

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

Nguyễn Phương Khanh

**SỰ PHÂN TÍCH THÀNH NHÂN TỬ 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

Thành phố Hồ Chí Minh - 2010

LỜI CẢM ƠN

Tôi xin chân thành bày tỏ lòng biết ơn đối với quý Thầy Cô giảng viên trường Đại học Sư Phạm Thành Phố Hồ Chí Minh, trường Đại học Khoa Học Tự Nhiên Thành Phố Hồ Chí Minh đã giảng dạy và trang bị cho tôi đầy đủ kiến thức làm nền tảng cho quá trình viết luận văn này.

Tôi xin chân thành cảm ơn quý Thầy Cô trong hội đồng chấm luận văn đã dành thời gian đọc, nhận xét 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 THPT Bình Chánh, trường THPT Phan Đăng Lưu đã giúp đỡ và tạo điều kiện thuận lợi cho tôi trong suốt khóa học.

Tôi xin chân thành tỏ lòng biết ơn đến gia đình, bạn bè, đồng nghiệp đã hỗ trợ và giúp đỡ rất nhiều để tôi hoàn thành luận văn này.

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

Trân trọng cảm ơn.

LỜI MỞ ĐẦU

Cho K là một trường mở rộng hữu hạn của Q và D là vành các số nguyên đại số trong K . Ta biết rằng D nói chung không phải là một miền nhân tử hóa. Cụ thể là trong D định lý cơ bản của số học có thể sẽ không còn đúng nữa, một số có thể phân tích được thành tích các phần tử nguyên tố theo nhiều cách khác nhau. Bởi vậy, số học trong vành D là khó nghiên cứu.

Tuy nhiên, dựa theo ý tưởng của Dedekind: “ Mỗi ideal thật sự của D đều có sự phân tích duy nhất thành tích của các ideal tối đại ”, chúng ta vẫn có thể xây dựng được số học trên vành các số nguyên đại số.

Bởi những lý do trên, chúng tôi đã quyết định chọn đề tài là: “ Sự phân tích thành nhân tử trên vành các số nguyên đại số”. Mục đích của luận văn này là nghiên cứu sự phân tích một ideal thành tích các ideal tối đại trong một số vành số nguyên đại số, từ đó xây dựng số học trên vành các số nguyên đại số này.

Bố cục của luận văn được chia làm 3 chương

Chương 1: CÁC KIẾN THỨC CƠ BẢN

Trong chương này chúng tôi trình bày các kiến thức cơ bản liên quan đến các đề tài : phần tử nguyên trên một miền, các ideal trong miền Dedekind, các khái niệm liên hợp trên một trường số đại số bậc n và thặng dư bậc hai.

Chương 2: CÁC IDEAL TRONG VÀNH CÁC SỐ NGUYÊN ĐẠI SỐ

Nội dung chính của chương này là nghiên cứu các tính chất của các ideal của vành các số nguyên đại số D ; chứng minh mọi ideal thật sự của D đều có thể biểu diễn dưới dạng tích của các ideal nguyên tố của D và sự biểu diễn này là duy nhất.

Chương 3 : SỰ PHÂN TÍCH MỘT IDEAL THÀNH TÍCH CÁC IDEAL NGUYÊN TỐ TRONG TRƯỜNG BẬC HAI

Mục đích của chương này là mô tả các ideal tối đại của vành D khi K là một trường bậc hai; mô tả thuật toán phân tích một phần tử của D thành tích các ideal tối đại. Từ đó áp dụng khảo sát một cách chi tiết trên vành

$$D = \{ a + b \cdot \sqrt{-10} \mid a, b \in \mathbb{Z} \} \text{ và } \text{vành } D = \{ a + b \cdot \frac{1+\sqrt{-15}}{2} \mid a, b \in \mathbb{Z} \}.$$

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

CHƯƠNG 1

CÁC KIẾN THỨC CƠ BẢN

1.1 PHẦN TỬ NGUYÊN TRÊN MỘT MIỀN

1.1.1 Định nghĩa

Cho A, B là các miền nguyên với $A \subseteq B$. Phần tử $b \in B$ được gọi là nguyên trên A nếu nó thỏa mãn phương trình đa thức

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0 \text{ với } a_0, a_1, \dots, a_{n-1} \in A$$

Như vậy mọi phần tử $a \in A$ đều nguyên trên A vì nó là nghiệm của $x - a \in A[x]$

1.1.2 Định nghĩa

Một số phức mà nguyên trên $\mathbb{Z}$ được gọi là một số nguyên đại số

Tập tất cả các số nguyên đại số kí hiệu là Ω

1.1.3 Định nghĩa

Cho A, B là các miền nguyên với $A \subseteq B$. Nếu mỗi $b \in B$ là nguyên trên A ta nói B là nguyên trên A

1.1.4 Tính chất

- Cho $A \subseteq B \subseteq C$ là tháp các miền nguyên. Nếu C là nguyên trên A thì C nguyên trên B
- Cho A, B là các miền nguyên với $A \subseteq B$ và B là một A -module hữu hạn sinh. Khi đó B nguyên trên A .
- Cho A, B là các miền nguyên với $A \subseteq B$; $b_1, b_2, \dots, b_n \in B$. Khi đó $b_1, b_2, \dots, b_n$ là nguyên trên $A \Leftrightarrow A[b_1, b_2, \dots, b_n]$ là một A -module hữu hạn sinh.
- Cho A, B là các miền nguyên với $A \subseteq B$. Nếu $b_1, b_2 \in B$ là nguyên trên A thì $b_1 + b_2$, $b_1 - b_2$ và $b_1 \cdot b_2$ là nguyên trên A

1.1.5 Định lý

Cho A, B là các miền nguyên với $A \subseteq B$. Khi đó tập các phần tử của B mà nguyên trên A là một miền nguyên con của B chứa A

1.1.6 Hệ quả

Tập tất cả các số nguyên đại số là một miền nguyên

1.1.7 Định nghĩa

Cho A, B là các miền nguyên với $A \subseteq B$. Ta gọi bao đóng nguyên của A trong B là một miền nguyên con của B bao gồm tất cả các phần tử của B mà nguyên trên A . Bao đóng nguyên của A trong B được kí hiệu là A^B .

Nếu K là trường các thương của A thì bao đóng nguyên của A trong K , kí hiệu A^K , được gọi là bao đóng nguyên của A .

Nếu $A^K = A$ thì ta nói A là vành đóng nguyên

1.1.18 Tính chất

Cho A, B là các miền nguyên với $A \subseteq B$. Khi đó $A \subseteq A^B \subseteq B$

1.2 Các ideal trong vành Dedekind

1.2.1 Định nghĩa

Một miền nguyên D thỏa 3 tính chất sau

- D là vành Noether
- D đóng nguyên
- Mọi ideal nguyên tố của D đều là ideal tối đại

được gọi là một vành Dedekind.

1.2.2 Mệnh đề

Cho P là một ideal thật sự của một miền nguyên D . Khi đó P là một ideal nguyên tố của D khi và chỉ khi với bất kỳ hai ideal A, B của D mà $AB \subset P$ thì hoặc $A \subset P$ hoặc $B \subset P$.

1.2.3 Định lý

Trong miền Noether, mọi ideal khác không đều chứa tích của một hoặc một số hữu hạn các ideal nguyên tố.

Chứng minh

Giả sử rằng trong miền Noether D có ideal không thỏa tính chất trên. Gọi S là tập các ideal này, do đó $S \neq \emptyset$. Do D là Noether nên trong S có phần tử tối đại A . Mặt khác, vì A không chứa tích của một hoặc một số hữu hạn các ideal nguyên tố nên chính A cũng không là một ideal nguyên tố. Theo mệnh đề

1.2.2 thì có các ideal B, C sao cho

$$BC \subset A; B \not\subset A; C \not\subset A$$

Ta đặt

$$B_1 = A + B, C_1 = A + C$$

thì

$$A \subset B_1, A \subset C_1; A \neq B_1, C_1$$

Do A là phần tử tối đại nên $B_1, C_1 \notin S$. Thế nên có các ideal nguyên tố $P_1, \dots, P_k$ sao cho

$$P_1, \dots, P_h \subseteq B_1, P_{h+1}, \dots, P_k \subseteq C_1$$

Nhưng vì

$$B_1 C_1 = (A + B)(A + C) \subseteq A$$

nên

$$P_1, \dots, P_k \subseteq A$$

Mâu thuẫn việc $A \in S$.

Vậy trong miền Noether, mọi ideal khác không đều chứa tích của một hoặc một số hữu hạn các ideal nguyên tố.

1.2.4 Hệ quả

Trong miền Dedekind, mọi ideal khác không đều chứa tích của một hoặc một số hữu hạn các ideal nguyên tố.

1.2.5 Định nghĩa

Cho vành Dedekind D và K là trường các thương của D . Một tập con A khác rỗng của K với 3 tính chất sau:

$$\text{i) } \alpha \in A, \beta \in A \Rightarrow \alpha + \beta \in A$$

$$\text{ii) } \alpha \in A, r \in D \Rightarrow r\alpha \in A$$

$$\text{iii) } \exists \gamma \in D, \gamma \neq 0 : \gamma A \subseteq D$$

được gọi là một ideal phân của D .

