

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM TP.HỒ CHÍ MINH**

Lê Quang Hào

**SỐ HỌC TRÊN VÀNH CÁC SỐ
NGUYÊN ĐẠI SỐ**

**Chuyên ngành : Đại số và Lý thuyết số
Mã số : 60 46 05**

LUẬN VĂN THẠC SĨ TOÁN HỌC

**Người hướng dẫn khoa học :
PGS.TS My Vinh Quang**

Tp. Hồ Chí Minh – 2005

LỜI CẢM ƠN

Tôi xin chân thành bày tỏ lòng biết ơn đối với quý Thầy Cô trong tổ Đại số trường Đại học Sư phạm Thành phố Hồ Chí Minh và trường Đại học Khoa học Tự nhiên thành phố Hồ Chí Minh đã trực tiếp giảng dạy và trang bị cho tôi đầy đủ kiến thức làm nền tảng cho quá trình viết luận văn này.

Đặc biệt tôi xin chân thành tỏ lòng biết ơn sâu sắc đối với PGS.TS My Vinh Quang người đã trực tiếp hướng dẫn tôi hoàn thành luận văn này.

Tôi xin chân thành cảm ơn quý Thầy Cô trong hội đồng chấm luận văn đã dành thời gian đọc và đóng góp nhiều ý kiến quý báu cho luận văn.

Tôi xin chân thành cảm ơn phòng Khoa học Công nghệ và Sau Đại học trường Đại học Sư Phạm thành phố Hồ Chí Minh, trường Trung học phổ thông chuyên Huỳnh Mẫn Đạt tỉnh Kiên Giang đã giúp đỡ và tạo điều kiện thuận lợi cho tôi trong quá trình học tập.

Tôi tỏ lòng biết ơn đến gia đình, anh em và bạn bè đã hỗ trợ và giúp đỡ tôi về tinh thần cũng như vật chất để tôi hoàn thành luận văn này.

MỤC LỤC

Lời cảm ơn	1
Mục lục	2
Mở đầu	3
Chương 1 : CÁC KIẾN THỨC CƠ BẢN	5
1.1 : Nửa nhóm với sự phân tích thành các nhân tử nguyên tố	5
1.2 : Nhóm Abel hữu hạn sinh	8
1.3 : Chuẩn và vết của số đại số	12
1.4 : Ideal trong vành giao hoán có đơn vị	14
1.5 : Thặng dư bậc hai	16
Chương 2 : CÁC IDEAL TRONG VÀNH CÁC SỐ NGUYÊN ĐẠI SỐ	18
2.1 : Vành các số nguyên đại số của trường mở rộng hữu hạn của $\mathbb{Q}$...	18
2.2 : Một số tính chất của vành D	19
2.3 : Nửa nhóm các Ideal của vành D	22
Chương 3 : SỐ HỌC TRONG VÀNH CÁC SỐ NGUYÊN ĐẠI SỐ	31
3.1 : Các khái niệm cơ bản	31
3.2 : Hàm chuẩn N – Các tính chất của hàm chuẩn	32
3.3 : Hàm Euler – Các tính chất của hàm Euler	34
3.4 : Các định lý số học trên vành D	39
Chương 4 : SỐ HỌC TRÊN VÀNH $D = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$	42
4.1 : Vành $D = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$	42
4.2 : Thuật toán phân tích ra thừa số nguyên tố - Các ví dụ	50
Kết luận	53
Tài liệu tham khảo	55

LỜI MỞ ĐẦU

Vành D các số nguyên đại số của trường mở rộng hữu hạn K của Q nói chung không phải là vành Gauss (xem ví dụ chương 4), cho nên số học trong đó rất khó nghiên cứu. Cụ thể là trong vành D , định lý cơ bản của số học không còn đúng nữa, một số có thể phân tích được thành tích các phần tử nguyên tố theo nhiều cách khác nhau (xem ví dụ chương 4). Mục đích của luận văn này là dựa vào sự phân tích duy nhất của các ideal của D thành tích các ideal tối đại, chúng tôi xây dựng số học trên vành các số nguyên đại số.

Bố cục của luận văn được chia thành 4 chương :

- **Chương 1** : Các kiến thức cơ bản

Trong chương này chúng tôi trình bày các kiến thức cơ bản liên quan đến đề tài : nửa nhóm với sự phân tích thành các phần tử nguyên tố; nhóm abel hữu hạn sinh; chuẩn và vết của số đại số; thặng dư bậc hai.

- **Chương 2** : Các ideal trong vành các số nguyên đại số

Mục đích của chương này là nghiên cứu tính chất của các ideal của vành các số nguyên đại số D và chứng minh mọi ideal của vành D phân tích được thành tích của các ideal tối đại.

- **Chương 3** : Số học trong vành các số nguyên đại số của trường mở rộng hữu hạn của Q .

Dựa vào sự phân tích duy nhất của các ideal của vành D thành các ideal tối đại từ đó chúng tôi xây dựng số học trên vành các số nguyên đại số.

- **Chương 4** : Số học trên vành $D = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$

Mục đích của chương này là khảo sát một cách chi tiết số học trên vành

$D = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$, cụ thể ta mô tả các ideal tối đại của vành D ; mô tả thuật toán phân tích một phần tử của D thành tích của các ideal tối đại. Đồng thời đưa ra một số ví dụ minh họa.

Vì khả năng và thời gian còn hạn chế nên luận văn này không thể tránh khỏi những thiếu sót. Kính mong quý Thầy Cô và các bạn đóng góp ý kiến bổ sung để luận văn được hoàn chỉnh hơn.

CHƯƠNG 1

CÁC KIẾN THỨC CƠ BẢN

Trong chương này chúng tôi trình bày các kiến thức cơ bản liên quan đến đề tài : Nửa nhóm với sự phân tích thành các nhân tử nguyên tố; Nhóm Abel tự do; Chuẩn và vết của số đại số ; Thặng dư bậc hai

1.1 NỬA NHÓM VỚI SỰ PHÂN TÍCH THÀNH CÁC NHÂN TỬ NGUYÊN TỐ

1.1.1 Định nghĩa : Cho P là nửa nhóm nhân giao hoán có đơn vị E .

Ta nói $B|A$ nếu tồn tại $C \in P$ sao cho $A = B.C$

- Nếu $B|A$; $B \neq A$; $B \neq E$ thì ta nói B là ước thực sự của A .
- $P \in P$ được gọi là phần tử nguyên tố nếu P không có ước thực sự
- Phần tử $C \in P$ được gọi là USCLN của A, B nếu $C|A$, $C|B$ và C chia hết cho mọi ước chung của của A và B , ký hiệu $C = (A, B)$
- Phần tử $C \in P$ được gọi là BSCNN của A, B nếu $C : A$, $C : B$ và C là ước của mọi bội số chung của A, B , ký hiệu $C = [A, B]$

Hoàn toàn tương tự ta có khái niệm USCLN; BSCNN của nhiều phần tử.

1.1.2 Định nghĩa : Nửa nhóm giao hoán có đơn vị P được gọi là nửa nhóm với sự phân tích duy nhất thành các nhân tử nguyên tố nếu với $\forall A \in P$, $A \neq E$ đều có thể viết duy nhất, không kể thứ tự, dưới dạng

$$A = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_n^{k_n} ; n \geq 1 ; p_i \text{ nguyên tố } , k_i \geq 1.$$

Từ nay về sau ta quy ước P là nửa nhóm với sự phân tích thành các nhân tử nguyên tố.

Ta có nhận xét sau :

Nếu $A = P_1^{\alpha_1} \dots P_n^{\alpha_n}$, $\alpha_i \geq 0$; $B = P_1^{\beta_1} \dots P_n^{\beta_n}$, $\beta_i \geq 0$. Khi đó,

$$A|B \Leftrightarrow \alpha_i \leq \beta_i, \forall i$$

1.1.3 Mệnh đề : Trong $\mathcal{P}$ hai phần tử bất kỳ đều có duy nhất USCLN và BSCNN

Chứng minh : Giả sử $A \in \mathcal{P}$, $B \in \mathcal{P}$ với

$$A = P_1^{k_1} \dots P_n^{k_n}; B = P_1^{l_1} \dots P_n^{l_n}; k_i \geq 0, l_i \geq 0$$

⊕ Xét phần tử $C = P_1^{\alpha_1} \dots P_n^{\alpha_n}$ trong đó $\alpha_i = \min \{k_i, l_i\}$, $i = \overline{1, n}$ rõ ràng

$$C \in \mathcal{P}, C|A, C|B. \text{ Lấy phần tử } D \text{ sao cho } D|A, D|B \Rightarrow D = P_1^{m_1} \dots P_n^{m_n}$$

với $m_i \leq k_i$; $m_i \leq l_i$, $i = \overline{1, n} \Rightarrow m_i \leq \alpha_i \forall i = \overline{1, n} \Rightarrow D|C$. Vậy ta có

$$C = (A, B).$$

C là duy nhất vì giả sử $D = (A, B)$, $D = P_1^{\gamma_1} \dots P_n^{\gamma_n}$. Do $D|C \Rightarrow \gamma_i \leq \alpha_i$, mặt khác $C|D \Rightarrow \alpha_i \leq \gamma_i$. Vậy $\alpha_i = \gamma_i$, từ đó suy ra $D = C$.

⊕ Xét phần tử $C = P_1^{\alpha_1} \dots P_n^{\alpha_n}$ trong đó $\alpha_i = \max \{k_i, l_i\}$, $i = \overline{1, n}$. Rõ ràng

$$C \in \mathcal{P}, C : A, C : B. \text{ Lấy phần tử } D : A, D : B \Rightarrow D = P_1^{t_1} \dots P_n^{t_n} \text{ với } t_i \geq$$

$$k_i,$$

$t_i \geq l_i$, $i = \overline{1, n} \Rightarrow t_i \geq \alpha_i$, $i = \overline{1, n} \Rightarrow D : C$. Vậy ta có $C = [A, B]$. Tương tự ở trên ta chứng minh được C là duy nhất.

1.1.4 Mệnh đề :

Nếu $(A, C) = E$ và B tùy ý thì $(AB, C) = (B, C)$

Chứng minh

Do $(A, C) = E$ nên không mất tính chất tổng quát ta giả sử

$A = P_1^{k_1} \dots P_t^{k_t}$; $C = P_{t+1}^{k_{t+1}} \dots P_n^{k_n}$ và giả sử $B = P_1^{l_1} \dots P_t^{l_t} \dots P_n^{l_n}$ khi đó

$$(B, C) = P_{t+1}^{\min\{k_{t+1}, l_{t+1}\}} \dots P_n^{\min\{k_n, l_n\}}$$

Mặt khác $A \cdot B = P_1^{k_1+l_1} \dots P_t^{k_t+l_t} \dots P_n^{k_n+l_n}$

$$\Rightarrow (AB, C) = P_{t+1}^{\min\{k_{t+1}, l_{t+1}\}} \dots P_n^{\min\{k_n, l_n\}} \text{ hay } (AB, C) = (B, C)$$

1.1.5 Mệnh đề : $A, B, C \in \mathcal{P}$; $AB : C$ và $(A, C) = E$ thì $B : C$

Chứng minh

Do $AB : C \Rightarrow (AB, C) = C$. Mặt khác theo mệnh đề 1.1.3 ta có

$$(AB, C) = (B, C) \text{ hay } (B, C) = C \Rightarrow B : C$$

1.1.6 Mệnh đề : $A, B, C \in \mathcal{P}$ và $A : B$, $A : C$, $(B, C) = E$ thì $A : BC$

Chứng minh

Giả sử $A = P_1^{k_1} \dots P_n^{k_n}$; $B = P_1^{l_1} \dots P_t^{l_t}$; $C = P_{t+1}^{l_{t+1}} \dots P_n^{l_n}$

(do $(B, C) = E$). Mặt khác vì $A : B$, $A : C$ nên $(A, B) = B$; $(A, C) = C$

hay $(A, B) = P_1^{l_1} \dots P_t^{l_t}$; $(A, C) = P_{t+1}^{l_{t+1}} \dots P_n^{l_n}$. ta lại có $B.C = P_1^{l_1} \dots P_n^{l_n}$

$$(A, BC) = P_1^{\min\{k_1, l_1\}} \dots P_n^{\min\{k_n, l_n\}} = P_1^{l_1} \dots P_t^{l_t} \dots P_n^{l_n} \text{ hay } (A, BC) = BC$$

1.1.7 Mệnh đề : P nguyên tố, $P|AB$ thì $P|A$ hoặc $P|B$

Chứng minh

Giả sử $P|A$, $P|B$ suy ra sự phân tích của A không chứa P và sự phân tích của B không chứa P do đó AB không chứa P . Suy ra $P|AB$ (trái giả thiết).

Vậy $P|A$ hoặc $P|B$

1.1.8 Mệnh đề $\forall A, B, C \in \mathcal{P}$ thì

$$a) [A, B]C = [AC, BC]$$

$$b) (A, B)C = (AC, BC)$$

$$c) A, B = AB$$

Chứng minh

$$\text{Giả sử } A = P_1^{k_1} \dots P_n^{k_n}; B = P_1^{l_1} \dots P_n^{l_n}; C = P_1^{t_1} \dots P_n^{t_n}$$

$$a) \text{ Ta có } [A, B] = P_1^{\max\{k_1, l_1\}} \dots P_n^{\max\{k_n, l_n\}}$$

$$\Rightarrow [A, B].C = P_1^{\max\{k_1, l_1\}+t_1} \dots P_n^{\max\{k_n, l_n\}+t_n}$$

$$[AC, BC] = P_1^{\max\{k_1+t_1, l_1+t_1\}} \dots P_n^{\max\{k_n+t_n, l_n+t_n\}}$$

$$= P_1^{\max\{k_1, l_1\}+t_1} \dots P_n^{\max\{k_n, l_n\}+t_n} \text{ Vậy } [A, B]C = [AC, BC]$$

$$b) \text{ Tương tự } (A, B)C = (AC, BC)$$

$$c) \text{ Ta có } A, B = P_1^{\max\{k_1, l_1\}+\min\{k_1, l_1\}} \dots P_n^{\max\{k_n, l_n\}+\min\{k_n, l_n\}}$$

$$= P_1^{k_1+l_1} \dots P_n^{k_n+l_n} = AB$$

1.2 NHÓM ABEL HỮU HẠN SINH

1.2.1 Định nghĩa : Cho G là một nhóm Abel, hệ $\{\alpha_i\}_{i \in I} \subset G$ gọi là độc lập tuyến tính nếu $\sum_{i \in I} a_i \alpha_i = 0$ với $\forall a_i \in \mathbb{Z}$ và hữu hạn các $a_i \neq 0$ thì

$$a_i \alpha_i = 0 \quad \forall i$$

1.2.2 Định nghĩa :

Hệ $\{\alpha_i\}_{i \in I} \subset G$ được gọi là hệ sinh của nhóm abel G nếu $G = \langle \alpha_i \rangle_{i \in I}$ tức là với $\forall g \in G$ đều được viết dưới dạng $g = \sum_{i \in I} a_i \alpha_i$ với $\forall a_i \in \mathbb{Z}$ và hữu

hạn các $a_i \neq 0$.

Hệ $\{\alpha_i\}_{i \in I} \subset G$ được gọi là cơ sở của G nếu nó độc lập tuyến tính và là hệ sinh của G .

Từ định nghĩa cơ sở của nhóm abel ta có kết quả : Nhóm abel G có cơ sở $\{\alpha_i\}_{i \in I}$ khi và chỉ khi G phân tích được thành tổng trực tiếp của các nhóm xiclic sinh bởi α_i , tức là $G = \sum_{i \in I} \langle \alpha_i \rangle$

Trong lý thuyết môđun ta biết rằng nhóm abel (có thể xem như là môđun trên $\mathbb{Z}$) là nhóm abel tự do khi và chỉ khi nó phân tích được thành tích các nhóm xiclic cấp vô hạn. Do đó, G là nhóm abel tự do khi và chỉ khi G là nhóm abel không xoắn, có cơ sở.

