R + \ldots + a_nR$.

Chứng minh

Giả sử A^{-1} nghịch đảo của A. Do $1 \in R = AA^{-1}$ nên $1 = a_1a'_1 + ... + a_na'_n$, với $a_i \in A, a'_i \in A^{-1}$. Khi đó, với mọi $a \in A$ ta có $a = a_1(a'_1a) + ... + a_n(a'_na)$, trong đó $a'_ia \in A^{-1}A = R$. Do đó $a \in a_1R + \ldots + a_nR$. Như vậy $A \subseteq a_1R + \ldots + a_nR$. Ngược lại, hiển nhiên $a_1R + \ldots + a_nR \subseteq A$. Do đó $A = a_1R + \ldots + a_nR$.

Hệ quả 4

Nếu mọi ideal nguyên khác 0 của R đều khả nghịch thì R là vành Noether.

§6. Miền nguyên Dedekind

Miền nguyên Dedekind

Miền nguyên R được gọi là *miền nguyên Dedekind* nếu mọi ideal thực sự của R đều viết được thành tích của hữu hạn các ideal nguyên tố của R.

Mệnh đề 5

Mọi PID đều là miền nguyên Dedekind.

Chứng minh

Cho R là một PID và I là một ideal thực sự khác 0 của R. Khi đó $I = \langle a \rangle$, với $0 \neq a \in R$. Phân tích a thành tích các thừa số nguyên tố: $a = \varepsilon p_1 ... p_n$, với $\varepsilon \in R^*$ và các p_i là các phần tử nguyên tố. Khi đó $I = \langle p_1 \rangle ... \langle p_n \rangle$, là tích của các ideal nguyên tố $\langle p_i \rangle$.

§6. Miền nguyên Dedekind

Bổ đề 6

Cho $I_1, \ldots, I_m$ và $J_1, \ldots, J_n$ là các ideal nguyên tố khác $\{0\}$ của miền nguyên R sao cho $I_1 ... I_m = J_1 ... J_n$. Khi đó, nếu mọi I_i, J_j đều khả nghịch trong $\mathcal{L}_*(R)$ thì $m = n$ và tồn tại một hoán vị $\sigma \in S_n$ sao cho $I_i = J_{\sigma(i)}$ với mọi i.

Chứng minh

- Giả sử $m = 1$ và $n \geq 2$. Đặt $A_1 = J_1$ và $A_2 = J_2...J_n$. Khi đó $I_1 = A_1A_2$. Mà I_1 là ideal nguyên tố nên $A_1 \subseteq I_1$ hoặc $A_2 \subseteq I_1$. Nếu $A_1 \subseteq I_1$ thì $R = I_1^{-1}I_1 = I_1^{-1}A_1A_2 \subseteq (I_1^{-1}I_1)A_2 = RA_2 \subseteq A_2$, mâu thuẫn. Tương tự, nếu $A_2 \subseteq I_1$ ta cũng có điều mâu thuẫn. Vậy $m = 1$ khi và chỉ khi $n = 1$.
- Nếu $m, n \geq 2$ thì, bằng cách thay đổi vị trí các ideal nếu cần, ta có thể giả sử I_1 không chứa thực sự trong nó bất kỳ một ideal I_i nào với mọi $i \geq 2$. Do I_1 là ideal nguyên tố nên tồn tại J_j sao cho $J_j \subseteq I_1$. Đánh số lại nếu cần, ta có thể giả sử $J_1 \subseteq I_1$. Tương tự, do J_1 cũng là ideal nguyên tố nên ta tìm được I_i sao cho $I_i \subseteq J_1$. Vậy $I_i \subseteq J_1 \subseteq I_1$. Do cách chọn I_1 nên ta suy ra $I_i = I_1$, kéo theo $J_1 = I_1$. Từ $I_1...I_m = J_1...J_n$, nhân hai vế với I_1^{-1}, nhận được $I_2 \dots I_m = J_2 \dots J_n$. Tiếp tục quá trình trên và chú ý đến trường hợp đầu, ta được kết quả cần chứng minh.

Bổ đề 7

Cho R là miền nguyên Dedekind. Khi đó, mọi ideal nguyên tố khả nghịch của R đều tối đại.

Chứng minh

Giả sử I là ideal nguyên tố khả nghịch nhưng không tối đại của R. Khi đó tồn tại $a \in R \setminus I$ sao cho $I + aR \neq R$. Suy ra $\{0\} \neq I + a^2R \subseteq I + aR \subsetneq R$. Do đó $I + aR = I_1...I_m$ (1) và $I + a^2R = J_1...J_n$ (2), với các I_i, J_j là các ideal nguyên tố của R. Xét đồng cấu tự nhiên $\varphi : R \to R/I$. Do I là ideal nguyên tố nên $\overline{R} = R/I$ là miền nguyên. Ta có $\overline{aR} = \overline{I_1}...\overline{I_m}$ (3) và $\overline{a^2R} = \overline{J_1}...\overline{J_n}$(4), trong đó $\overline{A}$ là ảnh của $A \subseteq R$ qua đồng cấu tự nhiên φ. Hiển nhiên $\overline{I_i}$ và $\overline{J_k}$ đều là các ideal nguyên tố của miền nguyên R/I.

Từ (3) suy ra $\overline{R} = \left(\frac{1}{\overline{a}}\right)\overline{I_1}\ldots\overline{I_m}$ (5) và $\overline{R} = \left(\frac{1}{\overline{a^2}}\right)\overline{J_1}\ldots\overline{J_n}$ (6).