Nhận xét

1/ Nếu A là một ideal phân của D và $A \subset D$ thì A là một ideal của D .

2/ Nếu A là một ideal phân của D thì $I = \gamma A$ là một ideal của D và $A = \frac{I}{\gamma}$.

Như vậy mỗi ideal phân A của D đều viết được dưới dạng $A = \frac{I}{\gamma}$. Chú ý rằng cách viết này không duy nhất.

3/ Do D là vành Dedekind nên mọi ideal I của D đều hữu hạn sinh. Giả sử

$$I = \langle \alpha_1, \dots, \alpha_n \rangle$$

thì

$$A = \frac{1}{\gamma} I = \frac{1}{\gamma} \langle \alpha_1, \dots, \alpha_n \rangle = \left\langle \frac{\alpha_1}{\gamma}, \dots, \frac{\alpha_n}{\gamma} \right\rangle$$

Do đó mọi ideal phân của D cũng hữu hạn sinh

4/ Nếu A, B là các ideal phân của D thì $A = \frac{I}{\gamma}, B = \frac{J}{\delta}; \gamma, \delta \in D \setminus \{0\}$, khi đó

$A+B$ và AB là các ideal phân của D với mẫu số tương ứng là $\gamma\delta$.

1.2.6 Định lý

Cho vành Dedekind D và K là trường các thương của D . Với mỗi ideal nguyên tố P của D ta định nghĩa

$$C = \{ \alpha \in K \mid \alpha P \subseteq D \}$$

Khi đó $\tilde{P}$ là ideal phân của D .

1.2.7 Bổ đề

Cho P là một ideal nguyên tố của một vành Dedekind D . Khi đó

$$D \subset \tilde{P} \text{ và } D \neq \tilde{P}$$

Chứng minh

Để thấy $D \subseteq \tilde{P}$. Để kết luận $D \neq \tilde{P}$ ta cần chỉ ra rằng $\tilde{P}$ chứa phần tử $\gamma \in \tilde{P}$ nhưng $\gamma \notin D$.

Lấy $\beta \in P \setminus \{0\}$. Theo định lý 1.2.3 thì có các ideal nguyên tố $P_1, \dots, P_k$ ($k \geq 1$) mà

$$P_1 \dots P_k \subseteq \langle \beta \rangle$$

Chọn k là số nguyên dương nhỏ nhất thỏa điều kiện trên.

Do

$$P_1 \dots P_k \subseteq \langle \beta \rangle \subseteq P$$

và

P là một ideal nguyên tố

nên ta có

$$P_i \subseteq P; \text{ với chỉ số } i \text{ nào đó, } i \in \{1, 2, \dots, k\}$$

Có thể đánh số lại nếu cần thiết ta giả sử rằng

$$P_1 \subseteq P$$

Nhưng vì D là vành Dedekind nên P_1 là ideal tối đại, vì thế

$$P_1 = P$$

Bây giờ ta xét 2 trường hợp $k=1$ và $k \geq 2$.

+ Nếu $k = 1$ thì

$$P = P_1 = \langle \beta \rangle$$

Vì $\beta \neq 0$ ta có thể đặt $\gamma = \frac{1}{\beta} \in K$. Giả sử $\gamma \in D$, khi đó

$$1 = \beta \cdot \frac{1}{\beta} = \beta \cdot \gamma \in \langle \beta \rangle$$

$\Rightarrow P = \langle \beta \rangle = D$ mâu thuẫn việc P là một ideal nguyên tố của D .

Do đó $\gamma \notin D$.

Mặt khác

$$\gamma P = \frac{1}{\beta} \cdot \langle \beta \rangle = \langle 1 \rangle = D$$

$$\Rightarrow \gamma \in \tilde{P}$$

$$\Rightarrow \gamma \in \tilde{P} \setminus D \text{ khi } k=1.$$

+ Nếu $k \geq 2$, theo cách chọn k là số nguyên dương nhỏ nhất ta có

$$P_2 \dots P_k \not\subseteq \langle \beta \rangle$$

Do đó có phần tử $\delta \in P_2 \dots P_k$ nhưng $\delta \notin \langle \beta \rangle$.

Vì $\beta \neq 0$ ta có thể đặt $\gamma = \frac{\delta}{\beta} \in K$. Khi đó

. $\gamma \notin D$ vì nếu $\gamma \in D \Rightarrow \delta = \gamma \beta \in \langle \beta \rangle$ vô lý.

. $\gamma \in \tilde{P}$ vì $\gamma P = \delta \cdot \frac{1}{\beta} P_1 \subset \frac{1}{\beta} P_1 \cdot P_2 \dots P_k = \frac{1}{\beta} \cdot \langle \beta \rangle = \langle 1 \rangle$ hay $\gamma P \subset D$.

$\Rightarrow \gamma \in \tilde{P} \setminus D$ khi $k \geq 2$.

Vậy

$$D \neq \tilde{P}.$$

1.2.8 Bổ đề

$$\tilde{P} P = D$$

Chứng minh

+ Trước hết ta chứng minh $\tilde{P} P = D$ hay $\tilde{P} P = P$

Do P là ideal của D nên có thể xem là một ideal phân với mẫu số 1. Vì $\tilde{P}$ và P đều là ideal phân của D nên $\tilde{P} P$ là ideal phân của D . Hơn nữa, $\tilde{P} P \subset D$ nên là một ideal của D . Khi đó

Vì

$$. 1 \in \tilde{P} \Rightarrow P \subseteq \tilde{P} P$$

$$. \tilde{P} P \subset D$$

. P là ideal nguyên tố, D là vành Dedekind $\Rightarrow P$ là ideal tối đại

nên

$$\tilde{P} P = D \text{ hay } \tilde{P} P = P$$

+ Tiếp theo chúng ta chỉ ra $\tilde{P} P \neq P$

Giả sử rằng $\tilde{P} P = P$, ta chứng minh $\tilde{P}$ đóng với phép nhân. Lấy $\alpha \in \tilde{P}$,

$\beta \in \tilde{P}$, khi đó

$$\alpha P \subseteq \tilde{P} P = P, \beta P \subseteq \tilde{P} P = P$$

$$\Rightarrow \alpha \beta P \subseteq \alpha P \subseteq P$$

$$\Rightarrow \alpha \beta \in \tilde{P}$$

Do đó $\tilde{P}$ đóng với phép nhân. Điều này chứng tỏ $\tilde{P}$ là miền nguyên chứa D nghiêm ngặt. Vì D là vành Noether nên $\tilde{P}$ là một ideal phân hữu hạn sinh. Do vậy nên $\tilde{P}$ lại là một D -module hữu hạn sinh. Theo tính chất 1.1.4b) thì

$\tilde{P}$ nguyên trên D. Tuy nhiên, vì D dedekind nên D đóng nguyên. Từ đó ta có $\tilde{P} = D$. Vô lý vì $\tilde{P}$ chứa D một cách nghiêm ngặt.

Vậy $\tilde{P} P \neq P$ hay $\tilde{P} P = D$.

1.2.9 Định lý

Trong vành Dedekind D, mọi ideal A khác $\langle 0 \rangle$ và khác D đều phân tích được thành tích các ideal nguyên tố của D. Hơn nữa, sự phân tích này là duy nhất.

Chứng minh

+ Trước hết ta chứng minh sự phân tích được

Gọi S là tập các ideal khác $\langle 0 \rangle$ và khác D mà không phân tích được thành tích các ideal nguyên tố. Giả sử $S \neq \emptyset$, khi đó trong S có phần tử tối đại A vì D là vành Noether. Theo định lý 1.2.3 thì tồn tại các ideal nguyên tố $P_1, \dots, P_k$ ($k \geq 1$) sao cho

$$P_1 \dots P_k \subseteq A$$

Gọi k là số nguyên dương nhỏ nhất mà tích $P_1 \dots P_k \subseteq A$. Nếu $k = 1$ thì $P_1 \subseteq A \subset D$. Vì P_1 nguyên tố, D Dedekind nên P_1 tối đại. Như vậy $P_1 = A$ vô lý vì $A \in S$.

Do đó $k \geq 2$. Theo bổ đề 1.2.8 ta có

$$\tilde{P}_1 P_1 = D$$

$$\Rightarrow \tilde{P}_1 P_1 P_2 \dots P_k = D P_2 \dots P_k$$

$$\Rightarrow \tilde{P}_1 A \supseteq \tilde{P}_1 P_1 P_2 \dots P_k = P_2 \dots P_k (*)$$

Từ chứng minh của bổ đề 1.2.7 ta có $D \subset \tilde{P}_1$ cho nên $A = DA \subseteq \tilde{P}_1 A$

Lúc này, nếu $A = \tilde{P}_1 A$ thì từ (*) ta được $P_2 \dots P_k \subseteq A$ mâu thuẫn cách chọn k. Do vậy

$$A \subset \tilde{P}_1 A$$

Do tính tối đại của A trong S nên $\tilde{P}_1 A$ là ideal khác $\langle 0 \rangle$ và khác D không thuộc S. Ta có

$$\tilde{P}_1 A = Q_2 \dots Q_k,$$

với $Q_2, \dots, Q_k$ là các ideal nguyên tố của D

Lúc này ta thấy

$$A = AD = A \tilde{P}_1 P_1 = P_1 Q_2 \dots Q_k$$

là một tích các ideal nguyên tố, điều này mâu thuẫn cách chọn $A \in S$.