1.2.3 Định lý : G là nhóm abel tự do thì các cơ sở có cùng lực lượng.

Chứng minh :

Giả sử $\alpha = \{\alpha_i\}_{i \in I}$ là cơ sở của G và giả sử p là một số nguyên tố, từ đó ta có $\mathbb{Z}/p\mathbb{Z}$ là một trường. Khi đó nhóm thương G/pG có cấu trúc không gian vectơ trên trường $\mathbb{Z}/p\mathbb{Z}$ với tích vô hướng được xác định như sau :

$$\varphi : \mathbb{Z}/p\mathbb{Z} \times G/pG \rightarrow G/pG$$

$$(a + p\mathbb{Z}, g + pG) \mapsto ag + pG$$

Ta thấy rằng phép nhân này không phụ thuộc đại diện các lớp vì nếu :

$$\begin{cases} a + p\mathbb{Z} = a' + p\mathbb{Z} \\ g + pG = g' + pG \end{cases} \Rightarrow \begin{cases} a' = a + pz, z \in \mathbb{Z} \\ g' = g + pu, u \in G \end{cases}$$

Khi đó $a'g' = (a + pz)(g + pu) = ag + pau + pzg + pzpu \in ag + pG$

Vậy $a'g' + pG = ag + pg$

Vì $\{\alpha_i\}_{i \in I}$ là cơ sở của G nên với $\forall g \in G$ ta đều biểu diễn một cách duy nhất dưới dạng $g = \sum_{i \in I} a_i \alpha_i$ với $\forall a_i \in \mathbb{Z}$ và hữu hạn các $a_i \neq 0$. Từ đó suy ra mỗi

phần tử $g + pG \in G/pG$ đều được dưới dạng :

$$g + pG = \sum_{i \in I} a_i \alpha_i + pG = \sum_{i \in I} (a_i \alpha_i + pG)$$

$$= \sum_{i \in I} (a_i + pZ)(\alpha_i + pG).$$
 Bây giờ ta chứng minh hệ $\{\alpha_i + pG\}_{i \in I}$ là độc lập tuyến tính. Thật vậy xét đẳng thức $\sum_{i \in I} (a_i \alpha_i + pG) = 0$ hay $\sum_{i \in I} \overline{a_i \alpha_i} = 0$
 $\Rightarrow a_i \alpha_i \in pG \Rightarrow \exists u \in G$ để $a_i \alpha_i = pu$. Do $u \in G \Rightarrow u = \sum_{i \in I} b_i \alpha_i$
 $\Rightarrow a_i \alpha_i = p \sum_{i \in I} b_i \alpha_i \Rightarrow \sum_{i \in I} (a_i - pb_i) \alpha_i = 0$ mà G không xoắn nên suy ra
 $a_i - pb_i = 0 \Rightarrow a_i = pb_i$ hay $a_i : p \Rightarrow \overline{a_i} = 0$
 Vậy $\sum_{i \in I} (a_i + pZ)(\alpha_i + pG) = 0$ kéo theo $a_i + pZ = 0$ hay hệ $\{\alpha_i + pG\}_{i \in I}$ độc lập tuyến tính. Vậy hệ $\{\alpha_i + pG\}_{i \in I}$ là cơ sở của không gian vector trên trường Z/pZ . Từ đó suy ra $|\alpha| = |\{\alpha_i + pG\}_{i \in I}| = \dim G/pG$ vậy $|\alpha|$ là duy nhất xác định.

1.2.4 Định nghĩa : Số phần tử của một cơ sở của nhóm abel tự do G gọi là hạng của G . Ký hiệu $\text{rank } G$.

1.2.5 Hệ quả : Cho G là một nhóm abel tự do có $\text{rank } G = n$. Khi đó mọi hệ độc lập tuyến tính trong G đều có số vector không vượt quá n .

Chứng minh

Giả sử $\alpha_1, \dots, \alpha_k$ là hệ độc lập tuyến tính trong G , theo chứng minh trên ta suy ra $\overline{\alpha_1}, \dots, \overline{\alpha_k}$ là hệ độc lập tuyến tính trong G/pG trên trường Z/pZ mà $\dim G/pG = n$ nên $k \leq n$.

Theo lý thuyết nhóm abel ta có định lý: Nếu G là nhóm abel hữu hạn sinh thì G phân tích được thành tích hữu hạn các nhóm xiclic. Từ đó ta có nếu G là nhóm abel hữu hạn sinh, không xoắn thì G là tổng trực tiếp hữu hạn của các nhóm xiclic cấp vô hạn.

1.2.6 Mệnh đề : Cho M là một nhóm abel tự do và N là nhóm con của M . Thế thì N cũng là một nhóm abel tự do và $\text{rank}N \leq \text{rank}M$.

Chứng minh

Ta chứng minh qui nạp theo $m = \text{rank}M$

- Với $m = 0$: Hiển nhiên đúng
- Giả sử mệnh đề đúng với $m - 1$. Ta chứng minh mệnh đề đúng với m .

Nếu $N = 0$ hiển nhiên đúng. Giả sử $N \neq 0$, khi đó lấy $0 \neq \alpha \in N$, ta có $\alpha = c_1\omega_1 + \dots + c_m\omega_m$, trong đó $\{\omega_i\}_{i=1, \dots, m}$ là cơ sở của M . Ta có thể giả sử $c_1 \neq 0$. Đặt $I = \{c_1 \mid \exists \alpha \in N : \alpha = c_1\omega_1 + \dots + c_m\omega_m\}$. Ta thấy I là ideal khác 0 của vành Z . Vì Z là vành chính nên $I = \langle c_{11} \rangle$, $c_{11} \neq 0 \Rightarrow \exists \mu_1 \in N$ sao cho $\mu_1 = c_{11}\omega_1 + \dots + c_{1m}\omega_m$. Trong M ta xét $M_0 = \langle \omega_2, \dots, \omega_m \rangle$, $\text{rank}M_0 = m - 1$. Ta có $N \cap M_0$ là nhóm con của M_0 , theo giả thiết qui nạp $N \cap M_0$ có cơ sở giả sử $\mu_2, \dots, \mu_k$ với $k \leq m$. Bây giờ ta chứng minh $\mu_1, \mu_2, \dots, \mu_k$ là cơ sở của N . Thật vậy lấy $\alpha \in N$ suy ra tồn tại q_1 sao cho $\alpha - q_1\mu_1 = c'_2\omega_2 + \dots + c'_m\omega_m \in M_0$. Ta có $\alpha = q_1\mu_1 + \dots + q_k\mu_k$. Mặt khác hệ $\mu_1, \dots, \mu_k$ độc lập tuyến tính vì $c_1\mu_1 + \dots + c_k\mu_k = 0 \Rightarrow -c_1\mu_1 = c_2\mu_2 + \dots + c_k\mu_k$, ta nhận thấy vế phải của đẳng thức này thuộc M_0 . Từ đó suy ra $c_1\mu_1 \in M_0 \Rightarrow c_1\mu_1 = b_2\omega_2 + \dots + b_m\omega_m$, mặt khác ta lại có $c_1\mu_1 = c_1c_{11}\omega_1 + c_2c_{12}\omega_2 + \dots + c_mc_{1m}\omega_m \Rightarrow c_1c_{11}\omega_1 + b'_2\omega_2 + \dots + b'_m\omega_m = 0 \Rightarrow c_1c_{11} = 0 \Rightarrow c_1 = 0$ (vì $c_{11} \neq 0$) $\Rightarrow c_2 = \dots = c_k = 0$.

Vậy hệ $\{\mu_1, \dots, \mu_k\}$ là cơ sở của N . Từ đó ta có N là nhóm abel tự do và $\text{rank}N \leq \text{rank}M$.

1.3 : CHUẨN VÀ VẾT CỦA SỐ ĐẠI SỐ

1.3.1 Định nghĩa : Một số phức α thỏa mãn một phương trình đa thức $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$ với $\forall a_i \in Q$, các a_i không đồng thời bằng 0, được gọi là một số đại số.

Nếu α là một số đại số, khi đó tồn tại một đa thức khác không, đơn hệ có hệ số thuộc Q , bất khả quy trong $Q[x]$ nhận α làm nghiệm. Đa thức đó ta gọi là đa thức tối thiểu của α . kí hiệu $\text{Irr}(\alpha, Q, x)$, như vậy

$$\text{Irr}(\alpha, Q, x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0, \forall a_i \in Q.$$

1.3.2 Định nghĩa :

α là một số đại số bậc k trên Q , khi đó $[Q(\alpha) : Q] = k$. Đa thức tối thiểu của α là :

$\text{Irr}(\alpha, Q, x) = x^k + a_{k-1}x^{k-1} + \dots + a_1x + a_0$ có k nghiệm là α_i khi đó

$\text{Irr}(\alpha, Q, x) = (x - \alpha_1) \dots (x - \alpha_k)$. Ta định nghĩa

$$N_{Q(\alpha)/Q}(\alpha) = \prod_{i=1}^k \alpha_i = (-1)^k a_0$$

$$\text{Tr}_{Q(\alpha)/Q}(\alpha) = \sum_{i=1}^k \alpha_i = -a_{k-1}$$

Trường hợp tổng quát K là mở rộng hữu hạn bậc n của Q , $[K : Q] = n$, $\alpha \in K$ thì $Q(\alpha) \subset K$ ta có : $[K : Q] = [K : Q(\alpha)] [Q(\alpha) : Q]$. Ta định nghĩa

$$N_{K/Q}(\alpha) = [N_{Q(\alpha)/Q}(\alpha)]^{\frac{n}{k}} = [(-1)^k a_0]^{\frac{n}{k}}$$

$$\text{Tr}_{K/Q}(\alpha) = [\text{Tr}_{Q(\alpha)/Q}(\alpha)]^{\frac{n}{k}} = [-a_{k-1}]^{\frac{n}{k}}$$

- $N_{K/Q}(\alpha)$ được gọi là chuẩn của α và viết tắt $N(\alpha)$

- $\text{Tr}_{K/Q}(\alpha)$ được gọi là vết của α và viết tắt $\text{Tr}(\alpha)$

Chú ý rằng vì $[K : Q] = n$ nên có đúng n đơn cấu $f : K \rightarrow C$ mà $f|_Q = \text{id}$

nên ta có thể chứng minh được $N(\alpha) = \prod_{i=1}^n f_i(\alpha)$; $\text{Tr}(\alpha) = \sum_{i=1}^n f_i(\alpha)$, trong đó f_i

là các đơn cấu từ $K \rightarrow C$, $i = \overline{1, n}$

Đôi khi để cho tiện ta ký hiệu $f_i(\alpha) = \alpha^{(i)}$, khi đó $N(\alpha) = \prod_{i=1}^n \alpha^{(i)}$,

$$\text{Tr}(\alpha) = \sum_{i=1}^n \alpha^{(i)}$$

1.3.3 Các tính chất :

a / N là đồng cấu nhóm từ $(K^*, \cdot)$ vào $(Q^*, \cdot)$

b/ Tr là ánh xạ tuyến tính từ K vào Q với K và Q coi như là các không gian vectơ trên Q .

c/ Với $\alpha \in Q$ thì $N(\alpha) = \alpha^n$, $\text{Tr}(\alpha) = n \alpha$

Chứng minh :

Theo định nghĩa trên rõ ràng với $\alpha \in K$ thì $N(\alpha) \in Q$, $\text{Tr}(\alpha) \in Q$.

a/ Với $\alpha, \beta \in K^*$ ta có $N(\alpha\beta) = \prod_{i=1}^n f_i(\alpha\beta) = \prod_{i=1}^n f_i(\alpha) \cdot f_i(\beta)$

$$= \prod_{i=1}^n f_i(\alpha) \cdot \prod_{i=1}^n f_i(\beta) = N(\alpha) \cdot N(\beta).$$

b/ • Với $\alpha, \beta \in K$ ta có $\text{Tr}(\alpha + \beta) = \sum_{i=1}^n f_i(\alpha + \beta) = \sum_{i=1}^n f_i(\alpha) + \sum_{i=1}^n f_i(\beta)$

$$= \text{Tr}(\alpha) + \text{Tr}(\beta)$$

- Với $\forall a \in Q$ ta có $\text{Tr}(a\alpha) = \sum_{i=1}^n f_i(a\alpha) = \sum_{i=1}^n af_i(\alpha) = a \sum_{i=1}^n f_i(\alpha) = a\text{Tr}(\alpha)$

c/ Do $\alpha \in Q$ nên $f_i(\alpha) = \alpha$. Vậy $N(\alpha) = \prod_{i=1}^n f_i(\alpha) = \prod_{i=1}^n \alpha = \alpha^n$;

$$\text{Tr}(\alpha) = \sum_{i=1}^n (\alpha) = \sum_{i=1}^n \alpha = n\alpha.$$

1.3.4 Định nghĩa : Nếu $[K : Q] = n$ và $\omega_1, \dots, \omega_n$ là cơ sở của không gian vec tơ K trên Q . Khi đó tồn tại một cơ sở $\omega_1^*, \dots, \omega_n^*$ sao cho

$$\text{Tr}(\omega_i \omega_j^*) = \delta_{ij} = \begin{cases} 1 & \text{nếu } i = j \\ 0 & \text{nếu } i \neq j \end{cases}$$

Cơ sở $\omega_1^*, \dots, \omega_n^*$ như trên gọi là cơ sở đối ngẫu của $\omega_1, \dots, \omega_n$

1.4 IDEAL TRONG VÀNH GIAO HOÁN CÓ ĐƠN VỊ

1.4.1 Các khái niệm cơ bản :

- Cho $(X, +, \cdot)$ là một vành. Nếu phép nhân là giao hoán và có phần tử đơn vị thì ta gọi X là vành giao hoán có đơn vị.

- Cho X là một vành, A là vành con của X . A được gọi là ideal của vành X nếu $\forall a \in A, \forall x \in X$ thì $xa \in A$ và $ax \in A$. Ta ký hiệu $A \triangleleft X$.

- Cho X là vành giao hoán, có đơn vị, A là một ideal của X , $A \neq X$. A được gọi là ideal tối đại của X nếu các ideal của X chứa A chính là X và A ; A được gọi là ideal nguyên tố nếu với $u, v \in X$ mà $uv \in A$ thì $u \in A$ hoặc $v \in A$.

1.4.2 Mệnh đề :

Cho X là vành giao hoán, có đơn vị, $A \triangleleft X$. Khi đó

a) A là ideal nguyên tố $\Leftrightarrow X/A$ là một miền nguyên

b) A là ideal tối đại $\Leftrightarrow X/A$ là một trường

Chứng minh :

a) $\Rightarrow$). Do A là ideal của X nên $X/A = \{x+A | x \in X\}$ là một vành thương của vành X trên A . Vì A là nguyên tố nên $A \neq X$ do đó X/A có nhiều hơn một phần tử. Gọi e là phần tử đơn vị của X thì $e + A$ là phần tử đơn vị của X/A . Do X là vành giao hoán nên X/A cũng là vành giao hoán. Giả sử $x + A, y + A$ là hai phần tử tùy ý của X/A mà $(x+A)(y+A) = 0 \Rightarrow xy + A = 0 \Rightarrow xy \in A$ mà A nguyên tố nên $x \in A$ hoặc $y \in A$ suy ra $x + A = 0$ hoặc $y + A = 0$ hay X/A không có ước của không, do đó X/A là một miền nguyên.

$\Leftarrow$). Do X/A là một miền nguyên nên X/A có hơn một phần tử, do đó $A \neq X$.