Do đó các $\overline{I}_i$ và $\overline{J}_k$ đều là các ideal phân thức khả nghịch của miền nguyên $\overline{R}$, suy ra tất cả các ideal $\overline{I}_i$ và $\overline{J}_k$ đều khác $\{\overline{0}\}$. Nhận xét rằng $\overline{a^2R} = (\overline{aR})^2$, nên từ (3), (4) và từ Bổ đề 6 suy ra $n = 2m$ và, sắp xếp lại các ideal $\overline{J}_k$ nếu cần, ta có $\overline{I_h} = \overline{J_h} = \overline{J_{m+h}}, 1 \le h \le m$ (7). Từ (1) và (2) ta thấy rằng ideal I nằm trong mọi ideal I_h và J_h. Do đó, áp dụng Định lý về sự tương ứng suy ra $I_h = J_h = J_{m+h}$. Do đó $(I + aR)^2 = I + a^2R$ (8). Suy ra $I \subseteq I + a^2R = (I + aR)^2 \subseteq I^2 + aR$. Do đó với mọi $x \in I$, tồn tại $y \in I^2, z \in R$ sao cho $x = y + az$ hay $az = x - y \in I$. Vì I nguyên tố và $a \notin I$ nên từ đó suy ra $z \in I$, do đó $x \in I^2 + aI$. Suy ra $I^2 + aI = I$. Theo giả thiết I khả nghịch trong $\mathcal{L}_*(R)$, nên nhân hai vế của đẳng thức trên với I^{-1}, nhận được $I + aR = R$, là một mâu thuẫn. Vậy bổ đề đã được chứng minh.

Định lý 8

Cho R là miền nguyên. Khi đó, R là miền nguyên Dedekind khi và chỉ khi $\mathcal{L}_*(R)$ là một nhóm.

Chứng minh

Chiều đảo. Giả sử $\mathcal{L}_*(R)$ là một nhóm. Theo Hệ quả 4, R là vành Noether. Đặt $\Re$ là tập hợp tất cả các ideal J của R, $\{0\} \subset J \subset R$, sao cho J không phân tích thành tích của một số hữu hạn các ideal tối đại của R. Giả sử $\Re \neq \emptyset$. Do R là vành Noether nên trong $\Re$ có ít nhất một phần tử tối đại, gọi là I. Hiển nhiên I không là ideal tối đại của R, nên tồn tại một ideal tối đại M của R sao cho $I \subset M$. Suy ra $M^{-1}I \subseteq M^{-1}M = R$, do đó $M^{-1}I$ là ideal nguyên của R. Mặt khác, ta có $I = RI = M^{-1}MI = M^{-1}(MI) \subseteq M^{-1}I$.

Nếu $I \neq M^{-1}I$ thì từ tính tối đại của I trong $\Re$ suy ra $M^{-1}I$ phân tích thành tích của một số hữu hạn các ideal tối đại của R, nên $I = M(M^{-1}I)$ cũng có tính chất ấy. Do đó $I = M^{-1}I$, hay $I = MI$. Từ đó $M = (MI)I^{-1} = II^{-1} = R$, là một mâu thuẫn.

Chiều thuận. Giả sử R là miền nguyên Dedekind và A là một ideal phân thức khác $\{0\}$ bất kỳ của R, ta chứng minh A khả nghịch. Vì $A \neq \{0\}$ nên tồn tại $0 \neq d \in R$ sao cho $I = dA$ là ideal của R. Theo giả thiết I phân tích thành tích những ideal nguyên tố của R: $I = dA = I_1 \dots I_n$, trong đó I_k là ideal nguyên tố. Hiển nhiên A khả nghịch nếu I khả nghịch, còn I khả nghịch nếu mọi I_k khả nghịch. Vậy ta chỉ cần chứng minh mọi ideal nguyên tố khác $\{0\}$ đều khả nghịch. Do đó ta có thể giả sử I là một ideal nguyên tố khác $\{0\}$. Lấy phần tử $0 \neq a \in I$. Khi đó Ra là ideal khác $\{0\}$ của R. Phân tích Ra thành tích các ideal nguyên tố của R: $Ra = J_1 \dots J_m$.

Suy ra $R = \left(\frac{1}{a}R\right)(Ra) = \left(\frac{1}{a}R\right)J_1 \dots J_m$.

Đẳng thức trên chứng tỏ mọi J_k đều khả nghịch. Vì $I \neq R, I$ nguyên tố và $a \in I$ nên từ điều kiện $Ra = J_1 \dots J_m \subseteq I$ suy ra tồn tại $k \in \{1, \dots, m\}$ sao cho $J_k \subseteq I$. Vì J_k là ideal nguyên tố và khả nghịch, nên theo Bổ đề 7, J_k là ideal tối đại của R. Suy ra $J_k = I$, do đó I khả nghịch.

BÀI TẬP

Bài 6.1

a) Cho K là trường. Chứng minh rằng $K[x]$ là miền nguyên Dedekind.
b) Chứng minh rằng $\mathbb{Z}[x]$ không là miền nguyên Dedekind.
c) Tổng quát, chứng minh rằng, nếu R là miền nguyên nhưng không là trường thì $R[x]$ không là miền nguyên Dedekind.

Bài 6.2

Cho R là miền nguyên Dedekind. Chứng minh rằng mọi ideal của R đều là ideal chính hoặc ideal sinh bởi hai phần tử.

Bài 6.3

Chứng minh rằng mọi miền nguyên Dedekind đều là vành Noether.

BÀI TẬP

Bài 6.4

Chứng minh rằng $\mathbb{Z}[\sqrt{-3}]$ không là miền nguyên Dedekind.

Bài 6.5

Cho R là miền nguyên Dedekind với trường các thương K và A, B là các ideal phân thức của R. Ta nói A *chia hết cho* B, nếu tồn tại ideal nguyên C của R sao cho $A = BC$. Chứng minh A chia hết cho B khi và chỉ khi $A \subset B$.