Vậy $S = \emptyset$ và sự phân tích được là hợp lý.

+ Ta chứng minh sự phân tích là duy nhất

Giả sử B là một ideal khác $\langle 0 \rangle$ và khác D có sự phân tích

$$B = P_1 \dots P_k = Q_1 \dots Q_l$$

với $P_1, \dots, P_k$, là các ideal nguyên tố.

$$\Rightarrow P_1 \dots P_k \subseteq Q_1$$

Vì Q_1 là ideal nguyên tố nên có $P_i \subseteq Q_1$, bằng cách đánh số lại nếu cần thiết ta giả sử $P_1 \subseteq Q_1$.

Do P_1 là ideal nguyên tố, D là vành Dedekind nên P_1 tối đại, từ đó suy ra

$$P_1 = Q_1$$

Do đó ta có

$$B \tilde{P}_1 = \tilde{P}_1 P_1 \dots P_k = P_2 \dots P_k$$

và

$$B \tilde{P}_1 = B \tilde{Q}_1 = Q_1 \dots Q_l$$

Suy ra

$$P_2 \dots P_k = Q_2 \dots Q_l$$

Nếu $k \neq l$, không mất tổng quát ta giả sử $k < l$. Bằng cách tương tự việc chứng minh $P_1 = Q_1$, ta cũng có $P_i = Q_i$; $i=2, \dots, k$. Ta có

$$P_2 \dots P_k = Q_2 \dots Q_k = Q_2 \dots Q_k \cdot Q_{k+1} \dots Q_l = P_2 \dots P_k Q_{k+1} \dots Q_l$$

$$\Rightarrow \tilde{P}_2 \dots \tilde{P}_k P_2 \dots P_k = \tilde{P}_2 \dots \tilde{P}_k P_2 \dots P_k Q_{k+1} \dots Q_l$$

$$\Rightarrow D = Q_{k+1} \dots Q_l \subset Q_l \text{ vô lý.}$$

Do đó $k = l$ và $P_i = Q_i$; $i=1, \dots, k$

Vậy sự phân tích một ideal khác $\langle 0 \rangle$ và khác D thành tích các ideal nguyên tố của D là duy nhất.

* Nhận xét

1/ Nếu A là một ideal thật sự của D thì A có sự phân tích

$$A = Q_1 \dots Q_l, \quad Q_1, \dots, Q_l \text{ là các ideal nguyên tố}$$

Gọi $P_1, \dots, P_n$ là tất cả các ideal nguyên tố phân biệt trong nhóm $Q_1, \dots, Q_l$. Giả sử mỗi P_i xuất hiện a_i lần, khi đó

$$A = P_1^{a_1} \dots P_n^{a_n}$$

với a_i là các số nguyên dương thỏa $a_1 + \dots + a_n = h$.

Nếu $A = D = \langle 1 \rangle$ thì $a_1 = \dots = a_n = 0$

Như vậy, mọi ideal khác $\langle 0 \rangle$ của D đều có thể biểu diễn dưới dạng tích của các lũy thừa các ideal nguyên tố của D.

2/ Giả sử A, B là các ideal khác $\langle 0 \rangle$ của vành Dedekind D. Khi đó AB cũng là một ideal khác $\langle 0 \rangle$ của D. Gọi $P_1, \dots, P_n$ là tất cả các ideal nguyên tố phân biệt xuất hiện trong sự phân tích của A, B hoặc AB. Khi đó

$$A = \prod_{i=1}^n P_i^{a_i}, \quad B = \prod_{i=1}^n P_i^{b_i}, \quad AB = \prod_{i=1}^n P_i^{c_i}$$

trong đó a_i, b_i, c_i là các số nguyên không âm.

Ta có

$$\prod_{i=1}^n P_i^{c_i} = AB = \prod_{i=1}^n P_i^{a_i} \prod_{i=1}^n P_i^{b_i} = \prod_{i=1}^n P_i^{a_i+b_i}$$

Do sự phân tích là duy nhất nên

$$c_i = a_i + b_i, i = 1, 2, \dots, n$$

Vậy nếu

$$A = \prod_{i=1}^n P_i^{a_i}, \quad B = \prod_{i=1}^n P_i^{b_i}$$

thì

$$AB = \prod_{i=1}^n P_i^{a_i+b_i}$$

1.2.10 Định nghĩa

Giả sử A, B là các ideal khác $\langle 0 \rangle$ của vành Dedekind D. Ta nói A là ước của B, kí hiệu $A|B$ nếu có ideal C của D sao cho $A.C = B$

Nhận xét:

Nếu

$$A = \prod_{i=1}^n P_i^{a_i} \text{ và } B = \prod_{i=1}^n P_i^{b_i}$$

thì

$$A|B \Leftrightarrow a_i \leq b_i; i = 1, \dots, n$$

1.2.11 Định lý

Tập tất cả các ideal phân khác không của vành Dedekind D với phép nhân lập thành một nhóm Abel với phần tử đơn vị là $\langle 1 \rangle = D$, phần tử nghịch đảo của

$$A = \prod_{i=1}^n P_i^{a_i}$$

là

$$A^{-1} = \prod_{i=1}^n P_i^{-a_i}$$

trong đó $P_i, i=1, \dots, n$ là các ideal nguyên tố phân biệt và $a_i, i=1, \dots, n$ là các số nguyên.

Chứng minh

+ Trước hết ta chứng minh mọi ideal phân khác $\langle 0 \rangle$ của D đều biểu diễn được dưới dạng tích của các lũy thừa của các ideal nguyên tố phân biệt của D. Giả sử A là ideal phân khác $\langle 0 \rangle$ của D.. Chọn $\alpha \in D \setminus \{0\}, \beta \in D \setminus \{0\}$ là hai mẫu số của ideal phân A. Khi đó

$$\langle \alpha \rangle A = B \text{ và } \langle \beta \rangle A = C$$

với B, C là các ideal khác $\langle 0 \rangle$ của D.

Giả sử rằng

$$\langle \alpha \rangle = \prod_{i=1}^n P_i^{r_i} \quad B = \prod_{i=1}^n P_i^{s_i}$$

$$\langle \beta \rangle = \prod_{i=1}^n P_i^{t_i} \quad C = \prod_{i=1}^n P_i^{u_i} \quad \text{với } P_1, \dots, P_n \text{ là các ideal nguyên tố phân biệt}$$

và r_i, s_i, t_i, u_i ($i = 1, \dots, n$) là các số nguyên không âm.

Khi đó, vì

$$\langle \alpha \rangle C = \langle \alpha \rangle (\langle \beta \rangle A) = \langle \beta \rangle (\langle \alpha \rangle A) = \langle \beta \rangle B$$

nên

$$\prod_{i=1}^n P_i^{r_i + u_i} = \prod_{i=1}^n P_i^{s_i + t_i}$$

Theo định lý 1.2.9 thì

$$r_i + u_i = s_i + t_i$$

hay

$$s_i - r_i = u_i - t_i; \quad i = 1, \dots, n$$

Do đó, ta có thể định nghĩa sự phân tích của ideal phân A khác $\langle 0 \rangle$ của D dưới dạng tích của các lũy thừa của các ideal nguyên tố phân biệt của D như sau

$$A = \prod_{i=1}^n P_i^{s_i - r_i}$$

và định nghĩa này hợp lý vì không phụ thuộc cách chọn mẫu số của A. Theo định nghĩa này, do với mọi ideal nguyên tố P của D ta đều có

$$\tilde{P}P = D = \langle 1 \rangle = P^0$$

nên

$$\tilde{P} = P^{-1}$$

Nếu $P_1, \dots, P_n$ là các ideal nguyên tố phân biệt mà

$$\prod_{i=1}^n P_i^{a_i} = \prod_{i=1}^n P_i^{b_i} \quad \text{với } a_i, b_i, i = 1, \dots, n \text{ là các số nguyên}$$

(nguyên âm, nguyên dương hoặc có thể bằng 0) thì khi đó

$$\left(\prod_{i=1}^n P_i^M \right) \prod_{i=1}^n P_i^{a_i} = \left(\prod_{i=1}^n P_i^M \right) \prod_{i=1}^n P_i^{b_i}$$

với M là một số nguyên thỏa $M + a_i > 0$ và $M + b_i > 0$, $i = 1, \dots, n$

Theo định lý 1.2.9 thì

$$M + a_i = M + b_i > 0; \quad i = 1, \dots, n$$

$$\Rightarrow a_i = b_i; \quad i = 1, \dots, n$$

Do đó ta có thể thấy sự biểu diễn của một ideal phân khác không dưới dạng tích của các lũy thừa của các ideal nguyên tố phân biệt, với số mũ nguyên, là duy nhất.