Giả sử x, y là hai phần tử thuộc X sao cho $xy \in A \Rightarrow xy + A = 0$

$\Leftrightarrow (x + A)(y + A) = 0$. Vì X/A không có ước của không, suy ra $x + A = 0$

hoặc $y + A = 0 \Rightarrow x \in A$ hoặc $y \in A$. Vậy A ideal nguyên tố.

b) $\Rightarrow$) Do A là ideal tối đại của X nên $A \neq X$ do đó X/A có nhiều hơn một phần tử. Vì X là vành giao hoán, có đơn vị nên X/A cũng là vành giao hoán có đơn vị. Giả sử $x + A \in X/A$ mà $x \notin A$, xét ideal I của X mà $I = A + xX$. Khi đó $A \subsetneq I$ và $x \in I$. Vì A là tối đại nên $I = X \Rightarrow e \in I$. Do đó $e = a + xx'$ với $a \in A, x' \in X$ hay $e + A = (a + xx') + A = (x + A)(x' + A)$. Điều đó chứng tỏ phần tử $x + A$ khả nghịch. Do đó X/A là một trường

$\Leftarrow$) Do X/A là một trường nên X/A có nhiều hơn một phần tử do đó $A \neq X$. Giả sử I là một ideal của X sao cho $A \subsetneq I$, như vậy tồn tại phần tử $x_0 \in I$ mà $x_0 \notin A$. Ta xét $x_0 + A \in X/A$, vì $x_0 \notin A$ nên $x_0 + A$ khả nghịch nghĩa là có phần tử $x'_0 + A$ sao cho $(x_0 + A)(x'_0 + A) = x_0 x'_0 + A = e + A$ hay $x_0 x'_0 + a = e$. Vì $x_0 \in I$ và $a \in A \subset I$ nên $e \in I$ do đó $I = X$. Vậy A là ideal tối đại.

1.4.3 Các phép toán trên ideal:

Cho X là vành giao hoán, có đơn vị và gọi $\mathcal{P}$ là tập các ideal của X . Khi đó với $\forall A, B \in \mathcal{P}$ ta định nghĩa phép cộng, phép nhân trên $\mathcal{P}$ như sau :

- $A + B = \{ a+b/a \in A, b \in B \}$
- $A \cdot B = \{ \sum_{i \in I} a_i b_i / I \text{ hữu hạn}, a_i \in A, b_i \in B \}$

Nhận xét : $(\mathcal{P}, \cdot)$ là một nửa nhóm nhân giao hoán, có đơn vị $E = D$

1.5 : THẶNG DƯ BẬC HAI

1.5.1 Định nghĩa : Cho phương trình $x^2 \equiv a \pmod{p}$ ⁽¹⁾ trong đó p là một số nguyên tố lẻ và $(a, p) = 1$. Nếu phương trình (1) có nghiệm thì ta nói a là thặng dư bậc hai theo modun p , còn nếu phương trình (1) vô nghiệm thì ta nói a là bất thặng dư bậc hai theo modun p .

- Nếu a là thặng dư bậc hai theo modun p ta ký hiệu $\left(\frac{a}{p}\right) = 1$

(ký hiệu $\left(\frac{a}{p}\right)$ gọi là ký hiệu Lagrăng)

- Nếu a là bất thặng dư bậc hai theo modun p ta kí hiệu $\left(\frac{a}{p}\right) = -1$.

1.5.2 Tính chất :

$$a) \left(\frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

$$b) \text{ Nếu } a \equiv b \pmod{p} \text{ thì } \left(\frac{a}{p} \right) = \left(\frac{b}{p} \right)$$

$$c) \left(\frac{1}{p} \right) = 1 \text{ (với } p \text{ là số nguyên tố lẻ)}$$

$$d) \left(-\frac{1}{p} \right) = (-1)^{\frac{p-1}{2}}$$

$$e) \left(\frac{a_1 a_2 \dots a_k}{p} \right) = \left(\frac{a_1}{p} \right) \left(\frac{a_2}{p} \right) \dots \left(\frac{a_k}{p} \right)$$

g) Nếu p và q là hai số nguyên tố lẻ phân biệt thì ta có

$$\left(\frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q} \right)$$

1.5.3 Định nghĩa : Cho P là một số lẻ lớn hơn 1 và $P = p_1 p_2 \dots p_r$ trong đó p_i ($i = \overline{1, r}$) là các số nguyên tố có thể trùng nhau và $(a, P) = 1$ khi đó kí hiệu Giắc cô bi được xác định bởi :

$$\left(\frac{a}{P} \right) = \left(\frac{a}{p_1} \right) \left(\frac{a}{p_2} \right) \dots \left(\frac{a}{p_r} \right) \text{ trong đó } \left(\frac{a}{p_i} \right) \text{ là kí hiệu Lagrăng.}$$

1.5.4 Tính chất :

$$a) \left(\frac{1}{P} \right) = 1$$

$$b) \left(\frac{-1}{P} \right) = (-1)^{\frac{P-1}{2}}$$

$$c) \left(\frac{2}{P} \right) = (-1)^{\frac{P^2-1}{8}}$$

CHƯƠNG 2

CÁC IDEAL TRONG VÀNH CÁC SỐ NGUYÊN ĐẠI SỐ

Trong chương này ta ký hiệu D là vành các số nguyên đại số của trường mở rộng hữu hạn K của Q với $[K : Q] = n$. Mục đích của chương này là nghiên cứu tính chất của các ideal của vành D và chứng minh mọi ideal của vành D phân tích được thành tích của các ideal tối đại.

2.1 : VÀNH CÁC SỐ NGUYÊN ĐẠI SỐ CỦA TRƯỜNG MỞ RỘNG HỮU HẠN CỦA Q

2.1.1 Định nghĩa : Một số đại số gọi là số nguyên đại số nếu nó thỏa mãn trên Q một phương trình đa thức đơn hệ với hệ số nguyên. Như vậy u là số nguyên đại số $\Leftrightarrow$ đa thức tối tiểu của u là $\text{Irr}(u, Q, x) \in Z[x]$

2.1.2 Định lý : Tập hợp tất cả các số nguyên đại số là một miền nguyên

Để chứng minh định lý 2.1.2 trước hết ta chứng minh bổ đề sau

2.1.3 Bổ đề :

Số u là một số nguyên đại số khi và chỉ khi nhóm cộng sinh ra bởi tất cả các lũy thừa $1, u, u^2, \dots$ của u là nhóm abel hữu hạn sinh.

Chứng minh :

$\Rightarrow$) Do u là số nguyên đại số nên nó thỏa mãn phương trình

$p(u) = a_0 + a_1u + \dots + a_{n-1}u^{n-1} + u^n = 0^{(1)}$, Với $\forall a_i \in Z$. Phương trình (1) biểu thị u^n là một phần tử trong nhóm $G = \langle 1, u, \dots, u^{n-1} \rangle$. Bằng phép quy nạp ta chứng minh được với $\forall k \geq 1, k \in Z$ thì $u^k \in G$.

($\Leftarrow$) Giả sử nhóm G sinh ra bởi $1, u, u^2, \dots$ có thể được sinh ra bởi n số bất kỳ $v_1, v_2, \dots, v_n$ của G , khi đó $\forall v_j \in G$ ta có $v_j = \sum_i a_j u^i \in G$

$\Rightarrow uv_j = \sum a_j u^{j+1} \in G \Rightarrow \forall u, v_i \in G \text{ và } u \cdot v_i = \sum a_{ij} v_j \ (\forall a_{ij} \in Z)$. Từ đó ta có hệ phương trình tuyến tính thuần nhất:

[illegible]

Vì hệ (I) có nghiệm $(v_1, \dots, v_n)$ với v_i không bằng 0 tất cả nên ma trận các hệ số $A - uI$ suy biến (với $A = [a_{ij}]_{n \times n}$) $\Rightarrow |A - uI| = 0$

$\Leftrightarrow (-1)^n u^n + b_{n-1} u^{n-1} + \dots + b_1 u + b_0 = 0$ ⁽²⁾ (trong đó b_i là những đa thức nào đó của các số nguyên a_{ij} nên b_i cũng là số nguyên). Từ phương trình (2) ta có u là một số nguyên đại số.

Bây giờ ta chứng minh định lý 2.1.2 :

Giả sử u và v là các số nguyên đại số $\Rightarrow u^k$ và v^k đều có thể biểu thị theo một số hữu hạn các lũy thừa $1, u, \dots, u^{n-1}$ và $1, v, \dots, v^{r-1}$

$\mathbf{V}^k(\mathbf{u}, \mathbf{v})^k = \mathbf{u}^k \mathbf{v}^k \in \langle \mathbf{1}, \mathbf{u}, \mathbf{v}, \dots, \mathbf{u}^k \mathbf{v}^t, \dots, \mathbf{u}^{n-1} \mathbf{v}^{r-1} \rangle$. Mặt khác

$$(u + v)^k = \sum C_n^k u^i v^{k-i} \in \langle 1, u, v, \dots, u^{n-1} v^{r-1} \rangle \text{ mà } G = \langle u^i v^j \rangle, 0 \leq i \leq n-1;$$

$0 \leq j \leq r - 1$ là một nhóm hữu hạn sinh nên theo bổ đề 2.1.3 ta suy ra $u + v$ và $u \cdot v$ là các số nguyên đại số.

2.2 : MỘT SỐ TÍNH CHẤT CỦA VÀNH D

2.2.1 Mệnh đề : Nếu $\alpha \in K$ thì tồn tại $c \in Z$ sao cho $c\alpha \in D$

Chứng minh :

Do $\alpha \in K$ nên tồn tại đa thức $f(x) = a_k x^k + \dots + a_1 x + a_0$ với các hệ số nguyên nhận α làm nghiệm tức là $a_k \alpha^k + \dots + a_1 \alpha + a_0 = 0$ ⁽¹⁾. Nhân hai vế của (1) với a_k^{k-1} ta có :

$$a_k^k \alpha^k + a_k^{k-1} \cdot a_{k-1} \alpha^{k-1} + \dots + a_k^{k-1} a_1 \alpha + a_k^{k-1} a_0 = 0$$

$$\Leftrightarrow (a_k \alpha)^k + a_{k-1} (a_k \alpha)^{k-1} + \dots + a_k^{k-2} a_1 (a_k \alpha) + a_k^{k-1} a_0 = 0$$

Đặt $c = a_k$ ta có $c\alpha \in D$

2.2.2 Mệnh đề :

Nếu hệ $\{\alpha_1, \dots, \alpha_n\} \subset D$ là hệ độc lập tuyến tính trong $(K, +)$ thì $\{\alpha_1, \dots, \alpha_n\}$ cũng là hệ độc lập tuyến tính trong $(D, +)$

Chứng minh

Giả sử hệ $\{\alpha_i\}_{i=1, n}$ phụ thuộc tuyến tính trong $(D, +)$ nên $\exists a_i \in Z$ $a_i \neq 0$ để

$$\sum_{i=1}^n a_i \alpha_i = 0, \text{ không mất tính chất tổng quát ta giả sử } a_1 \neq 0 \text{ để}$$

$$a_1 \alpha_1 + a_2 \alpha_2 + \dots + a_n \alpha_n = 0$$

$$\Rightarrow \alpha_1 + b_2 \alpha_2 + \dots + b_n \alpha_n = 0, b_i \in Q$$

$$\Rightarrow \alpha_1, \dots, \alpha_n \text{ phụ thuộc tuyến tính trong } (K, +) \text{ (mâu thuẫn gt).}$$

Vậy $\alpha_1, \dots, \alpha_n$ độc lập tuyến tính trong $(D, +)$

2.2.3 Mệnh đề : D là một nhóm abel tự do có cơ sở hữu hạn và

$$\text{rank } D = [K : Q] = n$$

Chứng minh

Do $[K : Q] = n$ nên một cơ sở của không gian vector K trên Q sẽ gồm n vector. Giả sử $\alpha_1, \alpha_2, \dots, \alpha_n$ là một cơ sở của K trên Q . Theo mệnh đề 2.2.1 ta có thể nhân vào cơ sở đó các số nguyên $c_1, \dots, c_n$ để cho các tích $c_1 \alpha_1, \dots, c_n \alpha_n$ thuộc D . Ta dễ thấy hệ sau khi nhân cũng độc lập tuyến tính.

Do đó không mất tính chất tổng quát, ta có thể xem $\alpha_1, \alpha_2, \dots, \alpha_n \in D$. Từ đó ta có $\alpha_1, \dots, \alpha_n$ cũng độc lập tuyến tính trong D . Giả sử $\alpha_1^*, \dots, \alpha_n^*$ là cơ sở đối ngẫu của $\alpha_1, \dots, \alpha_n$.

Giả sử M là nhóm con của $(K, +)$ sinh bởi $\alpha_1^*, \dots, \alpha_n^*$ và

$M = \langle \alpha_1^*, \dots, \alpha_n^* \rangle$. Ta suy ra M là nhóm abel tự do và $\text{rank } M = n$. Ta chứng minh $D \subset M$. Thật vậy với $\forall \alpha \in D$ thì $\alpha = a_1\alpha_1^* + \dots + a_n\alpha_n^*$

$$(a_i \in Q, i = \overline{1, n}). \text{ Ta có } \text{Tr}(\alpha\alpha_i) = \text{Tr}\left(\sum_{k=1}^n a_k \alpha_k^* \alpha_i\right) = \sum_{k=1}^n a_k \text{Tr}(\alpha_k^* \alpha_i) \\ = \sum_{k=1}^n a_k \delta_{ki} = a_i \text{ mà } \alpha\alpha_i \in D \text{ nên } a_i = \text{Tr}(\alpha\alpha_i) \in Z \Rightarrow \alpha \in M \Rightarrow D \subset M, \text{ theo}$$

định lý 1.2.6 thì D là nhóm abel tự do và $\text{rank } D \leq \text{rank } M = n$ (1). Mặt khác do $\alpha_1, \dots, \alpha_n$ độc lập tuyến tính trong D nên ta có $\text{rank } D \geq n$ (2). Từ (1) và (2) ta có $\text{rank } D = n$.

2.2.4 Mệnh đề : Cho $A \triangle D$ thì A là nhóm Aben tự do và $\text{rank } A = \text{rank } D = n$

Chứng minh

Do $A \subset D$ áp dụng mệnh đề 2.2.3 ta có A là nhóm abel tự do và $\text{rank } A \leq n$. Giả sử $\alpha_1, \alpha_2, \dots, \alpha_n$ là một cơ sở của D . Lấy $\alpha \in D, \alpha \neq 0$, khi đó $\alpha\alpha_1, \alpha\alpha_2, \dots, \alpha\alpha_n$ độc lập tuyến tính trên Z . Thật vậy, giả sử $a_1(\alpha\alpha_1) + \dots + a_n(\alpha\alpha_n) = 0 \Rightarrow a_1\alpha_1 + \dots + a_n\alpha_n = 0$. Từ đó suy ra $a_1 = a_2 = \dots = a_n = 0$. Mặt khác do A là ideal của D nên n phần tử độc lập tuyến tính $\alpha\alpha_1, \dots, \alpha\alpha_n \in A$, nên $\text{rank } A \geq n$. Do đó $\text{rank } A = n$

2.2.5 Mệnh đề : Nếu $a \in Z^*$ thì $|D / \langle a \rangle| = |a|^n$

Nếu A là ideal khác 0 của D thì $|D/A|$ hữu hạn.