Bây giờ, trên tập các ideal phân khác $\langle 0 \rangle$ của D ta định nghĩa phép nhân như sau

Nếu

$$A = \prod_{i=1}^n P_i^{a_i}, B = \prod_{i=1}^n P_i^{b_i}$$

với $P_1, \dots, P_n$ là các ideal nguyên tố phân biệt và $a_i, b_i, i=1, \dots, n$ là các số nguyên (nguyên âm, nguyên dương hoặc có thể bằng 0) thì khi đó

$$AB = \prod_{i=1}^n P_i^{a_i+b_i}$$

Như vậy, tập tất cả các ideal phân khác không của vành Dedekind D với phép nhân trên lập thành một nhóm Abel với phần tử đơn vị là $\langle 1 \rangle = D$, phần tử nghịch đảo của

$$A = \prod_{i=1}^n P_i^{a_i}$$

là

$$A^{-1} = \prod_{i=1}^n P_i^{-a_i}$$

trong đó $P_i, i=1, \dots, n$ là các ideal nguyên tố phân biệt và $a_i, i=1, \dots, n$ là các số nguyên.

1.2.12 Định nghĩa

Cho $A = \prod_{i=1}^n P_i^{a_i}$ với $P_i, i=1, \dots, n$ là các ideal nguyên tố phân biệt của vành

Dedekind, $a_i (i=1, \dots, n)$ là các số nguyên.

Đặt

$$\text{ord}_{P_i}(A) = a_i$$

Với bất kỳ ideal nguyên tố $P \neq P_i, i=1, \dots, n$ ta định nghĩa

$$\text{ord}_P(A) = 0$$

Nhận xét

— A được gọi là một ideal nguyên của D khi và chỉ khi $\text{ord}_P(A) \geq 0$; với mọi ideal nguyên tố P .

— Nếu $\text{ord}_P(A) = 0$; với mọi ideal nguyên tố P thì $A = D$.

— $\text{ord}_P(\langle 1 \rangle) = 0$ và $\text{ord}_P(P^k) = k$

— Tập tất cả các ideal nguyên và ideal phân khác không của vành Dedekind D với phép nhân lập thành một nhóm Abel với phần tử đơn vị là $\langle 1 \rangle = D$, phần tử nghịch đảo của

$$A = \prod_{i=1}^n P_i^{a_i}$$

là

$$A^{-1} = \prod_{i=1}^n P_i^{-a_i}$$

trong đó $P_i, i=1, \dots, n$ là các ideal nguyên tố phân biệt và $a_i, i=1, \dots, n$ là các số nguyên.

1.2.13 Định nghĩa

Cho A, B là các ideal phân khác không của vành D . Ta nói A là ước của B , kí hiệu $A|B$ nếu có ideal nguyên C của D sao cho

$$B = AC$$

Nhận xét

$$A|B \Leftrightarrow \text{ord}_P(A) \leq \text{ord}_P(B) \text{ với mọi ideal tố } P \Leftrightarrow B \subseteq A$$

1.2.14 Tính chất

- i) $\text{ord}_P(AB) = \text{ord}_P(A) + \text{ord}_P(B)$
- ii) $\text{ord}_P(A+B) = \min \{ \text{ord}_P(A), \text{ord}_P(B) \}$

1.2.15 Định nghĩa

Cho K là trường các thương của vành Dedekind D . Với mỗi $\alpha \in K \setminus \{0\}$ ta định nghĩa

$$\text{ord}_P(\alpha) = \text{ord}_P(\langle \alpha \rangle)$$

với mọi ideal nguyên tố P của D .

1.2.16 Tính chất

- a) $\alpha \in A \Leftrightarrow \text{ord}_P(\alpha) \geq \text{ord}_P(A)$, với mọi ideal nguyên tố P của D .
- b) với $\alpha \in K^*, \beta \in K^*$ thì

$$\text{ord}_P(\alpha\beta) = \text{ord}_P(\alpha) + \text{ord}_P(\beta)$$
- c) với $\alpha, \beta, \alpha + \beta \in K^*$ thì

$$\text{ord}_P(\alpha + \beta) \geq \min \{ \text{ord}_P(\alpha), \text{ord}_P(\beta) \}$$
- d) với $\alpha, \beta, \alpha + \beta \in K^*$ thỏa $\text{ord}_P(\alpha) \neq \text{ord}_P(\beta)$ thì

$$\text{ord}_P(\alpha + \beta) = \min \{ \text{ord}_P(\alpha), \text{ord}_P(\beta) \}$$

1.2.17 Định lý

Cho K là trường các thương của vành Dedekind D . Khi đó, với bất kỳ tập hữu hạn các ideal nguyên tố $P_1 \dots P_k$ của D cùng tập các số nguyên tương ứng $a_1, \dots, a_k$ luôn tồn tại $\alpha \in K$ sao cho

$$i/ \text{ord}_{P_i}(\alpha) = a_i, i=1, \dots, k$$

$$ii/ \text{ord}_P(\alpha) \geq 0, \text{ với mọi ideal nguyên tố } P \neq P_1 \dots P_k$$

1.2.18 Định nghĩa

Cho K là trường các thương của vành Dedekind D và A là một ideal nguyên hoặc ideal phân khác không của D . Khi đó với $a, b, c \in A$ ta viết

$$a \equiv b \pmod{A} \Leftrightarrow A \mid \langle a-b \rangle$$

Nhận xét

$$i/ A \mid \langle a-b \rangle \Leftrightarrow \langle a-b \rangle \subseteq A \Leftrightarrow a-b \in A \Leftrightarrow a + A = b + A$$

$$ii/ a \equiv a \pmod{A}$$

$$iii/ a \equiv b \pmod{A} \Rightarrow b \equiv a \pmod{A}$$

$$iv/ a \equiv b \pmod{A}, b \equiv c \pmod{A} \Rightarrow a \equiv c \pmod{A}$$

$$v/ a \equiv b \pmod{A} \Rightarrow ac \equiv bc \pmod{A}$$

1.2.19 Định lý

Cho D là vành Dedekind

a) Cho $P_1, \dots, P_n$ là các ideal nguyên tố phân biệt của D ; $\alpha_1, \dots, \alpha_n \in D$

và $a_1, \dots, a_n$ là các số nguyên dương. Khi đó tồn tại $\alpha \in D$ thỏa

$$\alpha \equiv \alpha_i \pmod{P_i^{a_i}}; i=1, \dots, n$$

b) Cho $I_1, \dots, I_n$ là các ideal của D đôi một nguyên tố cùng nhau

và $\alpha_1, \dots, \alpha_n \in D$. Khi đó tồn tại $\alpha \in D$ thỏa

$$\alpha \equiv \alpha_i \pmod{I_i}; i=1, \dots, n$$

1.2.20 Định lý

Cho D là vành Dedekind và A là một ideal nguyên hoặc phân của D . Khi đó A được sinh bởi nhiều nhất hai phần tử.

1.3 Các khái niệm liên hợp trên một trường số đại số bậc n **1.3.1 Định lý**

Cho K là một mở rộng bậc n trên Q ($[K:Q] = n$). Khi đó có đúng n đơn cấu trường

$$\sigma_k : K \rightarrow C (k=1, \dots, n)$$

1.3.2 Định nghĩa

Cho $\alpha \in K$ kí hiệu là $\text{irr}_Q(\alpha)$ là đa thức tối tiểu của α trên Q

$$\text{irr}_Q(\alpha) = x^k + a_{k-1}x^{k-1} + \dots + a_1x + a_0; a_0, a_1, \dots, a_{k-1} \in Q$$

Cho $\alpha \in K$ với K là một trường số đại số bậc n trên Q . Nếu $[Q(\alpha):Q] = k$ ta nói α là một số đại số bậc k , khi đó

$$\text{irr}_Q(\alpha) = x^k + a_{k-1}x^{k-1} + \dots + a_1x + a_0 = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_k)$$

có k nghiệm và tất cả các nghiệm này đều gọi là các phân tử liên hợp của α trên Q .

Số phân tử liên hợp $= k \leq n$

Ta gọi

$\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_n(\alpha)$ là tập các K -liên hợp đầy đủ của α trên Q và đa thức

$$\text{fld}_K(\alpha) = \prod_{k=1}^n (x - \sigma_k(\alpha))$$

là đa thức trường của phân tử α trên K .

1.3.3 Tính chất

Cho $\alpha \in K$ với K là một trường số đại số bậc n trên Q . Khi đó

a) $\text{fld}_K(\alpha) \in Q[x]$

b) $\text{fld}_K(\alpha) = (\text{irr}_Q(\alpha))^s$ với $s = \frac{n}{\deg(\text{irr}_Q(\alpha))}$

c) $\alpha \in O_K$ thì $\text{fld}_K(\alpha) \in Z[x]$

d) $\alpha \in O_K$ thì tất cả các K -liên hợp của α là những số nguyên đại số.

e) Tất cả các K -liên hợp của α bằng nhau khi và chỉ khi $\alpha \in Q$.

f) Tất cả các K -liên hợp của α đôi một khác nhau khi và chỉ khi $K = Q(\alpha)$

1.3.4 Định nghĩa

Cho K là một trường số đại số bậc n trên Q

Cho

$\omega_1, \dots, \omega_n$ là n phân tử của K ;

$\sigma_k : K \rightarrow C (k = 1, \dots, n)$ là n đơn cấu trường

Với mỗi $i=1, \dots, n$ ta kí hiệu

$$\omega_i^{(1)} = \sigma_1(\omega_i) = \omega_i, \omega_i^{(2)} = \sigma_2(\omega_i), \dots, \omega_i^{(n)} = \sigma_n(\omega_i)$$

là các liên hợp của ω trên K .

Khi đó ta định nghĩa

$$D(\omega_1, \omega_2, \dots, \omega_n) = \left(\begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \dots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \dots & \omega_n^{(2)} \\ \vdots & \vdots & \dots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \dots & \omega_n^{(n)} \end{vmatrix} \right)^2$$

Và với $\alpha \in K$ ta kí hiệu

$$D(\alpha) = D(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) = \left(\begin{array}{cccc} 1 & \alpha^{(1)} & \dots & (\alpha^{(1)})^{n-1} \\ 1 & \alpha^{(2)} & \dots & (\alpha^{(2)})^{n-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \alpha^{(n)} & \dots & (\alpha^{(n)})^{n-1} \end{array} \right)^2$$

1.3.5 Tính chất

- a) $D(\alpha) = \prod_{1 \leq i < j \leq n} (\alpha^{(i)} - \alpha^{(j)})^2$ với $\alpha^{(1)} = \alpha, \alpha^{(2)}, \dots, \alpha^{(n)}$ là các liên hợp của α trên K .
- b) $K = Q(\alpha) \Leftrightarrow D(\alpha) \neq 0$

1.3.6 Định lý

Cho K là một trường số đại số bậc n trên Q . Khi đó

- a) Nếu $\omega_1, \dots, \omega_n \in K$ thì $D(\omega_1, \dots, \omega_n) \in Q$
- b) Nếu $\omega_1, \dots, \omega_n \in O_K$ thì $D(\omega_1, \dots, \omega_n) \in Z$
- c) Nếu $\omega_1, \dots, \omega_n \in K$ thì khi đó
- $$D(\omega_1, \dots, \omega_n) \neq 0 \Leftrightarrow \omega_1, \dots, \omega_n \text{ độc lập tuyến tính trên } Q.$$

1.4 THẶNG DƯ BẬC HAI

1.4.1 Định nghĩa

Cho p là một số nguyên tố lẻ. Xét phương trình

$$x^2 \equiv a \pmod{p}; (a, p) = 1 \quad (1).$$

Khi đó

+ Nếu phương trình (1) có nghiệm thì ta nói a là thặng dư bậc hai theo modun p .

+ 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 Legendre)

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

1.4.2 Tính chất

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

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

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

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

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

f) Nếu p và q là 2 số nguyên tố lẻ phân biệt thì ta có

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

Ta kết thúc chương này với định lý sau

1.4.5 Định lý

Cho G là nhóm Abel tự do với cơ sở $\omega_1, \omega_2, \dots, \omega_n$ sao cho mỗi phần tử của C đều biểu diễn được dưới dạng

$$x_1 \omega_1 + x_2 \omega_2 + \dots + x_n \omega_n; \quad x_1, x_2, \dots, x_n \in \mathbb{Z}$$

Nếu H là nhóm con của G với cơ sở $\eta_1, \eta_2, \dots, \eta_n$ hay

$$H = \{ y_1 \eta_1 + y_2 \eta_2 + \dots + y_n \eta_n \mid y_1, y_2, \dots, y_n \in \mathbb{Z} \}$$

Với mỗi $\eta_i \in H \subseteq G$ ta có

$$\eta_i = \sum_{j=1}^n c_{ij} \omega_j; \quad i=1, 2, \dots, n; \quad c_{ij} \in \mathbb{Z}$$

Đặt

$$C = [c_{ij}] \in M_n(\mathbb{Z})$$

Khi đó

$$[G:H] = |\det C|$$

CHƯƠNG 2

CÁC IDEAL TRONG VÀNH CÁC SỐ NGUYÊN ĐẠI SỐ

Ta kí hiệu K là một mở rộng bậc n của Q , $[K:Q] = n$,
 $D = O_K = \Omega \cap K$ là vành các số nguyên đại số của K .

2.1 Cơ sở của một ideal

2.1.1 Mệnh đề

Mỗi phần tử đại số α đều viết được dưới dạng $\alpha = \frac{\beta}{c}$ với β là số nguyên đại số ($\beta \in \Omega$) và c là số nguyên hữu tỷ ($c \in Z$)

Chứng minh

Do α là phần tử đại số nên α là nghiệm của một đa thức đơn khởi với hệ số trong Q , do đó

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0 \text{ với } a_0, a_1, \dots, a_{n-1} \in Q$$

$$\Rightarrow \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$$

Gọi $c \in Z$ là mẫu chung của tất cả a_i

$$\text{Do } c^n \cdot (\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0) = 0$$

$$\Rightarrow (c\alpha)^n + c \cdot a_{n-1} (c\alpha)^{n-1} + \dots + c^n a_0 = 0$$

$$\Rightarrow \beta^n + c \cdot a_{n-1} \beta^{n-1} + \dots + c^n a_0 = 0 ; \text{ với } \beta = c \cdot \alpha$$

$$\Rightarrow \beta \text{ là số nguyên đại số và } \alpha = \frac{\beta}{c}$$

2.1.2 Định lý

i/ Trường các thương của D chính là K

ii/ D là vành đóng nguyên

Chứng minh

i/ Gọi F là trường các thương của D

+ Ta chứng minh $F \subset K$: lấy $x = \frac{a}{b} \in F$; $a, b \in D$. Do $D \subset K$ và K là một

trường nên $x = \frac{a}{b} \in K \Rightarrow F \subset K$

+ Ta chứng minh $K \subset F$: lấy $\alpha \in K \Rightarrow \alpha$ là phần tử đại số $\Rightarrow \alpha = \frac{\beta}{c}$ với

$\beta \in \Omega, c \in Z$

Vì:

. $c \in Z \subset D$ nên $c \in D$

. $\beta = \alpha \cdot c \in \Omega \cap K = D \Rightarrow \beta \in D$

Nên:

$$\alpha = \frac{\beta}{c} \in F$$

$$\Rightarrow K \subset F$$

Vậy $F = K$

ii/ D là vành đóng nguyên

Lấy $\alpha \in D^K \Rightarrow \alpha$ nguyên trên D

Mà D nguyên trên Z

$\Rightarrow \alpha$ nguyên trên Z

$\Rightarrow \alpha \in \Omega$

Hơn nữa $\alpha \in K$

$\Rightarrow \alpha \in \Omega \cap K = D \Rightarrow \alpha \in D$

$\Rightarrow D^K \subset D$

Hiển nhiên $D \subset D^K$

$\Rightarrow D^K = D$

Vậy D là vành đóng nguyên

2.1.3 Bổ đề

Mọi ideal $I \neq \{0\}$ của D đều chứa ít nhất một số nguyên hữu tỉ khác không

Chứng minh

Lấy $\alpha \in I, \alpha \neq 0$. Do $\text{Irr}(\alpha) \in Z[x]$ nên có $c_0, c_1, \dots, c_{k-1} \in Z$ sao cho

$$\alpha^k + c_{k-1} \alpha^{k-1} + \dots + c_1 \alpha + c_0 = 0$$

Ta thấy

. nếu $k=1$

$\Rightarrow c_1 \alpha + c_0 = 0 \Rightarrow \alpha + c_0 = 0$ (vì $\text{Irr}(\alpha)$ đơn khởi)

$\Rightarrow c_0 = -\alpha \neq 0$

. nếu $k > 1$, giả sử $c_0 = 0$ thì dẫn đến $\alpha = 0$ là một nghiệm của $\text{Irr}(\alpha)$

$\Rightarrow c_0 \neq 0$

Do đó

$$c_0 = -(\alpha^k + c_{k-1} \alpha^{k-1} + \dots + c_1 \alpha) \neq 0$$

Hơn nữa

$$-(\alpha^k + c_{k-1} \alpha^{k-1} + \dots + c_1 \alpha) \in I$$

$\Rightarrow c_0 \in I \cap Z$

Vậy $I \cap Z \neq \{0\}$.

2.1.4 Bổ đề

Nếu K là một trường số đại số thì có một số nguyên đại số θ sao cho

$$K = Q(\theta).$$

Chứng minh

Do K là một trường số đại số nên có một số đại số ϕ thỏa $K = Q(\phi)$.