Chứng minh

Giả sử $\alpha_1, \alpha_2, \dots, \alpha_n$ là cơ sở của D . Đầu tiên ta nhận xét rằng $\alpha = a_1\omega_1 + \dots + a_n\omega_n : a$ trong $D \Leftrightarrow a_i : a$ trong $Z; \forall i = \overline{1, n}$. Thật vậy.

$$\alpha : a \Leftrightarrow \frac{\alpha}{a} \in D \Leftrightarrow \frac{a_1}{a}\omega_1 + \dots + \frac{a_n}{a}\omega_n \in D \Leftrightarrow a_i : a \text{ trong } Z \text{ với } \forall i = \overline{1, n}$$

Bây giờ ta đặt $S = \{a_1\omega_1 + \dots + a_n\omega_n / 0 \leq a_i \leq |a| \}$ thì $|S| = |a|^n$. Ta chứng minh S là hệ đại diện đầy đủ của các lớp tương đương trong vành $D/\langle a \rangle$. Thật vậy, lấy $\alpha = \sum_{i=1}^n a_i\omega_i \in S; \beta = \sum_{i=1}^n b_i\omega_i \in S$ khi đó nếu $\bar{\alpha} = \bar{\beta}$ thì

$$\alpha - \beta : a, \Leftrightarrow a_i - b_i : a, \forall i = \overline{1, n}$$

Mặt khác do $0 \leq a_i, b_i \leq |a|$ nên ta phải có $a_i = b_i, \forall i = \overline{1, n}$

Từ đó $\alpha = \beta$. Với mọi $x = \sum_{i=1}^n x_i\omega_i$, giả sử $x_i = aq_i + r_i$

trong đó $0 \leq r_i \leq |a|, \forall i = \overline{1, n}$. Đặt $r = \sum_{i=1}^n r_i\omega_i$ thì ta có $r \in S$ và $\bar{x} = \bar{r}$

Vậy $|D/\langle a \rangle| = |S| = |a|^n$.

Với $a \in A \Rightarrow \langle a \rangle \subset A \Rightarrow |D/A| \leq |D/\langle a \rangle| = |a|^n$. Vậy $|D/A|$ hữu hạn.

2.2.6 Mệnh đề : Cho A là ideal của D . Số ideal B thỏa $A \subset B \subset D$ là hữu hạn.

Chứng minh

Ta có B/A là vành con của D/A , theo mệnh đề 2.2.4 vành thương D/A là hữu hạn nên số vành con B/A là hữu hạn. Từ đó số ideal B thỏa $A \subset B \subset D$ là hữu hạn (vì $B/A = B'/A \Leftrightarrow B = B'$)

Do hệ (1) có nghiệm khác 0 nên $|B - \alpha E| = 0$ với $B = (a_{ij})_{n \times n}$. Từ đó đặt $f(x) = |xE - B|$ thì $f(x) = x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$ và $f(x)$ nhận α làm nghiệm còn các hệ số $a_i \in A, \forall i = \overline{1, n}$.

2.3.2 Bổ đề :

Cho A là ideal của D , tồn tại số tự nhiên $T = T(A)$ phụ thuộc chỉ vào A sao cho $\forall \alpha \in K$ tìm được $\beta \in A$ và số tự nhiên $s < T$ sao cho

$$|N(s\alpha - \beta)| < 1$$

Chứng minh

Theo mệnh đề 2.2.4, $\text{rank } A = [K : Q] = n$. Giả sử $\alpha_1, \alpha_2, \dots, \alpha_n$ là một cơ sở của A . Thế thì $\alpha_1, \alpha_2, \dots, \alpha_n$ cũng là cơ sở của K trên Q . Thật vậy $\alpha_1, \alpha_2, \dots, \alpha_n$ độc lập tuyến tính vì :

$q_1 \alpha_1 + \dots + q_n \alpha_n = 0$ ($q_i \in Q$). Gọi c là BSCNN của các mẫu số của $q_1, \dots, q_n$ thì $cq_1, \dots, cq_n \in Z$

$\Rightarrow (cq_1) \alpha_1 + \dots + (cq_n) \alpha_n = 0$ (1). Mặt khác $\alpha_1, \dots, \alpha_n$ là cơ sở của A nên từ (1) ta có $cq_1 = cq_2 = \dots = cq_n = 0$ suy ra $q_1 = q_2 = \dots = q_n = 0$.

mà $[K : Q] = n$ nên $\alpha_1, \dots, \alpha_n$ là cơ sở của K trên Q . Lấy $\alpha \in K$ bất kỳ, với mỗi $k \in N$ thì $k\alpha = q_1 \alpha_1 + \dots + q_n \alpha_n$.

Đặt $\beta_k = [q_1] \alpha_1 + \dots + [q_n] \alpha_n$ thì $\beta_k \in A$ và $k\alpha - \beta_k = y_1^k \alpha_1 + \dots + y_n^k \alpha_n$ trong đó $0 \leq y_i^k = q_i - [q_i] < 1 \forall i = \overline{1, n}$

Chia đoạn $[0; 1]$ thành M khoảng bằng nhau $\left[\frac{j}{M}, \frac{j+1}{M} \right]$

Với $j = 0, 1, \dots, M-1$ thì $[0; 1]^n$ sẽ được phân hoạch thành M^n hình hộp.

Có $M^n + 1$ bộ số $(y_1^k, \dots, y_n^k) \in [0; 1]^n$ với $k = 0, 1, \dots, M^n$. Do đó theo nguyên tắc Dirichle sẽ có hai bộ cùng rơi vào một hình hộp và giả sử đó là $(y_1^i, \dots, y_n^i)$ và $(y_1^j, \dots, y_n^j)$ với $i > j$

$$\text{thế thì } (i\alpha - \beta_i) - (j\alpha - \beta_j) = (y_n^i - y_n^j)\alpha_1 + \dots + (y_n^i - y_n^j)\alpha_n$$

$$s\alpha - \beta = y_1\alpha_1 + \dots + y_n\alpha_n$$

$$\text{với } 0 < s = i - j < M^n + 1 ; \beta = \beta_i - \beta_j \in A; y_m = y_m^i - y_m^j$$

$$\text{nên } |y_m| < \frac{1}{M} \text{ với } m = \overline{1, n}$$

$$\text{suy ra } (s\alpha - \beta)^{(i)} = (y_1\alpha_1 + \dots + y_n\alpha_n)^{(i)} = y_1\alpha_1^{(i)} + \dots + y_n\alpha_n^{(i)}$$

$$|(s\alpha - \beta)^{(i)}| = |y_1\alpha_1^{(i)} + \dots + y_n\alpha_n^{(i)}| \leq |y_1| |\alpha_1^{(i)}| + \dots + |y_n| |\alpha_n^{(i)}|$$

$$\leq \frac{1}{M} (|\alpha_1^{(i)}| + \dots + |\alpha_n^{(i)}|)$$

$$|N(s\alpha - \beta)| \leq \frac{1}{M^n} \text{ const. Chọn } M \text{ đủ lớn để } \frac{\text{const}}{M^n} < 1.$$

Khi đó với $T = T(A) = M^n + 1$ thì $s < T$.

2.3.3 Định nghĩa :

Trên tập các ideal của D ta định nghĩa quan hệ $\sim$ như sau :

$$A \sim B \Leftrightarrow \exists \alpha, \beta \in D \text{ sao cho } \langle \alpha \rangle A = \langle \beta \rangle B.$$

2.3.4 Mệnh đề : Quan hệ $\sim$ là quan hệ tương đương và số các lớp tương đương $D/\sim$ là hữu hạn.

Chứng minh

♦ $\sim$ là một quan hệ tương đương

- Phản xạ : Hiển nhiên
- Đối xứng : Hiển nhiên
- bắc cầu : Do $A \sim B \Leftrightarrow \exists \alpha, \beta_1 \in D \text{ sao cho } \langle \alpha \rangle A = \langle \beta_1 \rangle B$

$$B \sim C \Leftrightarrow \exists \beta_2, \gamma \in D \text{ sao cho } \langle \beta_2 \rangle B = \langle \gamma \rangle C$$

$$\text{Từ đó } \langle \beta_2 \rangle \langle \alpha \rangle A = \langle \beta_2 \rangle \langle \beta_1 \rangle B \text{ hay } \langle \beta_2 \alpha \rangle A = \langle \beta_1 \beta_2 \rangle B$$

$$\langle \beta_1 \rangle \langle \beta_2 \rangle B = \langle \beta_1 \rangle \langle \gamma \rangle C \text{ hay } \langle \beta_1 \beta_2 \rangle B = \langle \beta_1 \gamma \rangle C$$

$$\text{Suy ra } \langle \beta_2 \alpha \rangle A = \langle \beta_1 \gamma \rangle C \text{ hay } A \sim C$$

♦ $|D/\sim|$ là hữu hạn

A là ideal tùy ý với $\alpha \in A$ thì $N(\alpha) \in \mathbb{Z}$ nên sẽ tồn tại một $\alpha_0 \in A$ để $N(\alpha_0)$

là nguyên dương bé nhất. Với mỗi $a \in A$ đặt $\alpha = \frac{a}{\alpha_0} \in K$, vì D là một ideal

theo bổ đề 2.3.2 sẽ tồn tại $T = T(D)$ và $\beta \in D$ sao cho tồn tại $s < T$ để $|N(s\alpha - \beta)| < 1$. Từ đó $|N[(s\alpha - \beta)\alpha_0]| < N(\alpha_0)$ (1).

Mặt khác $(s\alpha - \beta)\alpha_0 = s\alpha\alpha_0 - \beta\alpha_0 = sa - \beta\alpha_0 \in A$ nên từ (1) ta có

$$N[(s\alpha - \beta)\alpha_0] = 0 \text{ hay } (s\alpha - \beta)\alpha_0 = 0 \text{ hay } \beta = s\alpha$$

$$\text{Suy ra } s\frac{a}{\alpha_0} = \beta \in D$$

Vậy α_0/sa do đó α_0/Na với $N = T$!

Bây giờ ta đặt $B = \{\beta \in D / \exists a \in A : \alpha_0\beta = Na\}$

- Rõ ràng B là một ideal của D

- Ta chứng minh $\langle \alpha_0 \rangle B = \langle N \rangle A$. Thật vậy lấy $\alpha_0\beta \in \langle \alpha_0 \rangle B$, thế thì

$\exists a \in A$ để $\alpha_0\beta = Na \in \langle N \rangle A$ suy ra $\langle \alpha_0 \rangle B \subset \langle N \rangle A$. Lấy $Na \in \langle N \rangle A$ thì $\alpha_0|Na$ nên $\exists \beta \in B$ sao cho $Na = \alpha_0\beta \in \langle \alpha_0 \rangle B$ suy ra $\langle N \rangle A \subset \langle \alpha_0 \rangle B$.

Vậy $\langle \alpha_0 \rangle B = \langle N \rangle A$ suy ra $A \sim B$.

- Tiếp theo ta lại có với bất kỳ $N\omega \in \langle N \rangle$ do $\alpha_0 \in A$ nên

$N\omega\alpha_0 \in \langle N \rangle A = \langle \alpha_0 \rangle B$ suy ra $\exists \beta \in B$ để $N\omega\alpha_0 = \alpha_0\beta$ hay $N\omega = \beta \in B$ từ đó $\langle N \rangle \subset B$.

Như vậy với bất kỳ $A \triangle D$ sẽ tồn tại $B \triangle D$ mà $B \sim A$, $\langle N \rangle \subset B \subset D$. Mà số ideal thỏa mãn chứa $\langle N \rangle$ theo mệnh đề 2.2.6 chỉ là hữu hạn. Vì thế $D/\sim$ cũng chỉ có hữu hạn lớp tương đương.

2.3.5 Định lý : Tập $\mathcal{P} \neq \{0\}$ các ideal của vành D làm thành một nửa nhóm với sự phân tích duy nhất thành tích các phần tử nguyên tố. Phần tử nguyên tố chính là các ideal tối đại.

Để chứng minh định lý 2.3.5, ta cần một số bổ đề sau.

2.3.6 Bổ đề : Cho A, B là các ideal của D nếu $AB = A$ thì

$$B = \langle 1 \rangle = D.$$

Chứng minh

Giả sử $\alpha_1, \dots, \alpha_n$ là một cơ sở của A . Ta chứng minh rằng :

$$AB = \{b_1\alpha_1 + \dots + b_n\alpha_n / b_i \in B, i = \overline{1, n} \}.$$

Thật vậy đặt $C = \{b_1\alpha_1 + \dots + b_n\alpha_n / b_i \in B, i = \overline{1, n}\}$

- Dễ thấy $C \subset AB$
- Với $\alpha \in AB$ thì $\alpha = \sum_{i \in I} a_i b_i$ trong đó I hữu hạn, $a_i \in A$, $b_i \in B$. Biểu

điễn các a_i qua $\alpha_1, \dots, \alpha_n$ rồi sau đó nhóm các hạng tử chứa $\alpha_1, \dots, \alpha_n$ lại với nhau thì $\alpha = b_1\alpha_1 + \dots + b_n\alpha_n$ trong đó $b_k \in B, k = \overline{1, n}$, suy ra $\alpha \in C$ hay $AB \subset C$.

Từ đó $AB = C$. Do vậy.

[illegible]

Áp dụng bổ đề 2.3.1 thì 1 là nghiệm của đa thức

$$f(x) = x^n + b_1x^{n-1} + \dots + b_{n-1}x + b_n \text{ với các hệ số nằm trong } B,$$

suỵ ra $1 + b_1 + \dots + b_n = 0$ hay $1 \in B$ và $B = \langle 1 \rangle = D$

2.3.7 Bổ đề : Cho A là ideal của D tồn tại $k \in \mathbb{N}^*$ sao cho $A^k = \langle p \rangle$,

$$\rho \in A$$

Chứng minh

Do mệnh đề 2.3.4 chỉ có hữu hạn lớp tương đương $D/\sim$ nên tồn tại

$k, l \in \mathbb{N}^*$ sao cho :

2.3.8 Bổ đề : Cho A, B, C là các ideal của D , $AB = AC$ suy ra $B = C$.

Chứng minh

Theo mệnh đề 2.3.7 tồn tại $k \in \mathbb{N}^*$ để $A^k = \langle \rho \rangle$ với $\rho \in A$

$AB = AC$ suy ra $A^{k-1}(AB) = A^{k-1}(AC)$ hay $A^k B = A^k C$

Suy ra $\langle \rho \rangle B = \langle \rho \rangle C$. Từ đó $B = C$

2.3.9 Bổ đề :

Cho A, B là các ideal của D . Nếu $B \subset A$ thì $B = A.C$ trong đó C là ideal của D .

Chứng minh

- Trước hết ta xét A là ideal chính, $A = \langle \alpha \rangle$

gọi $\alpha_1, \dots, \alpha_n$ là cơ sở của B thì do $B \subset \langle \alpha \rangle$ nên $\alpha_1, \dots, \alpha_n : \alpha$ suy ra

$$\frac{\alpha_1}{\alpha}, \frac{\alpha_2}{\alpha}, \dots, \frac{\alpha_n}{\alpha} \in D$$

Đặt $C = \langle \frac{\alpha_1}{\alpha}, \dots, \frac{\alpha_n}{\alpha} \rangle$ thì rõ ràng $\langle \alpha \rangle C = B$ hay $AC = B$.

- Giả sử $B \subset A$ theo mệnh đề 2.3.7 tồn tại $k \in \mathbb{N}^*$ sao cho $A^k = \langle \alpha \rangle$.

$B \subset A$ suy ra $BA^{k-1} \subset A^k = \langle \alpha \rangle$. Từ đó theo chứng minh ở trên thì $BA^{k-1} = \langle \alpha \rangle C$ hay $BA^{k-1} = A^k C$

hay $BA^{k-1} = (AC)A^{k-1}$. Do mệnh đề 2.3.8 thì $B = AC$.

2.3.10 Bổ đề

P là ideal tối đại $\Leftrightarrow P$ là phần tử nguyên tố trong P

Chứng minh :

$\Rightarrow$) Giả sử A là ước của $P \Rightarrow P = A.B \Rightarrow P \subset A \Rightarrow A = P$ hoặc $A = D$ (vì P là ideal tối đại trong D). Vậy P là phần tử nguyên tố trong P

$\Leftarrow$) Giả sử $P \subset A \subset D$, theo bổ đề 2.3.9 ta có $P = A.B$, do P là nguyên tố nên $A = P$ hoặc $A = D$. Vậy A là ideal tối đại.