Theo mệnh đề 2.1.1 thì $\phi = \frac{\theta}{b}$ với $\theta \in \Omega$, $b \in Z$.

Vậy thì $K = Q(\phi) = Q(\frac{\theta}{b}) = Q(\theta)$, vì $\frac{1}{b} \in Q$.

2.1.5 Bổ đề

Cho $I \neq \{0\}$ là một ideal của D . Khi đó tồn tại $\gamma \in I$ sao cho $K = Q(\gamma)$.

Chứng minh

Chọn $\theta \in D$ sao cho $K = Q(\theta)$. Do θ là một phân tử đại số nên có dạng

$$\theta = \frac{\alpha}{a} \text{ với } \alpha \in D, a \in Z$$

Theo bổ đề 2.1.3 có $b \in I \cap Z \neq \{0\}$, do đó $\gamma = \alpha \cdot b$ thì $\gamma \in I$

$$\text{Xét } Q(\gamma) = Q(\alpha b) = Q(\frac{\theta a}{b}) = Q(\theta) \text{ vì } \frac{a}{b} \in Q$$

Vậy $K = Q(\gamma)$, $\gamma \in I$.

2.1.6 Bổ đề

Giả sử K là một trường số đại số với $[K:Q] = n$, gọi $I \neq \{0\}$ là một ideal trong D . Khi đó tồn tại $\eta_1, \dots, \eta_n \in I$ sao cho $D(\eta_1, \dots, \eta_n) \neq 0$.

Chứng minh

Theo bổ đề 2.1.4 ta có $K = Q(\theta)$, với $\theta \in D$. Do $I \neq \{0\}$ là một ideal của D , theo bổ đề 2.1.3 thì có $c \in I \cap Z$, $c \neq \{0\}$. Đặt

$$\eta_1 = c, \eta_2 = c\theta, \dots, \eta_n = c\theta^{n-1}$$

thì

$$\eta_1, \dots, \eta_n \in I \text{ vì } I \text{ là ideal của } D.$$

Hơn nữa

$$D(\eta_1, \dots, \eta_n) = D(c, c\theta, \dots, c\theta^{n-1}) = c^{2n} \cdot D(1, \theta, \dots, \theta^{n-1}) = c^{2n} \cdot D(\theta) \neq 0.$$

2.1.7 Định lý

Giả sử K là một trường số đại số với $[K:Q] = n$, gọi $I \neq \{0\}$ là một ideal trong D . Khi đó tồn tại $\eta_1, \dots, \eta_n \in I$ sao cho mỗi phân tử $\alpha \in I$ đều có thể được biểu diễn duy nhất dưới dạng $\alpha = x_1\eta_1 + \dots + x_n\eta_n$; $x_i \in Z$.

Chứng minh

Do I là ideal khác không của D , theo bổ đề 2.1.6 thì tồn tại $\eta_1, \dots, \eta_n \in I$ sao cho $D(\eta_1, \dots, \eta_n) \neq 0$. Vì $\eta_1, \dots, \eta_n \in D$ nên $D(\eta_1, \dots, \eta_n) \in Z$. Do đó $|D(\eta_1, \dots, \eta_n)|$ là một số nguyên dương. Ta đặt

$$S = \{ |D(\eta_1, \dots, \eta_n)| \mid \eta_1, \dots, \eta_n \in I, D(\eta_1, \dots, \eta_n) \neq 0 \}$$

Với cách đặt trên thì rõ ràng S là tập khác rỗng các số nguyên dương, và như vậy nên S chứa phần tử nhỏ nhất, ta gọi phần tử đó là

$$|D(\eta_1, \dots, \eta_n)|, \eta_1, \dots, \eta_n \in I.$$

Vì $D(\eta_1, \dots, \eta_n) \neq 0$ nên $\{\eta_1, \dots, \eta_n\}$ là một cơ sở của không gian vector K trên Q .

Khi đó với $\alpha \in I$ thì có duy nhất $x_1, \dots, x_n \in \mathbb{Q}$ thỏa $\alpha = x_1\eta_1 + \dots + x_n\eta_n$.

Bây giờ ta giả sử rằng có $x_i \in \{x_1, \dots, x_n\}$ không là số nguyên, bằng cách đánh số lại $\eta_1, \dots, \eta_n$, nếu cần thiết, chúng ta giả sử $x_1 \notin \mathbb{Z}$. Khi đó có duy nhất $l \in \mathbb{Z}$ thỏa

$$l < x_1 < l+1$$

Đặt $\gamma = \alpha - l\eta_1$

Vì $\alpha \in I$ và $\eta_1 \in I$ nên $\gamma \in I$, hơn nữa

$$\gamma = (x_1 - l)\eta_1 + x_2\eta_2 + \dots + x_n\eta_n$$

Tác động n đơn cấu trường σ_k ($k = 1, 2, \dots, n$) vào phương trình trên ta được

$$\begin{cases} \gamma^{(1)} = (x_1 - l)\eta_1^{(1)} + x_2\eta_2^{(1)} + \dots + x_n\eta_n^{(1)} \\ \gamma^{(2)} = (x_1 - l)\eta_1^{(2)} + x_2\eta_2^{(2)} + \dots + x_n\eta_n^{(2)} \\ \gamma^{(n)} = (x_1 - l)\eta_1^{(n)} + x_2\eta_2^{(n)} + \dots + x_n\eta_n^{(n)} \end{cases}$$

trong đó

$$\gamma^{(1)} = \gamma, \gamma^{(2)}, \dots, \gamma^{(n)} \text{ là các K liên hợp của } \gamma$$

và

$$\eta_i^{(1)} = \eta_i, \eta_i^{(2)}, \dots, \eta_i^{(n)} \text{ là các K liên hợp của } \eta_i \text{ (} i = 1, 2, \dots, n \text{)}.$$

Bằng phương pháp Cramer ta được

$$x_1 - l = \frac{\begin{vmatrix} \gamma^{(1)}\eta_2^{(1)} & \dots & \eta_n^{(1)} \\ \gamma^{(2)}\eta_2^{(2)} & \dots & \eta_n^{(2)} \\ \vdots & \ddots & \vdots \\ \gamma^{(n)}\eta_2^{(n)} & \dots & \eta_n^{(n)} \end{vmatrix}}{\begin{vmatrix} \eta_1^{(1)}\eta_2^{(1)} & \dots & \eta_n^{(1)} \\ \eta_1^{(2)}\eta_2^{(2)} & \dots & \eta_n^{(2)} \\ \vdots & \ddots & \vdots \\ \eta_1^{(n)}\eta_2^{(n)} & \dots & \eta_n^{(n)} \end{vmatrix}}$$

Do đó

$$(x_1 - l)^2 = \frac{D(\gamma, \eta_2, \dots, \eta_n)}{D(\eta_1, \eta_2, \dots, \eta_n)}$$

$$\Rightarrow 0 < |D(\gamma, \eta_2, \dots, \eta_n)| = (x_1 - l)^2 |D(\eta_1, \eta_2, \dots, \eta_n)| < |D(\eta_1, \eta_2, \dots, \eta_n)|$$

Điều này mâu thuẫn cách chọn $|D(\eta_1, \dots, \eta_n)|$.

Như vậy, tất cả x_i đều là số nguyên và mỗi phần tử $\alpha \in I$ đều có thể được biểu diễn duy nhất dưới dạng $\alpha = x_1\eta_1 + \dots + x_n\eta_n$; $x_i \in \mathbb{Z}$.

2.1.8 Định nghĩa

Cho K là một trường số đại số bậc n , I là một ideal khác không của D . Nếu $\{\eta_1, \dots, \eta_n\}$ là tập các phần tử của I sao cho mỗi phần tử $\alpha \in I$ đều có thể biểu diễn duy nhất dưới dạng $\alpha = x_1\eta_1 + \dots + x_n\eta_n$, ($x_1, \dots, x_n \in \mathbb{Z}$) thì $\{\eta_1, \dots, \eta_n\}$ được gọi là một cơ sở của ideal I .

2.1.9 Định lý

Cho I là một ideal khác không của D . Khi đó

a) Nếu $\{\eta_1, \dots, \eta_n\}$ và $\{\lambda_1, \dots, \lambda_n\}$ là hai cơ sở của I thì

$$D(\eta_1, \dots, \eta_n) = D(\lambda_1, \dots, \lambda_n) \text{ và } \eta_i = \sum_{j=1}^n c_{ij}\lambda_j, i = 1, 2, \dots, n$$

với c_{ij} ($i, j = 1, 2, \dots, n$) $\in \mathbb{Z}$ sao cho $\det(c_{ij}) = \pm 1$

b) Nếu $\{\eta_1, \dots, \eta_n\}$ là cơ sở của I và $\lambda_1, \dots, \lambda_n \in I$ sao cho

$$D(\eta_1, \dots, \eta_n) = D(\lambda_1, \dots, \lambda_n) \text{ thì } \{\lambda_1, \dots, \lambda_n\} \text{ là cơ sở của } I.$$

Chứng minh

a) Vì $\{\lambda_1, \dots, \lambda_n\}$ là cơ sở của I ta có

$$I = \mathbb{Z}\lambda_1 + \dots + \mathbb{Z}\lambda_n$$

Do $\eta_1, \dots, \eta_n \in I$ nên có $c_{ij} \in \mathbb{Z}$ ($i, j = 1, 2, \dots, n$) sao cho

$$\eta_i = \sum_{j=1}^n c_{ij}\lambda_j, i = 1, 2, \dots, n (*)$$

Vì $\{\eta_1, \dots, \eta_n\}$ là cơ sở của I ta cũng có

$$I = \mathbb{Z}\eta_1 + \dots + \mathbb{Z}\eta_n$$

Do $\lambda_1, \dots, \lambda_n \in I$ nên có $d_{ij} \in \mathbb{Z}$ ($i, j = 1, 2, \dots, n$) sao cho

$$\lambda_j = \sum_{k=1}^n d_{jk}\eta_k, j = 1, 2, \dots, n$$

Như vậy, với mỗi $i = 1, 2, \dots, n$ ta có

$$\eta_i = \sum_{j=1}^n c_{ij}\lambda_j = \sum_{j=1}^n c_{ij} \sum_{k=1}^n d_{jk}\eta_k = \sum_{k=1}^n \left(\sum_{j=1}^n (c_{ij}d_{jk}) \right) \eta_k$$

Vì $\{\eta_1, \dots, \eta_n\}$ là cơ sở của I , $\eta_1, \dots, \eta_n$ độc lập tuyến tính trên Q nên

$$\sum_{j=1}^n c_{ij}d_{jk} = \begin{cases} 1, & \text{khi } i = k \\ 0, & \text{khi } i \neq k \end{cases}$$

Đặt C và D là các ma trận $n \times n$ với $C = [c_{ij}]$, $D = [d_{ij}]$. Khi đó

$$C.D = I_n, I_n \text{ là ma trận đơn vị cấp } n.$$

Vậy

$$\det(C). \det(D) = \det(CD) = \det(I_n) = 1$$

Vì $\det(C), \det(D) \in Z$ nên $\det(C) = \det(D) = \pm 1$.

Từ (*) ta suy ra

$$\begin{aligned} D(\eta_1, \dots, \eta_n) &= (\det(c_{ij}))^2 \cdot D(\lambda_1, \dots, \lambda_n) \\ &= (\det(C))^2 \cdot D(\lambda_1, \dots, \lambda_n) = D(\lambda_1, \dots, \lambda_n) \end{aligned}$$

Do đó

$$D(\eta_1, \dots, \eta_n) = (\pm 1)^2 \cdot D(\lambda_1, \dots, \lambda_n) = D(\lambda_1, \dots, \lambda_n)$$

Ta chứng minh xong phần a)

b) Vì $\{\eta_1, \dots, \eta_n\}$ là cơ sở của I và $\lambda_1, \dots, \lambda_n \in I$ nên có $d_{ij} \in Z$ ($i, j = 1, 2, \dots, n$) sao cho

$$\lambda_i = \sum_{j=1}^n d_{ij} \eta_j, \quad (i = 1, 2, \dots, n)$$

Do đó

$$D(\lambda_1, \dots, \lambda_n) = (\det(d_{ij}))^2 D(\eta_1, \dots, \eta_n)$$

Vì $D(\lambda_1, \dots, \lambda_n) = D(\eta_1, \dots, \eta_n)$ ta được $(\det(d_{ij}))^2 = 1$

$$\Rightarrow \det(d_{ij}) = \pm 1$$

Như vậy ma trận $D = (d_{ij})$ có một nghịch đảo là

$$D^{-1} = C = (c_{ij}), \quad c_{ij} \in Z$$

và

$$\eta_i = \sum_{j=1}^n c_{ij} \lambda_j, \quad i = 1, 2, \dots, n.$$

Lấy $\alpha \in I$. Khi đó, vì $\{\eta_1, \dots, \eta_n\}$ là cơ sở của I nên có

$$a_1, \dots, a_n \in Z$$

$$\text{mà } \alpha = \sum_{i=1}^n a_i \eta_i$$

$$\Rightarrow \alpha = \sum_{i=1}^n a_i \eta_i = \sum_{i=1}^n a_i \sum_{j=1}^n c_{ij} \lambda_j = \sum_{j=1}^n \left(\sum_{i=1}^n a_i c_{ij} \right) \lambda_j$$

trong đó mỗi $\sum_{i=1}^n a_i c_{ij} \in Z$ ($j=1, 2, \dots, n$).

Điều này chứng tỏ mỗi phần tử $\alpha \in I$ đều có thể được biểu diễn dưới dạng

$$\alpha = b_1 \lambda_1 + \dots + b_n \lambda_n, \quad b_1, \dots, b_n \in Z$$

Bây giờ ta có thể giả sử α được biểu diễn theo dạng trên dưới 2 trường hợp

$$\alpha = b_1 \lambda_1 + \dots + b_n \lambda_n = b'_1 \lambda_1 + \dots + b'_n \lambda_n, \quad b'_1, \dots, b'_n \in Z$$

Do đó

$$e_1 \lambda_1 + \dots + e_n \lambda_n = 0, \quad \text{với } e_i = b_i - b'_i \in Z \quad (i=1, 2, \dots, n)$$

Nếu có $e_i \neq 0$ thì $\lambda_1, \dots, \lambda_n$ phụ thuộc tuyến tính trên Q và theo định lý 1.3.6.c thì

$$D(\lambda_1, \dots, \lambda_n) = 0$$

Do đó

$$D(\eta_1, \dots, \eta_n) = D(\lambda_1, \dots, \lambda_n) = 0$$

$\Rightarrow \eta_1, \dots, \eta_n$ phụ thuộc tuyến tính trên Q , điều này mâu thuẫn $\{\eta_1, \dots, \eta_n\}$ là cơ sở của I .

Do đó

$$e_i = b_i - b'_i = 0 \quad (i=1, 2, \dots, n)$$

$$\Rightarrow b_i = b'_i \quad (i=1, 2, \dots, n)$$

Điều này chứng tỏ sự biểu diễn của mỗi phần tử $\alpha \in I$ dưới dạng

$$\alpha = b_1\lambda_1 + \dots + b_n\lambda_n, \quad b_1, \dots, b_n \in Z$$

là duy nhất.

Vậy $\{\lambda_1, \dots, \lambda_n\}$ là cơ sở của I .

Định lý đã được chứng minh.

2.1.10 Định nghĩa

Cho I là một ideal khác không của D . Gọi $\{\eta_1, \dots, \eta_n\}$ là một cơ sở của I . Khi đó định thức $D(I)$ của I là một số nguyên khác không được cho bởi

$$D(I) = D(\eta_1, \dots, \eta_n)$$

2.2 Sự phân tích thành tích các ideal nguyên tố trong vành D

Trước hết ta có định lý sau

2.2.1 Định lý

D là một vành Noether.

Chứng minh

Giả sử I là một ideal của D . Khi đó, nếu $I = \{0\}$ thì $I = \langle 0 \rangle$ là hữu hạn sinh. Nếu $I \neq \{0\}$ thì theo định lý 2.1.7, tồn tại $\eta_1, \dots, \eta_n \in I$ sao cho mỗi phần tử $\alpha \in I$ đều có thể được biểu diễn duy nhất dưới dạng $\alpha = x_1\eta_1 + \dots + x_n\eta_n$; $x_i \in Z$, do đó I cũng hữu hạn sinh. Vậy D là một vành Noether.

2.2.2 Định lý

Trong vành D , mọi ideal nguyên tố P đều là ideal tối đại.

Chứng minh

Giả sử rằng khẳng định của định lý sai. Khi đó có ideal nguyên tố P_1 của D không là một ideal tối đại. Gọi S là tập tất cả các ideal thật sự của D chứa nghiêm ngặt P_1 . Vì P_1 không tối đại nên S là tập khác rỗng.

Theo định lý 2.2.1, D là một vành Noether nên S có chứa một phần tử tối đại P_2 sao cho

$$P_1 \subset P_2 \subset D$$

Do mọi ideal tối đại cũng là ideal nguyên tố nên P_2 là ideal nguyên tố.

Theo bổ đề 2.1.3 mọi ideal $\neq \{0\}$ của D đều chứa ít nhất một số nguyên hữu tỉ khác không nên

$P_1 \cap Z \neq \{0\}$, do $P_1 \cap Z$ là ideal nguyên tố của Z và Z là một miền ideal chính nên $P_1 \cap Z = \langle p \rangle$ với p là một số nguyên tố.

Như vậy

$$\langle p \rangle = P_1 \cap Z \subseteq P_2 \cap Z \subseteq Z$$

Vì $1 \notin P_2$ nên $P_2 \cap Z \neq Z$, hơn nữa $\langle p \rangle$ là ideal tối đại của Z nên

$$\langle p \rangle = P_1 \cap Z = P_2 \cap Z \subset Z$$

Vì

$$P_1 \subset P_2$$

nên có $\alpha \in P_2$ mà $\alpha \notin P_1$.