Bây giờ ta sử dụng các bổ đề trên để chứng minh định lý 2.3.5

- Giả sử A là ideal của D . Nếu A là ideal tối đại thì A có sự phân tích $A = A$. Ngược lại nếu A không tối đại thì tồn tại P_1 tối đại và $A \subseteq P_1$ suy ra $P_1|A$ hay $A = P_1A_1$. Tiếp tục, nếu A_1 tối đại thì A có sự phân tích $A = P_1A_1$. Ngược lại nếu không tối đại thì $A_1 = P_2A_2$ trong đó P_2 tối đại và $A = P_1P_2A_2$. Ta cứ tiếp tục quá trình như vậy, theo mệnh đề 2.2.6 thì chỉ có hữu hạn ideal chứa A nên quá trình này phải chấm dứt sau hữu hạn bước. Khi đó A có sự phân tích thành tích các ideal tối đại $A = P_1P_2 \dots P_n$ (*)

- Chứng minh sự phân tích ở (*) là duy nhất :

Trước hết ta chứng minh nếu P là ideal tối đại và $AB : P$ thì $A : P$ hoặc $B : P$. Thật vậy nếu $A : P$ thì điều cần chứng minh hiển nhiên là đúng. Giả sử $A : P$ thì $A \not\subset P$. Do đó $\exists a \in A$ mà $a \notin P$. Do $AB : P$ nên $AB \subset P$. Rõ ràng $\forall b \in B$ thì $ab \in AB \subset P$. Do P là tối đại nên P cũng là ideal nguyên tố. Mà $a \notin P$ nên $b \in P$, vì thế $B \subset P$ hay $B : P$.

Bây giờ giả sử A có sự phân tích khác $A = Q_1Q_2 \dots Q_k$ khi đó $P_1|Q_1 \dots Q_k$ nên theo chứng minh trên P_1 là ước của một trong các Q_i , ta có thể xem P_1 là ước của Q_1 , do Q_1 là nguyên tố nên $P_1 = Q_1$. Cứ tiếp tục như vậy và bằng quy nạp ta chứng minh được $n = k$ và $P_i = Q_i$ ($i = \overline{1, n}$).

Như vậy mọi ideal A của vành D đều phân tích một cách duy nhất thành tích của các ideal tối đại và định lý 2.3.5 được chứng minh.

CHƯƠNG 3

SỐ HỌC TRONG VÀNH CÁC SỐ NGUYÊN ĐẠI SỐ CỦA TRƯỜNG MỞ RỘNG HỮU HẠN CỦA $\mathbb{Q}$

Vành D các số nguyên đại số của trường mở rộng hữu hạn K của $\mathbb{Q}$ nói chung không phải là vành Gauss (xem ví dụ 4.1.1), hay nói cách khác trong vành D , định lý cơ bản của số học nói chung không còn đúng nữa, một số có thể phân tích được thành tích của các phần tử nguyên tố theo nhiều cách khác nhau (xem ví dụ 4.1.1), cho nên số học trong đó rất khó nghiên cứu. Mặt khác theo chương 2, mỗi ideal đều phân tích được duy nhất thành tích các ideal tối đại. Trong phần này dựa vào sự phân tích đó chúng tôi xây dựng số học trên vành các số nguyên đại số

3.1 CÁC KHÁI NIỆM CƠ BẢN

3.1.1 Định nghĩa :

Cho $a \in D$ và ideal $A \triangleleft D$. Ta nói a chia hết cho A , ký hiệu $a:A$, nếu $\langle a \rangle : A$ trong nửa nhóm $\mathbf{P}$

Từ bổ đề 2.3.9 ta có : $\langle a \rangle : A \iff \langle a \rangle \subset A \iff a \in A$.

Từ định nghĩa trên ta có : với $a, b \in D$ thì $a:b$ trong $D \iff a = b.c$,
 $c \in D \iff \langle a \rangle = \langle b \rangle \langle c \rangle \iff \langle a \rangle : \langle b \rangle$ trong $\mathbf{P}$

Nhận xét : Giả sử $a \in D$ và $\langle a \rangle = P_1^{k_1} \dots P_n^{k_n}$, P_i là các ideal tối đại, khi đó ta cũng có thể viết a được phân tích dưới dạng $a = P_1^{k_1} \dots P_n^{k_n}$

3.1.2 Định nghĩa :

Cho A là ideal của D và $a, b \in D$. Ta nói $a \equiv b \pmod{A}$ nếu $a - b \in A$ tức là $a - b \in A$

3.2 HÀM CHUẨN N – CÁC TÍNH CHẤT CỦA HÀM CHUẨN

3.2.1 Định nghĩa : Hàm $N : \mathbf{P} \rightarrow \mathbf{N}^*$

$$A \rightarrow N(A) = |D/A|$$

được gọi là hàm chuẩn. Số $N(A) = |D/A|$ được gọi là chuẩn của ideal A

Chú ý rằng: Định nghĩa này hợp lý vì với $\forall A \in \mathbf{P}$, $|D/A|$ hữu hạn

3.2.2 Định nghĩa : Cho $A \triangle D$, tập con $S_A = \{s/s \in D\}$ gọi là hệ thặng dư đầy đủ theo modun A nếu nó thỏa mãn các điều kiện sau :

$$+ \forall a \in D, \exists s \in S_A \text{ sao cho } s \equiv a \pmod{A}$$

$$+ s, s' \in S_A \text{ và } s \neq s' \text{ suy ra } s \not\equiv s' \pmod{A}$$

Nếu với mỗi lớp $\bar{a} \in D/A$ ta lấy ra một và chỉ một phần tử đại diện thì

ta được S_A là một hệ thặng dư đầy đủ theo modun A . Từ đó $N(A) = |S_A|$

3.2.3 Mệnh đề :

$$\forall A, B, \in \mathbf{P} \text{ tồn tại } \gamma \in D^* \text{ sao cho } \langle \gamma \rangle = AC \text{ với } (C, B) = E$$

Chứng minh :

$$\text{Giả sử } B = P_1^{k_1} \dots P_n^{k_n} \text{ (} P_i \text{ nguyên tố, } k_i > 1, i = \overline{1, n} \text{)}$$

Đặt $B_i = AP_1P_2 \dots P_{i-1}P_{i+1} \dots P_n$. Thế thì tồn tại $\gamma_i \in D^*$ sao cho $\langle \gamma_i \rangle \vdots B_i$,

$\langle \gamma_i \rangle \vdots B_iP_i$. Từ đó $\langle \gamma_i \rangle \vdots A \forall i = \overline{1, n}$ và $\langle \gamma_i \rangle \vdots AP_j \text{ (} i \neq j \text{)}$ và $\langle \gamma_i \rangle \vdots AP_i$

xét $\gamma = \gamma_1 + \dots + \gamma_n$ thì $\langle \gamma \rangle \vdots A$ và $\langle \gamma \rangle \vdots AP_i, i = \overline{1, n}$

Suy ra $\langle \gamma \rangle = AC$ với $(C, B) = E$

3.2.4 Mệnh đề :

Hàm chuẩn có tính chất nhân, tức là $N(AB) = N(A) \cdot N(B)$

Chứng minh

Do $A, B \triangle D$ nên theo mệnh đề 3.2.3 tồn tại $\gamma \in D^*$ sao cho $\langle \gamma \rangle = AC$ trong đó $(C, B) = E$.

Giả sử $N(A) = r$, $N(B) = s$ và $S_A = \{\alpha_1, \dots, \alpha_r\}$

$S_B = \{\beta_1, \dots, \beta_s\}$ lần lượt là hệ thặng dư đầy đủ theo modun A, B . Ta sẽ chứng minh $\{\alpha_i + \gamma \beta_j / 1 \leq i \leq r; 1 \leq j \leq s\}$ là hệ thặng dư đầy đủ theo modun $A.B$.

- Với $\alpha \in D$ thì $\alpha \equiv \alpha_i \pmod{A}$ với $1 \leq i \leq r$ nào đó. Từ đó suy ra $\alpha - \alpha_i \in A$. Mặt khác do $(\langle \gamma \rangle, AB) = (AC, AB) = A$ nên $A = \langle \gamma \rangle + AB$. Vì thế cho nên $\alpha - \alpha_i = \gamma \beta + \delta$ với $\delta \in AB$, điều này dẫn tới $\alpha - \alpha_i = \gamma \beta \pmod{AB}$.

Ta lại có do S_B là hệ thặng dư đầy đủ của mod B nên sẽ tồn tại $1 \leq j \leq s$ để $\beta \equiv \beta_j \pmod{B}$. Thành thử $\gamma \beta \equiv \gamma \beta_j \pmod{AB}$ vì $\langle \gamma \rangle \vdots A$.

Suy ra $\alpha - \alpha_i \equiv \gamma \beta_j \pmod{AB}$ hay $\alpha \equiv \alpha_i + \gamma \beta_j \pmod{AB}$.

- Giả sử $\alpha_i + \gamma \beta_j \equiv \alpha_k + \gamma \beta_l \pmod{AB}$ suy ra

$$\alpha - \alpha_k + \gamma (\beta_j - \beta_l) \equiv 0 \pmod{AB} \quad (1)$$

Mặt khác $\langle \gamma \rangle \vdots A$ nên từ (1) suy ra $\alpha_i \equiv \alpha_k \pmod{A}$ có nghĩa là $\alpha_i = \alpha_k$ từ đó (1) viết lại như sau : $\gamma (\beta_j - \beta_l) \equiv 0 \pmod{AB}$ hay $\langle \gamma (\beta_j - \beta_l) \rangle \vdots AB$
 $\Rightarrow \langle \gamma \rangle \langle \beta_j - \beta_l \rangle \vdots AB \Rightarrow AC \langle \beta_j - \beta_l \rangle \vdots AB$
 $\Rightarrow C \langle \beta_j - \beta_l \rangle \vdots B$ mà $(C, B) = E$ nên $\langle \beta_j - \beta_l \rangle \vdots B$
 $\Rightarrow \beta_j \equiv \beta_l \pmod{B} \Rightarrow \beta_j = \beta_l$ Như vậy $S_{AB} = \{\alpha_i + \gamma \beta_j / 1 \leq i \leq r; 1 \leq j \leq s\}$ là hệ thặng dư đầy đủ theo mod $AB \Rightarrow N(AB) = |S_{AB}| = r \cdot s = N(A) \cdot N(B)$

3.3 HÀM EULER – CÁC TÍNH CHẤT CỦA HÀM EULER

3.3.1 Định nghĩa :

Cho $A \triangle D$ ta nói rằng $(\bar{x}, A) = E$ nếu $(x, A) = E$.

Định nghĩa trên là hoàn toàn hợp lý. Thật vậy nếu $x' \in \bar{x}$

$$\Rightarrow x' - x \in A \Rightarrow (x', A) = (x, A) = E$$

3.3.2 Định nghĩa :

Cho $A \triangle D$, ta định nghĩa $(D/A)^* = \{\bar{x} \in D/A / \bar{x} \text{ khả nghịch} \}$

3.3.3 Mệnh đề :

Cho $A \triangle D$, $(\bar{x}, A) = E \Leftrightarrow \bar{x}$ khả nghịch

Chứng minh

$\Rightarrow$) : $(\bar{x}, A) = E$ ta suy ra $(x, A) = E$. Điều này có nghĩa là

$\langle x \rangle + A = D$. Từ đó $\exists x' \in D, a \in A$ để cho $x.x' + a = 1 \Rightarrow \bar{x}.\bar{x}' = \bar{1}$ hay $\bar{x}$ khả nghịch.

$\Leftarrow$) : $\bar{x}$ khả nghịch suy ra $\exists \bar{x}'$ sao cho $\bar{x}.\bar{x}' = \bar{1}$

Hay $x.x' - 1 \in A$. Từ đó $1 \in \langle x \rangle + A$ có nghĩa là $\langle x \rangle + A = D$ hay

$(x, A) = E$. Vậy $(D/A)^* = \{\bar{x}/\bar{x} \text{ khả nghịch} \} = \{\bar{x} / (x, A) = E\}$.

3.3.4 Định nghĩa :

Hàm $\varphi : \mathbf{P} \rightarrow \mathbf{N}^*$

$A \mapsto \varphi(A) = |(D/A)^*|$ được gọi là hàm Euler

3.3.5 Định nghĩa :

Cho A là ideal của D . tập con T_A được gọi là hệ thặng dư thu gọn theo mod A nếu thỏa mãn :

- $(s, A) = E \forall s \in T_A$
- $s, s' \in T_A$ và $s \neq s'$ thì $s \equiv s' \pmod{A}$

- $\forall a \in D$ mà $(a, A) = E$ thì $\exists s \in T_A$ sao cho $s \equiv a \pmod{A}$

Nếu với mỗi lớp $\bar{a} \in (D/A)^*$ ta lấy một và chỉ một phần tử đại diện thì ta được tập T_A là hệ thặng dư thu gọn theo mod A . Từ đó ta có $\varphi(A) = |T_A|$.

Sau đây chúng ta sẽ nghiên cứu một số tính chất của hàm Euler.

3.3.6 Mệnh đề :

Hàm Euler có tính nhân tức là nếu $A, B \Delta D$ và $(A, B) = E$ thì

$$\varphi(AB) = \varphi(A) \varphi(B).$$

Chứng minh

$$\text{Xét tương ứng } h: D/_{AB} \rightarrow D/_{A} \times D/_{B}$$

$$x + AB \mapsto (x + A, x + B)$$

Ta chứng minh h là một đẳng cấu vành

- h là một ánh xạ : Vì định nghĩa này không phụ thuộc vào cách chọn x , thật vậy $x_1 + AB = x_2 + AB \Rightarrow x_1 - x_2 \in AB \Rightarrow x_1 - x_2 \in A$,

$$x_1 - x_2 \in B \Rightarrow x_1 + A = x_2 + A, x_1 + B = x_2 + B$$

$$\Rightarrow (x_1 + A, x_1 + B) = (x_2 + A, x_2 + B)$$

- h là một đồng cấu : Hiển nhiên
- h là một đơn ánh vì $h(x + AB) = 0$ suy ra $x + A = \bar{0}; x + B = \bar{0}$

Do đó $x : A, x : B$. Mà $(A, B) = E$ nên theo mệnh đề 1.1.6 ta phải có $x : AB$ hay $x + AB = 0$.

- h là một toàn ánh : Thật vậy lấy phần tử $(x_1 + A, y_1 + B) \in D/_{A} \times D/_{B}$.

Do $(A, B) = E$ nên $A + B = D$ suy ra tồn tại $a_1 \in A, b_1 \in B$ sao cho $a_1 + b_1 = 1$.

Xét phần tử $x = b_1 x_1 + a_1 y_1$ thì rõ ràng $x \equiv x_1 \pmod{A}, x \equiv y_1 \pmod{B}$. Từ đó ta có: $h(x + AB) = (x + A, x + B) = (x_1 + A, y_1 + B)$. Vậy h là một đẳng cấu hay $D/_{AB} \cong D/_{A} \times D/_{B}$. Dễ thấy h là một đồng cấu vành do đó h là một

đẳng cấu vành. Mặt khác với $x \in D$ thì $(x, AB) = E \Leftrightarrow (x, A) = E$

và $(x, B) = E$ nên h cảm sinh đẳng cấu nhóm $h: (D/_{AB})^* \rightarrow (D/_{A})^* \times (D/_{B})^*$

Do đó $\varphi(AB) = \varphi(A) \varphi(B)$.

3.3.7 Mệnh đề :

Cho A, B là các ideal của D và $A|B$ suy ra $\varphi(A) | \varphi(B)$

Chứng minh:

Xét $h: (D/_{B})^* \rightarrow (D/_{A})^*$

$$x + B \mapsto x + A$$

Ta thấy quy tắc h không phụ thuộc vào phần tử đại diện, thật vậy với

$$x_1 + B = x_2 + B \Rightarrow x_1 - x_2 \in B \Rightarrow x_1 - x_2 \in A \Rightarrow x_1 + A = x_2 + A.$$

h là ánh xạ vì $A|B$ nên $(x, B) = E \Rightarrow (x, A) = E$. Dễ thấy rằng h là một đồng cấu nhóm.

Ta chứng minh h là toàn cấu tức chứng minh $(D/_{A})^* \subset \text{Im}h$. Thật vậy.

với mọi $x + A \in (D/_{A})^*$ suy ra $(x, A) = E$. Giả sử $P_i, (1 \leq i \leq k)$ là các ideal tối đại mà $P_i|B$ nhưng $P_i \nmid A$ (có thể không có ideal tối đại nào thỏa mãn điều kiện trên nhưng trong trường hợp này thì chứng minh của chúng ta đơn giản

Thế thì $(P_1 P_2 \dots P_k, A) = E$ suy ra $P + A = D$ với

$$P = \prod_{i=1}^k P_i. \text{ Từ đó tồn tại } p \in P, a \in A \text{ để } p + a = 1.$$

Xét $x' = px + a$ thì $x' \equiv x \pmod{A}$ và $x' \equiv 1 \pmod{P}$

Do đó $(x', A) = (x, A) = E$ và $(x', P) = E$ suy ra $(x', AP) = E$. Mà số các thừa số nguyên tố của B cũng giống như của AP . Vì thế $(x', B) = E$.

Do đó $x' + B \in (D/_{B})^*$.

Rõ ràng $h(x' + B) = x' + A = x + A$ suy ra $(D/_{A})^* \subset \text{Im}h$.

Vậy h là toàn cấu .

Theo định lý Note ta có $\text{Im} h \cong (D/B)^* / \ker h$

hay $(D/A)^* \cong (D/B)^* / \ker h$. Suy ra $\varphi(A) | \varphi(B)$.

3.3.8 Mệnh đề :

$n \in \mathbb{N}^*$, $A \triangle D$ thì $\varphi(A)^n = N(A)^{n-1} \cdot \varphi(A)$

Chứng minh

Nếu $n = 1$ thì mệnh đề đúng, ta chứng minh mệnh đề đúng với $n \geq 2$
Xét đồng cấu $h : (D/A^n)^* \rightarrow (D/A)^*$ Theo chứng minh ở 3.2.7 thì h là một

toàn cấu. $\text{Ker} h = \{ \overline{x/x} \equiv 1 \pmod{A} \} = \{ \overline{1+a/a} \in A \}$

Gọi $\{b_1, b_2, \dots, b_k\} = S_{A^{n-1}}$ là lớp các thặng dư đầy đủ theo mô đun A^{n-1}

Do $A | A^{n-1}$ nên theo mệnh đề 3.1.3 tồn tại $\alpha \in D$ sao cho $\langle \alpha \rangle = AB$ trong đó $(B, A^{n-1}) = E$.

Ta sẽ chứng minh $\text{ker} h = \{ \overline{1+a/a} \in A \} = \{ \overline{1+\alpha b_i} / 1 \leq i \leq k \}$

Thật vậy : Hiển nhiên $\{ \overline{1+\alpha b_i} / 1 \leq i \leq k \} \subset \text{ker} h$. Vì $\alpha b_i \in A$ do $\alpha \in A$

Với $a \in A$ bất kỳ do $(\langle \alpha \rangle, A^n) = (AB, A^n) = A(B, A^{n-1}) = A$ nên

$A = \langle \alpha \rangle + A^n$ từ đó $a = \alpha b + c$. Trong đó $c \in A^n$. Suy ra $a \equiv \alpha b_i \pmod{A^n}$.

Tồn tại $1 \leq i \leq k$ sao cho $b \equiv b_i \pmod{A^{n-1}}$. Do $\alpha : A$ nên $\alpha b \equiv \alpha b_i \pmod{A^n}$.

Vì thế $a \equiv \alpha b_i \pmod{A^n}$ hay $1+a \equiv 1+\alpha b_i \pmod{A^n}$. Suy ra $\overline{1+a} = \overline{1+\alpha b_i}$.

Thành thử $\text{ker} h \subset \{ \overline{1+\alpha b_i} / 1 \leq i \leq k \}$. Từ đó $\text{ker} h = \overline{1+\alpha b_i} / 1 \leq i \leq k$.

Mặt khác, giả sử $\overline{1+\alpha b_i} = \overline{1+\alpha b_j}$ thì $\langle \alpha(b_i - b_j) \rangle : A^n$

$\Rightarrow \langle \alpha \rangle \langle b_i - b_j \rangle : A^n \Rightarrow AB \langle b_i - b_j \rangle : A^n \Rightarrow B \langle b_i - b_j \rangle : A^{n-1}$

Mà $(B, A^{n-1}) = E$ nên $\langle b_i - b_j \rangle : A^{n-1} \Rightarrow b_i \equiv b_j \pmod{A^{n-1}}$. Do vậy $i = j$ và $b_i = b_j$ Vì thế $|\{ \overline{1 + \alpha b_i} / 1 \leq i \leq k \}| = k = N(A^{n-1}) = N(A)^{n-1}$ (do mệnh đề

3.2.4). Theo định lý Note thì $(D/A)^* \cong (D/A^n)^* / \ker h$.

Từ đó theo công thức Lagrange ta có $\varphi(A) = \frac{\varphi(A)}{|\ker h|} = \frac{\varphi(A^n)}{N(A)^{n-1}}$

Suy ra $\varphi(A^n) = N(A)^{n-1} \varphi(A)$.

3.3.9 Mệnh đề :

a) P là ideal tối đại của D thì $\varphi(P) = N(P) - 1$

b) A là ideal của D , $A = P^n$ thì $\varphi(A) = N(P)^{n-1} [N(P) - 1]$

c) A là ideal của D , A có sự phân tích

$A = P_1^{k_1} \dots P_r^{k_r}$ trong đó $k_i > 0, \forall i \in \overline{1, r}$ và P_i là các ideal nguyên tố

thì :

$$\varphi(A) = N(A) \left[1 - \frac{1}{N(P_1)} \right] \dots \left[1 - \frac{1}{N(P_r)} \right]$$

Chứng minh :

a) Do P là ideal tối đại nên D/P là một trường. Từ đó

$(D/P)^* = (D/P) \setminus \{0\}$. Suy ra $\varphi(P) = N(P) - 1$.

b) $A = P^n$ nên do mệnh đề 3.2.8 ta có:

$$\varphi(A) = \varphi(P^n) = \varphi(P) \cdot N(P)^{n-1} = N(P)^{n-1} [N(P) - 1]$$

c) Từ $A = P_1^{k_1} \dots P_r^{k_r}$ với $P_1^{k_1}, \dots, P_r^{k_r}$ đôi một nguyên tố cùng nhau

ên $\varphi(A) = \varphi(P_1^{k_1}) \dots \varphi(P_r^{k_r})$ Mặt khác $\varphi(P_i^{k_i}) = N(P_i)^{k_i-1} [N(P_i) - 1]$

$$= N(P_i)^{k_i} \left[1 - \frac{1}{N(P_i)} \right] \text{ Nên } \varphi(A) = \prod_{i=1}^r N(P_i)^{k_i} \left[1 - \frac{1}{N(P_i)} \right]$$

$$\begin{aligned}
&= \prod_{i=1}^r N(P_i^{k_i}) \left[1 - \frac{1}{N(P_i)} \right] = N \left[\prod_{i=1}^r N(P_i^{k_i}) \right] \prod_{i=1}^r \left[1 - \frac{1}{N(P_i)} \right] \\
&= N(A) \cdot \prod_{i=1}^r \left[1 - \frac{1}{N(P_i)} \right]
\end{aligned}$$

3.3.10 Mệnh đề :

Cho A là ideal của D khi đó $\sum_{B|A} \varphi(B) = N(A)$

Chứng minh

- Với $A = P^n$ suy ra $B \in \{D, P^1, P^2, \dots, P^n\}$

$$\begin{aligned}
\sum_{B|A} \varphi(B) &= \varphi(D) + \varphi(P) + \dots + \varphi(P^n) \\
&= 1 + N(P) - 1 + N(P)^2 - 1 + \dots + N(P)^n - N(P)^{n-1} \\
&= N(P)^n = N(P^n) = N(A)
\end{aligned}$$

- Với $A = P_1^{\alpha_1} \dots P_r^{\alpha_r}$, khi đó $B|A \Leftrightarrow B = P_1^{a_1} \dots P_r^{a_r}$

với $0 \leq a_i \leq \alpha_i, \forall i = 1, r$

$$N(A) = N \left[\prod_{i=1}^r P_i^{\alpha_i} \right] = \prod_{i=1}^r N(P_i^{\alpha_i}) = \prod_{i=1}^r \sum_{0 \leq a_i \leq \alpha_i} (P_i^{a_i}) = \sum_{0 \leq a_i \leq \alpha_i} \left(\prod_{i=1}^r P_i^{a_i} \right) = \sum_{B|A} \varphi(B)$$

3.4. CÁC ĐỊNH LÝ SỐ HỌC TRÊN VÀNH D

3.4.1 Định lý Euler :

$a \in D, A \Delta D$ sao cho $(a, A) = E$. Khi đó $a^{\varphi(A)} \equiv 1 \pmod{A}$

Chứng minh

Vì mọi phần tử của $(D/A)^*$ đều khả nghịch nên $(D/A)^*$ là một nhóm có cấp là $\varphi(A)$. Vì $(a, E) = 1$ nên theo mệnh đề 3.3.3 suy ra $\bar{a} \in (D/A)^*$. Từ đó cấp của $\bar{a}$ là ước của $\varphi(A)$. Do vậy, $\bar{a}^{\varphi(A)} = \bar{1}$ hay $a^{\varphi(A)} \equiv 1 \pmod{A}$.
 Từ định lý Euler ta rút ra các hệ quả sau :

3.4.2 Hệ quả :

P là ideal tối đại của D thì $a^{N(P)} \equiv a \pmod{P}$

Chứng minh

- Nếu $a : P \Rightarrow a^{N(P)} - a = a [a^{N(P)-1} - 1] : P$

Hay $a^{N(P)} \equiv a \pmod{P}$

- Nếu $(a, P) = E$ theo định lý Euler thì

$a^{\varphi(P)} \equiv 1 \pmod{P}$ nên $a^{\varphi(P)+1} \equiv a \pmod{P}$, mà P là ideal tối đại nên

$N(P) = \varphi(P) + 1$ Do đó $a^{N(P)} \equiv a \pmod{P}$

3.4.3 Hệ quả

$\alpha, \beta \in D$ và $(\langle \alpha \rangle, \langle \beta \rangle) = E$ thì $\alpha^{\varphi(\beta)} \equiv 1 \pmod{\beta}$

3.4.4 Hệ quả :

$A \Delta D, a \in D$ sao cho $(a, A) = E$. Nếu $s \equiv t \pmod{\varphi(A)}$

Thì $a^s \equiv a^t \pmod{A}$

3.4.5 Định lý Wilson :

Cho P là ideal tối đại của D và $s = \varphi(P) = N(P) - 1$. Nếu

$\{\xi_1, \dots, \xi_s\}$ là hệ thặng dư thu gọn theo mod P thì $\xi_1 \xi_2 \dots \xi_s \equiv -1 \pmod{P}$

Chứng minh

Trong trường D/P ta xét phương trình $x^s - \bar{1} = \bar{0} \quad (1)$

với $\forall i \in \{1, 2, \dots, s\}$ thì $\bar{\xi}_i \in (D/P)^*$. Từ đó $(\xi_i, P) = E$. Theo định lý Euler

ta có :

$$\xi_i^s \equiv 1 \pmod{P} \text{ hay } \bar{\xi}_i^s - \bar{1} = \bar{0}$$

Từ đó ta thấy $\bar{\xi}_1, \dots, \bar{\xi}_s$ là tất cả các nghiệm của phương trình (1)

Do đó $x^s - \bar{1} = \prod_{i=1}^s (x - \bar{\xi}_i)$. Theo định lý Viet ta có

$\prod_{i=1}^s \overline{\xi_i} = (-1)^s (-\bar{1}) \quad (2)$. Giả sử trường hữu hạn D/P có đặc số p

- Nếu $p = 2$: khi đó $|D/P| = 2^n$ là số chẵn nên s lẻ suy ra (2)

trở thành $\prod_{i=1}^s \overline{\xi_i} = (-1)(-\bar{1}) = \bar{1} = -\bar{1}$

- Nếu $p > 2$: khi đó $|D/P| = p^n$ là số lẻ nên s chẵn suy ra (2) trở thành

$$\prod_{i=1}^s \overline{\xi_i} = 1. (-\bar{1}) = -\bar{1}. \text{ Vậy } \prod_{i=1}^r \xi_i = -1 \pmod{P}$$

CHƯƠNG 4

SỐ HỌC TRÊN VÀNH $D = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$

Mục đích của chương này là khảo sát một cách chi tiết số học trên vành $D = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$, cụ thể ta mô tả các ideal tối đại của vành D ; mô tả thuật toán phân tích một phần tử của D thành tích của các ideal tối đại. Đồng thời đưa ra một số ví dụ minh họa.

4.1 VÀNH $D = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$

Trước khi khảo sát tính chất số học của vành D , ta chứng minh D không phải là vành Gauss và khái niệm USCLN trên D không tồn tại. Do đó, số học trên vành D nói chung là khó nghiên cứu.

4.1.1 Các ví dụ :

- Các phần tử $2; 3; \sqrt{-6}$ là các phần tử bất khả quy trong D
- D không phải là vành Gauss
- USCLN của 6 và $2\sqrt{-6}$ không tồn tại

Chứng minh :

- Giả sử $2 = \alpha.\beta$ với $\alpha, \beta \in D$ ta chứng minh α hoặc β khả nghịch.

Vì $2 = \alpha.\beta \Rightarrow N(2) = N(\alpha).N(\beta) \Rightarrow 4 = N(\alpha).N(\beta)$. Ta xét các khả năng:

KN1 : $N(\alpha) = 1$; $N(\beta) = 4$ khi $N(\alpha) = 1 \Rightarrow a^2 + 6b^2 = 1 \Rightarrow a = \pm 1, b = 0 \Rightarrow \alpha$ khả nghịch

KN2 : $N(\alpha) = 4, N(\beta) = 1$ Tương tự như trên

KN3 : $N(\alpha) = 2; N(\beta) = 2$ khi đó $a^2 + 6b^2 = 2$ điều này cũng không xảy ra

- Giả sử $3 = \alpha.\beta$ với $\alpha, \beta \in D$. Khi đó $N(3) = N(\alpha).N(\beta)$

$\Rightarrow 9 = N(\alpha) \cdot N(\beta)$. Ta xét các khả năng:

KN1 : $N(\alpha) = 1, N(\beta) = 9$. Do $N(\alpha) = 1$ nên $a^2 + 6b^2 = 1$, tương tự trên α khả nghịch

KN2 : $N(\alpha) = 3 ; N(\beta) = 1$ Tương tự như trên

KN3 : $N(\alpha) = 3 ; N(\beta) = 3$. Do đó ta có $a^2 + 6b^2 = 3$. Điều này cũng không xảy ra.

• Giả sử $\sqrt{-6} = \alpha \cdot \beta$ với $\alpha, \beta \in D$. Khi đó $N(\sqrt{-6}) = N(\alpha) \cdot N(\beta)$

$\Rightarrow 6 = N(\alpha) \cdot N(\beta)$. Ta xét các khả năng.

KN1 : $N(\alpha) = 1 ; N(\beta) = 6$ hoặc $N(\alpha) = 6, N(\beta) = 1$. Tương tự như trên.

KN2 : $N(\alpha) = 2, N(\beta) = 3$. Do đó $a^2 + 6b^2 = 2$. Không xảy ra.

KN3 : $N(\alpha) = 3; N(\beta) = 2$. Không xảy ra .

Vậy 2, 3, $\sqrt{-6}$ là các phần tử bất khả quy trong D.

b) Ta thấy 6 có hai sự phân tích thành tích của các phần tử bất khả qui trong D là $6 = 2 \cdot 3 = -\sqrt{-6} \cdot \sqrt{-6}$ nên D không phải vành Gauss. Từ đó ta có D cũng không phải là vành chính.

c) Ta thấy 6 có các ước số $\pm 1; \pm 2; \pm 3; \pm \sqrt{-6}$

$2\sqrt{-6}$ có các ước số là $\pm 1; \pm 2; \pm \sqrt{-6}; \pm 2\sqrt{-6}$. Từ đó USC của 6 và $2\sqrt{-6}$ là $\pm 1; \pm 2; \pm \sqrt{-6}$. Rõ ràng trong các USC ở trên không có USC nào chia hết cho các USC còn lại.

4.1.2 Mệnh đề :

$D = \{a + b\sqrt{-6} / a, b \in \mathbb{Z}\}$ là vành các số nguyên đại số của

$K = \mathbb{Q}(\sqrt{-6})$ trên $\mathbb{Q}$.

Chứng minh :

Gọi D' là vành các số nguyên đại số của $K = \mathbb{Q}(\sqrt{-6})$ trên $\mathbb{Q}$.

Với $\alpha = a + b\sqrt{-6} \in D$ thì α là nghiệm của đa thức

$f(x) = (x - a)^2 + 6b^2$ suy ra $\alpha \in D'$. Vậy $D \subset D'$ rõ ràng phần tử $\alpha \in D'$ bất kỳ ta có thể biểu diễn dưới dạng $\alpha = (a + b\sqrt{-6})/c$ trong $a, b, c \in \mathbb{Z}$ và $(a, b, c) = 1$. Giả sử $f(x)$ là đa thức tối thiểu của α . Do α là số nguyên đại số nên $f(x) \in \mathbb{Z}[x]$ do đó

$$f(x) = (x - \alpha)(x - \bar{\alpha}) \Rightarrow f(x) = x^2 - \frac{2a}{c}x + \frac{a^2 + 6b^2}{c^2} \text{ do } f(x) \in \mathbb{Z}[x] \text{ suy ra}$$

$$\frac{2a}{c} \in \mathbb{Z} \Rightarrow \frac{4a^2}{c^2} \in \mathbb{Z} \text{ và } \frac{24b^2}{c^2} \in \mathbb{Z} \Rightarrow \frac{2a}{c} \in \mathbb{Z} \text{ và } \frac{24b^2}{c^2} \in \mathbb{Z}$$

Giả sử p là ước nguyên tố lớn hơn 2 của c suy ra $p|2a$ nên $p|a$; $p^2|24b^2$ suy ra $p|b^2 \Rightarrow p|b$. Từ đó $(a, b, c) : p$ (vô lý). Vì thế c không có ước số nguyên tố lớn hơn 2. Ta cũng thấy $c \neq 4$ vì nếu ngược lại $c = 4$ thì $4|2a \Rightarrow 2|a$; $16|24b^2 \Rightarrow 2|3b^2 \Rightarrow 2|b$. Từ đó $(a, b, c) : 2$ (vô lý). Vậy chỉ có thể $c = 1$ hoặc $c = 2$.

- Với $c = 2$: Ta có $4|a^2 + 6b^2$

Nếu $a : 2$ thì $6b^2 : 4 \Rightarrow b^2 : 2 \Rightarrow b : 2$ suy ra $(a, b, c) = 2$ (vô lý)

Nếu $a \equiv 1 \pmod{2} \Rightarrow a^2 \equiv 1 \pmod{4}$ mà $6b^2$ chẵn nên $a^2 + 6b^2$ lẻ $\Rightarrow a^2 + 6b^2 : 4$ (vô lý)

- Với $c = 1$: Khi đó $\alpha = a + b\sqrt{-6}$ với $a, b \in \mathbb{Z} \Rightarrow \alpha \in D \Rightarrow D' \subset D$.

Tóm lại ta có: $D = D'$ hay D là vành các số nguyên đại số của $K = \mathbb{Q}\sqrt{-6}$ trên $\mathbb{Q}$.

4.1.3 Mệnh đề :

Nếu $\alpha = a + b\sqrt{-6} \in D$ thì $N(\langle \alpha \rangle) = N(\alpha) = a^2 + 6b^2$

Chứng minh

Giả sử $f(x)$ là đa thức tối thiểu của α

- Nếu $\alpha \in \mathbb{Q}$ thì $f(x) = x - \alpha$ và $N(\alpha) = \alpha^{(1)}.\alpha^{(2)} = \alpha.\alpha = \alpha^2 = a^2 + 6b^2$

• Nếu $\alpha \notin Q$ thì $\deg f = 2$. Từ đó $f(x) = (x - \alpha)(x - \bar{\alpha})$ và $N(\alpha) = \alpha^{(1)} \cdot \alpha^{(2)} = \alpha \cdot \bar{\alpha} = a^2 + 6b^2$.

Trước tiên ta thấy rằng $|D / \langle \alpha \rangle| = |D / \langle \bar{\alpha} \rangle|$. Thật vậy, ta có $a \in \langle \alpha \rangle$ thì $\bar{a} \in \langle \bar{\alpha} \rangle$. Vì thế nếu S là hệ thặng dư đầy đủ theo mod $\langle \alpha \rangle$ thì $\bar{S} = \{\bar{s} / s \in S\}$ là hệ thặng dư đầy đủ theo mod $\langle \bar{\alpha} \rangle$. Từ đó $N(\langle \alpha \rangle) = |S| = |\bar{S}| = N(\langle \bar{\alpha} \rangle)$. Mặt khác $N(\alpha) = \alpha \cdot \bar{\alpha}$ nên $\langle N(\alpha) \rangle = \langle \alpha \rangle \langle \bar{\alpha} \rangle$ hay $N(\langle \alpha \rangle) \cdot N(\langle \bar{\alpha} \rangle) = N(\langle N(\alpha) \rangle) = N(\alpha)^2 = (a^2 + 6b^2)^2$
 $\Rightarrow N(\langle \alpha \rangle)^2 = (a^2 + 6b^2)^2 \Rightarrow N(\langle \alpha \rangle) = a^2 + 6b^2 = N(\alpha)$.

4.1.4 Bổ đề :

Cho $A \triangle D$ và $N(A) = p$ là một số nguyên tố thì A là ideal tối đại của D .

Chứng minh :

Giả sử $A \subset B \subset D$. Thế thì $B|A \Rightarrow N(B)|N(A)$ hay $N(B)|p \Rightarrow N(B) = 1$ hoặc $N(B) = p$.

Nếu $N(B) = 1 \Rightarrow B = D$

Nếu $N(B) = p$ thì $N(A) = N(B)$. Giả sử $A = B.C \Rightarrow N(C) = 1$. Theo trên ta có $C = D$ suy ra $A = B.D = B$.

Vậy A là ideal tối đại.

Định lý sau đây cho phép chúng ta mô tả tất cả các ideal tối đại của D .

4.1.5 Định lý : Cho p là một số nguyên tố nào đó, khi đó :

a) Với $p = 2; 3$ thì :

- $\langle 2 \rangle = M_2^2$ với $M_2 = \langle 2, \sqrt{-6} \rangle$. M_2 là ideal tối đại và $N(M_2) = 2$.
- $\langle 3 \rangle = M_3^2$ với $M_3 = \langle 3, \sqrt{-6} \rangle$. M_3 là ideal tối đại và $N(M_3) = 3$.

b) Với $p > 3$. Nếu $\frac{-6}{p} = 1$ thì tồn tại $a \in \mathbb{Z}$ để $a^2 + 6 \equiv 0 \pmod{p}$ và

ta có sự phân tích $\langle p \rangle = M_p \cdot \overline{M_p}$ trong đó $M_p = \langle p, a + \sqrt{-6} \rangle$;

$\overline{M_p} = \langle p, a - \sqrt{-6} \rangle$ và hơn nữa $M_p, \overline{M_p}$ là các ideal tối đại của D và

$$N(M_p) = N(\overline{M_p}) = p.$$

c) Với $p > 3$. Nếu $\left(\frac{-6}{p}\right) = -1$ thì $\langle p \rangle = M_p$ là ideal tối đại của D và

$$N(M_p) = p^2$$

Ngược lại, bất kỳ một ideal tối đại nào của D đều trùng với một trong các ideal M_p hoặc $\overline{M_p}$ với p là một số nguyên tố nào đó.

Chứng minh:

a) Ta có $2 = \sqrt{-6} \cdot \sqrt{-6} + 2 \cdot 4 \in M_2^2 \Rightarrow \langle 2 \rangle \subset M_2^2$. Mặt khác

$\sqrt{-6} \cdot \sqrt{-6} = -6 = 2(-3) \in \langle 2 \rangle$. Với $\forall \alpha, \beta \in M_2$ mà $\alpha = 2\alpha_1 + \sqrt{-6} \alpha_2$

với $\alpha_1, \alpha_2 \in D$ và $\beta = 2\beta_1 + \sqrt{-6} \beta_2$ với $\beta_1, \beta_2 \in D$

khi đó $\alpha \cdot \beta = 2(2\alpha_1\beta_1 + \sqrt{-6}\alpha_1\beta_2 + \sqrt{-6}\alpha_2\beta_1) - 6\beta_1\beta_2 \in \langle 2 \rangle$

$\Rightarrow M_2^2 \subset \langle 2 \rangle$. Vậy $\langle 2 \rangle = M_2^2$. Ta lại có $N(M_2^2) = N(\langle 2 \rangle) = 2^2 \Rightarrow N(M_2) = 2$

mà 2 là số nguyên tố nên M_2 là ideal tối đại.

• Ta có $3 = \sqrt{-6} \cdot \sqrt{-6} + 3 \cdot 3 \in M_3^2 \Rightarrow \langle 3 \rangle \subset M_3^2$. Mặt khác

$\sqrt{-6} \cdot \sqrt{-6} = -6 = 3 \cdot (-2) \in \langle 3 \rangle$. Với $\forall \alpha, \beta \in M_3$ mà $\alpha = 3\alpha_1 + \sqrt{-6} \alpha_2$

với $\alpha_1, \alpha_2 \in D$; $\beta = 3\beta_1 + \sqrt{-6} \beta_2$ với $\beta_1, \beta_2 \in D$

khi đó $\alpha \cdot \beta = 3(3\alpha_1\beta_1 + \sqrt{-6}\alpha_2\beta_1) - 6\beta_1\beta_2 \in \langle 3 \rangle \Rightarrow M_3^2 \subset \langle 3 \rangle$.

Vậy $\langle 3 \rangle = M_3^2$. Ta lại có $N(M_3^2) = N(\langle 3 \rangle) = 3^2 \Rightarrow N(M_3) = 3$ mà 3 là số

nguyên tố nên M_3 ideal tối đại.

b) Nếu $(\frac{-6}{p}) = 1, p > 3$ thì tồn tại $a \in \mathbb{Z}$ để $a^2 + 6 \equiv 0 \pmod{p}$

nên $(2a, p) = 1 \Rightarrow \exists r, s \in \mathbb{Z}$ sao cho $2ar + ps = 1$. ta lại có

$$p(a + \sqrt{-6}) + p(a - \sqrt{-6}) \in M_p \cdot \overline{M_p} \Rightarrow 2pa \in M_p \cdot \overline{M_p}$$

$$\Rightarrow p = p(2ar + ps) = 2par + p^2s \in M_p \cdot \overline{M_p} \quad (1) \quad \text{Ngược lại giả sử}$$

$$\alpha \in M_p, \beta \in \overline{M_p} \text{ thì } \alpha = px + (p + a\sqrt{-6})y; \beta = pz + (a - \sqrt{-6})t$$

$$\Rightarrow \alpha\beta = p\omega + (a^2 + 6)yt \quad (\text{trong đó } \omega = pxz + xta + zya + (zy - xt)\sqrt{-6})$$

$$= p\omega + pmyt \in \langle p \rangle \quad (\text{với } pm = a^2 + 6 \text{ vì } a^2 + 6 \equiv 0 \pmod{p}) \text{ cho nên}$$

$$M_p \cdot \overline{M_p} = \left\{ \sum_{i \in I} \alpha_i \beta_i \mid I \text{ hữu hạn, } \alpha_i \in M_p, \beta_i \in \overline{M_p} \right\} \subset \langle p \rangle \quad (2), \text{ từ (1) và (2)}$$

$$\text{ta có } \langle p \rangle = M_p \cdot \overline{M_p} \quad \text{Từ đó } N(\langle p \rangle) = N(M_p \cdot \overline{M_p}) \Rightarrow N(M_p) \cdot N(\overline{M_p}) = p^2 \quad (*)$$

Mặt khác $N(M_p)$ và $N(\overline{M_p})$ khác 1. Vì giả sử $N(M_p) = 1 \Rightarrow M_p = D$

$$\Rightarrow \overline{M_p} = D \Rightarrow N(M_p) \cdot N(\overline{M_p}) = 1 \quad (\text{vô lý với } (*)). \text{ Vì thế từ } (*) \text{ ta có}$$

$N(M_p) = N(\overline{M_p}) = p$ mà p là số nguyên tố nên $M_p, \overline{M_p}$ là các ideal tối đại.

c) Xét $B = \langle p, \alpha \rangle$ với $\alpha = a + b\sqrt{-6}, a, b \in \mathbb{Z}$.

Bây giờ ta chứng minh nếu $(a, p) = 1$ hoặc $(b, p) = 1$ thì $B = D$. Thật vậy,

• Nếu $(b, p) = 1$ thì $\exists r, s \in \mathbb{Z}$ sao cho $br + ps = 1$

$$\Rightarrow \sqrt{-6}ps + r(a + b\sqrt{-6}) = (ps + br)\sqrt{-6} + ar = ar + \sqrt{-6} = a' + \sqrt{-6} \text{ với}$$

$$a' = ar. \text{ Rõ ràng } \sqrt{-6}ps + r(a + b\sqrt{-6}) \in B \Rightarrow a' + \sqrt{-6} \in B \text{ hay}$$

$\langle p, a' + \sqrt{-6} \rangle \subset B$. Mặt khác do $a^2 + 6 \not\equiv 0 \pmod{p}$ nên $(a^2 + 6, p) = 1 \Rightarrow \exists m, n \in \mathbb{Z}$ sao cho $(a^2 + 6)m + pn = 1 \quad (**)$ mà

$$(a^2 + 6)m + np = m(a' + \sqrt{-6})(a' - \sqrt{-6}) + np \in \langle p, a' + \sqrt{-6} \rangle$$

nên từ $(**)$ ta có $1 \in \langle p, a' + \sqrt{-6} \rangle \Rightarrow \langle p, a' + \sqrt{-6} \rangle = D$ hay $B = D$.

• Nếu $(a, p) = 1$, ta chỉ xét $(b, p) \neq 1$ suy ra $b : p$ nên
 $a = a + b\sqrt{-6} - p \cdot \frac{b}{p}\sqrt{-6} \in B$. Từ đó $\langle p, a \rangle \subset B$. Ta lại có $(a, p) = 1$ nên
 tồn tại $u, v \in \mathbb{Z}$ sao cho $au + pv = 1 \Rightarrow 1 \in \langle p, a \rangle$ hay $\langle p, a \rangle = D$. Điều này
 dẫn tới $B = D$.

Trường hợp nếu $a : p, b : p$ thì $a + b\sqrt{-6} : p$ suy ra $B = \langle p \rangle$.

Bây giờ ta chứng minh $\langle p \rangle$ là ideal tối đại. Giả sử $M \Delta D$ và $\langle p \rangle \subset M$.
 Theo mệnh đề 2.2.10 tồn tại $\alpha, \beta \in D^*$ sao cho $M = (\langle \alpha \rangle, \langle \beta \rangle) = \langle \alpha, \beta \rangle$ với
 $\alpha = a + b\sqrt{-6}, \beta = c + d\sqrt{-6}$. Ta xét hai trường hợp

TH1 : Nếu $a, b, c, d : p \Rightarrow M = \langle a + b\sqrt{-6}, c + d\sqrt{-6} \rangle$

TH2 : Nếu tồn tại một trong 4 số a, b, c, d không chia hết cho p . Giả sử
 $a : p$ khi đó $\langle p, \alpha \rangle = D$ mà $\langle p, \alpha \rangle \subset \langle \alpha, \beta \rangle = M$. Từ đó $M = D$. Vậy $\langle p \rangle$ là
 ideal tối đại.

Ngược lại, bây giờ ta chứng minh các ideal tối đại của D phải có dạng
 M_p hoặc $\overline{M}_p$. Giả sử M là ideal tối đại của D . Lấy $\alpha \in M$ thì $N(\alpha) : \alpha$ nên
 $N(\alpha) \in \langle \alpha \rangle \subset M \Rightarrow \langle N(\alpha) \rangle \subset M \Rightarrow M | \langle N(\alpha) \rangle$.

Mặt khác $N(\alpha) \in \mathbb{N}$ nên $N(\alpha) = p_1^{k_1} \dots p_r^{k_r}$ trong đó p_i là các số
 nguyên tố, $i = \overline{1, r}$. Do đó $\langle N(\alpha) \rangle = \langle p_1 \rangle^{k_1} \dots \langle p_r \rangle^{k_r}$. Mà các $\langle p_i \rangle$, $i = \overline{1, r}$
 chỉ có các thừa số nguyên tố là các ideal tối đại có dạng M_p hoặc $\overline{M}_p$ mà M
 lại là một trong các thừa số đó nên M phải có dạng M_p hoặc $\overline{M}_p$.

4.1.6 Hệ quả :

Cho p là một số nguyên tố, khi đó xảy ra một trong ba khả năng :

a) • Với $p = 2$ thì $\langle 2 \rangle = M_2^2$ với $M_2 = \langle 2; \sqrt{-6} \rangle$

• Với $p = 3$ thì $\langle 3 \rangle = M_3^2$ với $M_3 = \langle 3; \sqrt{-6} \rangle$

b) Với p có dạng $24k + 1; 24k + 5; 24k + 7; 24k + 11$ thì tồn tại

$a \in \mathbb{Z}$ để $a^2 + 6 \equiv 0 \pmod{p}$ và ta có sự phân tích $\langle p \rangle = M_p \cdot \overline{M}_p$ với

$M_p = \langle p, a + \sqrt{-6} \rangle$, $\overline{M}_p = \langle p, a - \sqrt{-6} \rangle$ và hơn nữa $M_p, \overline{M}_p$ là các ideal tối đại và $N(M_p) = N(\overline{M}_p) = p$

c) Với p có dạng $24k + 13; 24k + 17; 24k + 19; 24k + 23$ thì $\langle p \rangle = M_p$ là ideal tối đại và $N(M_p) = p^2$.

Các số nguyên tố dạng a), b) gọi là các số nguyên tố loại I, các số nguyên tố dạng c) gọi là các số nguyên tố loại II.

Chứng minh

a) Ta suy ngay từ định lý trên. Ta cần chứng minh b), c).

Áp dụng tính chất của công thức Lagrăng ta có

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) \text{ mà } \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}; \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

$$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2} \frac{p-1}{2}} \left(\frac{p}{3}\right). \text{ Từ đó ta có } \left(\frac{-6}{p}\right) = (-1)^{\frac{p^2-1}{8}} \left(\frac{p}{3}\right) (*)$$

b) • Xét $p = 24k + 5; p = 24k + 11$

$$\text{Khi đó } \frac{p^2-1}{8} \text{ lẻ, } p \equiv -1 \pmod{3}, \text{ kết hợp } (*) \text{ ta có } \left(\frac{-6}{p}\right) = (-1) \left(\frac{-1}{3}\right) = 1$$

• Xét $p = 24k + 1; p = 24k + 7$

$$\text{Khi đó } \frac{p^2-1}{8} \text{ chẵn, } p \equiv 1 \pmod{3}, \text{ kết hợp } (*) \text{ ta có } \left(\frac{-6}{p}\right) = \left(\frac{1}{3}\right) = 1$$

c) • Xét $p = 24k + 17; p = 24k + 23$

$$\text{Khi đó } \frac{p^2-1}{8} \text{ chẵn, } p \equiv -1 \pmod{3}, \text{ kết hợp } (*) \text{ ta có } \left(\frac{-6}{p}\right) = \left(\frac{-1}{3}\right) = -1$$

• Xét $p = 24k + 13; 24k + 19$

$$\text{Khi đó } \frac{p^2-1}{8} \text{ lẻ, } p \equiv 1 \pmod{3}, \text{ kết hợp } (*) \text{ ta có } \left(\frac{-6}{p}\right) = (-1) \left(\frac{1}{3}\right) = -1$$

4.2 THUẬT TOÁN PHÂN TÍCH RA THỪA SỐ NGUYÊN TỐ - CÁC VÍ DỤ

4.2.1 Thuật toán phân tích ra thừa số nguyên tố

Trong phần này, chúng ta sẽ chỉ ra thuật toán để phân tích một ideal A thành các ideal tối đại.

a) Trước hết ta xét A là ideal chính và $A = \langle \alpha \rangle$

với $\alpha = a + b\sqrt{-6}$, $a, b \in \mathbb{Z}$ $(a, b) = 1$

Giả sử $N(\alpha) = p_1 \dots p_k$ trong đó p_i , $i = \overline{1, k}$ là các số nguyên tố có thể trùng nhau, khi đó $\langle N(\alpha) \rangle = \langle p_1 \rangle \dots \langle p_k \rangle$

hay $\langle \alpha \rangle \langle \bar{\alpha} \rangle = \langle p_1 \rangle \dots \langle p_k \rangle$ ta chứng minh p_i ($i = \overline{1, k}$) là các số nguyên tố loại I. Thật vậy giả sử tồn tại p_i là số nguyên tố loại II suy ra $\langle p_i \rangle$ là ideal nguyên tố. Do $\langle p_i \rangle \mid \langle \alpha \rangle \langle \bar{\alpha} \rangle$ nên $\langle p_i \rangle \mid \langle \alpha \rangle$ hoặc $\langle p_i \rangle \mid \langle \bar{\alpha} \rangle$ suy ra $p_i \mid \alpha$ hoặc $p_i \mid \bar{\alpha}$ từ đó ta có $a \div p$, $b \div p$ (vô lý)

*, $(a, b) = d > 1$

Đặt $a = da'$, $b = db'$ thì $(a', b') = 1$. Giả sử $d = q_1 \dots q_m$ (q_i là các số nguyên tố có thể trùng nhau)

$$\langle \alpha \rangle = \langle a + b\sqrt{-6} \rangle = \langle d \rangle \langle a' + b'\sqrt{-6} \rangle$$

$$= \langle q_1 \rangle \dots \langle q_m \rangle \langle a' + b'\sqrt{-6} \rangle.$$

- Nếu q_i là 2 số nguyên tố loại I thì $\langle q_i \rangle = M_{q_i} \bar{M}_{q_i}$
- Nếu q_i là nguyên tố loại II thì $\langle q_i \rangle$ là tối đại
- $\langle a', b'\sqrt{-6} \rangle$ sẽ được phân tích như trên.

b) Giả sử A là một ideal bất kỳ của D . Thế thì tồn tại $\alpha = a + b\sqrt{-6}$,

$\beta = c + d\sqrt{-6}$ sao cho $A = (\langle\alpha\rangle, \langle\beta\rangle)$. Theo thuật toán ở trên thì ta có thể phân tích được

$$\langle\alpha\rangle = P_1^{k_1} \dots P_r^{k_r} \quad \text{và} \quad \langle\beta\rangle = P_1^{l_1} \dots P_r^{l_r}$$

$$\text{Do đó } A = P_1^{\min\{k_1, l_1\}} \dots P_r^{\min\{k_r, l_r\}}$$

4.2.2 Một số ví dụ

Sau đây chúng tôi đưa ra một số ví dụ minh họa về sự phân tích các ideal trong vành D thành các ideal tối đại.

a) Phân tích ra thừa số nguyên tố $\langle\alpha\rangle = \langle 429 + 143\sqrt{-6} \rangle$. Tính $\varphi(\langle\alpha\rangle)$.

$$\text{Ta có } \langle\alpha\rangle = \langle 11 \rangle \langle 13 \rangle \langle 3 + \sqrt{-6} \rangle$$

$$+) 13 \text{ có dạng } 24k + 13 \text{ nên } \langle 13 \rangle = M_{13}$$

$$+) 11 \text{ có dạng } 24k + 11 \text{ nên } \langle 11 \rangle = \langle 11, 7 + \sqrt{-6} \rangle \langle 11, 7 - \sqrt{-6} \rangle = M_{11} \bar{M}_{11}$$

$$+) \text{ Đặt } \beta = 3 + \sqrt{-6}. \text{ Ta có } (3, 1) = 1, N(\beta) = 3^2 + 6 = 15 = 3 \cdot 5$$

$$\langle 3 \rangle = M_3^2 = \langle 3, \sqrt{-6} \rangle^2$$

$$\langle 5 \rangle = \langle 5, 2 + \sqrt{-6} \rangle \langle 5, 2 - \sqrt{-6} \rangle = M_5 \bar{M}_5$$

$$\text{Mặt khác } 3 + \sqrt{-6} = 5 - (2 - \sqrt{-6}) \in \langle 5, 2 - \sqrt{-6} \rangle = \bar{M}_5$$

$$\text{Vậy } \langle\alpha\rangle = M_3 \cdot \bar{M}_5 \cdot M_{11} \cdot \bar{M}_{11} \cdot M_{13}$$

$$\varphi(\langle\alpha\rangle) = \varphi(M_3) \varphi(\bar{M}_5) \varphi(M_{11}) \varphi(\bar{M}_{11}) \varphi(M_{13})$$

$$\text{hay } \varphi(\langle\alpha\rangle) = (3 - 1)(5 - 1)(11 - 1)(11 - 1)(13^2 - 1) = 134400$$

b) Phân tích ra thừa số nguyên tố $\langle\alpha\rangle = \langle 1190 + 1785\sqrt{-6} \rangle$.

Tính $\varphi(\langle\alpha\rangle)$

$$\text{Ta có } \langle\alpha\rangle = \langle 5 \rangle \langle 7 \rangle \langle 17 \rangle \langle 2 + 3\sqrt{-6} \rangle$$

$$+) 5 \text{ có dạng } 24k + 5 \text{ nên } \langle 5 \rangle = \langle 5, 2 + \sqrt{-6} \rangle \langle 5, 2 - \sqrt{-6} \rangle = M_5 \bar{M}_5$$

$$+) 7 \text{ có dạng } 24k + 7 \text{ nên } \langle 7 \rangle = \langle 7, 1 + \sqrt{-6} \rangle \langle 7, 1 - \sqrt{-6} \rangle = M_7 \bar{M}_7$$

+) 17 có dạng $24k + 17$ nên $\langle 17 \rangle = M_{17}$

+) Đặt $\beta = 2 + 3\sqrt{-6}$. Ta có $(2, 3) = 1$, $N(\beta) = 4 + 54 = 58 = 2 \cdot 29$

$$\langle 2 \rangle = M_2^2 = \langle 2, \sqrt{-6} \rangle^2$$

$$\langle 29 \rangle = \langle 29, 9 + \sqrt{-6} \rangle \langle 29, 9 - \sqrt{-6} \rangle = M_{29} \cdot \overline{M}_{29}$$

Mặt khác $2 + 3\sqrt{-6} = 29 - 3(9 - \sqrt{-6}) \in \overline{M}_{29}$

$$\text{Vậy } \langle \alpha \rangle = M_2 \cdot M_5 \cdot \overline{M}_5 \cdot M_7 \cdot \overline{M}_7 \cdot M_{17} \cdot \overline{M}_{29}$$

$$\varphi(\langle \alpha \rangle) = \varphi(M_2) \cdot \varphi(M_5) \cdot \varphi(\overline{M}_5) \cdot \varphi(M_7) \cdot \varphi(\overline{M}_7) \cdot \varphi(M_{17}) \cdot \varphi(\overline{M}_{29})$$

$$\begin{aligned} \text{hay } \varphi(\langle \alpha \rangle) &= (2-1)(5-1)(5-1)(7-1)(7-1)(17^2-1)(29-1) \\ &= 4644864 \end{aligned}$$

c) Phân tích ra thừa số nguyên tố $\langle \alpha \rangle = \langle 55 + 22\sqrt{-6} \rangle$. Tính $\varphi(\langle \alpha \rangle)$.

Ta có $\langle \alpha \rangle = \langle 11 \rangle \langle 5 + 2\sqrt{-6} \rangle$.

+) 11 có dạng $24k + 11$ nên $\langle 11 \rangle = M_{11} \cdot \overline{M}_{11}$

+) Đặt $\beta = 5 + 2\sqrt{-6}$, $(5, 2) = 1$, $N(\beta) = 25 + 24 = 49 = 7^2$.

$$\text{Vậy } \langle \alpha \rangle = M_{11} \cdot M_7.$$

$$\varphi(\langle \alpha \rangle) = \varphi(M_{11}) \cdot \varphi(M_7) = (11-1)(7-1) = 60.$$

KẾT LUẬN

Ký hiệu D là vành các số nguyên đại số của trường mở rộng hữu hạn của Q . Sau khi nghiên cứu cấu trúc các ideal của vành D chúng tôi đã thu được một số kết quả như sau :

1 . Tập các ideal khác 0 của vành D là một nửa nhóm giao hoán, có đơn vị, với sự phân tích duy nhất thành các phần tử nguyên tố, các phần tử nguyên tố chính là các ideal tối đại.

2 . Xây dựng được số học trên vành các số nguyên đại số D , cụ thể là đã xây dựng được và nghiên cứu các tính chất cùng với các công thức tính các hàm số học sau:

+ Hàm chuẩn : $N : \mathbf{P} \rightarrow \mathbf{N}^*$

$$A \mapsto N(A) = |D/A|$$

+ Hàm Euler $\varphi : \mathbf{P} \rightarrow \mathbf{N}^*$

$$A \mapsto \varphi(A) = |(D/A)^*|$$

và các định lý số học trên vành D :

+ Định lý Euler : $a \in D, A \Delta D$ sao cho $(a, A) = E$.

Khi đó $a^{q(A)} \equiv 1 \pmod{A}$

+ Định lý Fecma : P là ideal tối đại của D thì $a^{N(P)} \equiv a \pmod{P}$

+ Định lý Winlson : Cho P là ideal tối đại của D và $s = \varphi(P) = N(P) - 1$.

Nếu $\{\xi_1, \dots, \xi_s\}$ là hệ thặng dư thu gọn theo mod P thì $\xi_1 \dots \xi_s \equiv -1 \pmod{P}$

3 . Như là một ví dụ minh họa cho các kết quả trên, chúng tôi xét trường hợp đặc biệt $K = \mathbb{Q}(\sqrt{-6})$ vành các số nguyên đại số là

$D = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$. Mặc dù D không phải là vành Gauss, nhưng áp dụng lý thuyết trên chúng tôi xây dựng được số học trên vành D . Tính toán cụ thể các hàm chuẩn, hàm Euler trên D ; đưa ra thuật toán phân tích một phần tử của D thành tích các ideal tối đại và các ví dụ cụ thể.

TÀI LIỆU THAM KHẢO

Tiếng Việt

- 1 . Ngô Thúc Lanh - Đại số tuyến tính – NXB Giáo dục – 1970
- 2 . My Vinh Quang - Bài tập đại số đại cương – NXB Giáo dục – 1999
- 3 . Lại Đức Thịnh - Số luận - NXB Giáo dục – 1969

Tiếng Anh

- 1 . L.Fuchs – Abelian Groups Pergamon Press – Oxprd – London – NewYork – Pari – 1960
- 2 . Saban Alaca and Kenneth S. Williams Introductory Algebraic Number Theory – Cambridge University press – 2004
- 3 . Z.I Borevich and I.R Shafarevich – Number Theory – Academic Perss – 1989