Do $\alpha \in D$ nên α là nghiệm của một đa thức đơn khởi với hệ số nguyên

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

và vì thế

$$\alpha^k + a_{k-1}\alpha^{k-1} + \dots + a_1\alpha + a_0 \in P_1 \quad (*)$$

Gọi l là số nguyên dương nhỏ nhất sao cho có $b_0, \dots, b_{l-1} \in Z$ mà

$$\alpha^l + b_{l-1}\alpha^{l-1} + \dots + b_1\alpha + b_0 \in P_1$$

Vì $\alpha \in P_2$ ta có

$$\alpha^l + b_{l-1}\alpha^{l-1} + \dots + b_1\alpha = \alpha(\alpha^{l-1} + b_{l-1}\alpha^{l-2} + \dots + b_1) \in P_2$$

Do đó

$b_0 = (\alpha^l + b_{l-1}\alpha^{l-1} + \dots + b_1\alpha + b_0) - (\alpha^l + b_{l-1}\alpha^{l-1} + \dots + b_1\alpha) \in P_2$ vì $P_1 \subset P_2$ và P_2 là một ideal.

Nhưng vì $b_0 \in Z$ nên

$$b_0 \in P_2 \cap Z = P_1 \cap Z$$

$$\Rightarrow b_0 \in P_1.$$

Từ (*) ta được

$$\alpha^l + b_{l-1}\alpha^{l-1} + \dots + b_1\alpha \in P_1$$

Bây giờ nếu $l=1$ thì $b_1 = 1$ và $\alpha \in P_1$ mâu thuẫn việc $\alpha \notin P_1$.

Do đó $l \geq 2$ và $\alpha(\alpha^{l-1} + b_{l-1}\alpha^{l-2} + \dots + b_1) \in P_1$.

Vì P_1 là ideal nguyên tố và $\alpha \notin P_1$ nên

$$\alpha^{l-1} + b_{l-1}\alpha^{l-2} + \dots + b_1 \in P_1$$

Do $l-1$ là số nguyên dương nên nếu biểu thức trên xảy ra sẽ mâu thuẫn cách chọn số nguyên dương l thỏa (*).

Vậy trong vành D , mọi ideal nguyên tố P đều là ideal tối đại.

Từ các kết quả trên ta thấy

- D là vành Noether (theo định lý 2.2.1)
- D là vành đóng nguyên (theo định lý 2.1.2), và
- Mọi ideal nguyên tố của D đều tối đại (theo định lý 2.2.2)

Vì D thỏa 3 tính chất nên D là vành Dedekind. Do đó, theo định lý 1.2.11 thì trong D, mọi ideal thật sự đều có thể được biểu diễn dưới dạng tích các ideal nguyên tố của D và sự biểu diễn này là duy nhất. Hơn nữa, theo định nghĩa 1.2.12 cùng với phân nhận xét của nó ta có thể khẳng định tập các ideal khác không của D lập thành một nhóm Abel.

2.3 CHUẨN CỦA MỘT IDEAL

2.3.1 Định nghĩa

Ta nói

- Một cơ sở của D được gọi là một cơ sở nguyên của K
- Nếu $\{\eta_1, \dots, \eta_n\}$ là một cơ sở nguyên của K ta kí hiệu $d(K) = D(\eta_1, \dots, \eta_n)$ gọi là định thức của trường K.
- Nếu I là một ideal khác không của D thì chuẩn của ideal I, kí hiệu

$$N(I), \text{ được xác định bởi công thức } N(I) = \sqrt{\frac{D(I)}{d(K)}}$$

2.3.2 Định lý

$N(I)$ là một số nguyên dương

Chứng minh

Gọi $\{\eta_1, \dots, \eta_n\}$ là một cơ sở của I và $\{\lambda_1, \dots, \lambda_n\}$ là một cơ sở nguyên của K. Do

$$\eta_1, \dots, \eta_n \in D \text{ nên có } c_{ij} \in Z \text{ (} i, j = 1, 2, \dots, n \text{) sao cho } \eta_i = \sum_{j=1}^n c_{ij} \lambda_j, \quad i = 1, 2, \dots, n$$

Do đó

$$D(\eta_1, \dots, \eta_n) = (\det(c_{ij}))^2 \cdot D(\lambda_1, \dots, \lambda_n)$$

$$\Rightarrow D(I) = (\det(c_{ij}))^2 \cdot d(K)$$

Từ $D(I) \neq 0$ ta có $\det(c_{ij}) \neq 0$ cho nên

$$N(I) = \sqrt{\frac{D(I)}{d(K)}} = |\det(c_{ij})|$$

là một số nguyên dương.

2.3.3 Ví dụ

Gọi c là một số nguyên khác không. Khi đó, chuẩn của ideal chính $\langle c \rangle$ của D sinh bởi c là

$$N(\langle c \rangle) = |c|^n$$

Chứng minh

Gọi $\{\lambda_1, \dots, \lambda_n\}$ là một cơ sở nguyên của K.. Khi đó

$\alpha \in \langle c \rangle \Leftrightarrow \alpha = c \cdot \beta$, với duy nhất $\beta \in D$

$\Leftrightarrow \alpha = c \cdot (x_1 \lambda_1 + \dots + x_n \lambda_n)$ với duy nhất $x_1, \dots, x_n \in Z$

$\Leftrightarrow \alpha = x_1(c\lambda_1) + \dots + x_n(c\lambda_n)$ với duy nhất $x_1, \dots, x_n \in Z$

Điều này chứng tỏ rằng $\{c\lambda_1, \dots, c\lambda_n\}$ là một cơ sở của ideal chính $\langle c \rangle$. Do đó

$$D(\langle c \rangle) = D(c\lambda_1, \dots, c\lambda_n) = c^{2n} \cdot D(\lambda_1, \dots, \lambda_n) = c^{2n} \cdot d(K)$$

$$\text{Thế nên } N(I) = \sqrt{\frac{D(\langle c \rangle)}{d(K)}} = \sqrt{c^{2n}} = |c|^n.$$

2.3.4 Định lý

Nếu I là một ideal khác không của D thì $N(I) = |D/I|$.

Chứng minh

Gọi $\{\eta_1, \dots, \eta_n\}$ là một cơ sở của I và $\{\lambda_1, \dots, \lambda_n\}$ là một cơ sở nguyên của K . Do

$\eta_1, \dots, \eta_n \in D$ nên có $c_{ij} \in Z$ ($i, j = 1, 2, \dots, n$) sao cho $\eta_i = \sum_{j=1}^n c_{ij} \lambda_j$, $i = 1, 2, \dots, n$.

Do đó

$$D(\eta_1, \dots, \eta_n) = (\det(c_{ij}))^2 \cdot D(\lambda_1, \dots, \lambda_n)$$

$$\Rightarrow D(I) = (\det(c_{ij}))^2 \cdot d(K)$$

Từ $D(I) \neq 0$ ta có $\det(c_{ij}) \neq 0$ cho nên

$$N(I) = \sqrt{\frac{D(I)}{d(K)}} = \sqrt{\frac{D(\eta_1, \dots, \eta_n)}{D(\lambda_1, \dots, \lambda_n)}} = |(\det(c_{ij}))| = |D/I| \text{ theo định lý 1.4.5.}$$

2.3.5 Định nghĩa

Cho K là một trường số đại số bậc n . Với $\alpha \in K$ ta đặt $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ là các K -liên hợp của α . Khi đó, vết của α , kí hiệu $tr(\alpha)$, và chuẩn của α , kí hiệu $N(\alpha)$ được định nghĩa như sau

$$tr(\alpha) = \alpha_1 + \alpha_2 + \dots + \alpha_n$$

$$N(\alpha) = \alpha_1 \cdot \alpha_2 \cdot \dots \cdot \alpha_n$$

2.3.6 Định lý

a) Nếu $\alpha \in K$ thì $tr(\alpha), N(\alpha) \in Q$

Nếu $\alpha \in D$ thì $tr(\alpha), N(\alpha) \in Z$

b) $tr(\alpha + \beta) = tr(\alpha) + tr(\beta)$ và $tr(\alpha \cdot \beta) = tr(\alpha) \cdot tr(\beta)$

c) Cho $\alpha \in D$, khi đó $N(\alpha) = \pm 1 \Leftrightarrow \alpha$ là phần tử khả nghịch của D

d) Cho $\alpha \in D$, khi đó $N(\alpha) = \pm p$, với p là một số nguyên tố thì α phần tử bất khả quy của D

e) Nếu $irr_Q(\alpha) = x^m + b_{m-1}x^{m-1} + \dots + b_0 \in Q[x]$ thì $N(\alpha) = (-1)^n \cdot (b_0)^{\frac{n}{m}}$

Chứng minh

Gọi $\sigma_k : K \rightarrow C$ ($k=1, \dots, n$) là n đơn cấu trường từ K vào C .

a) Xét đa thức trường của α

$$\begin{aligned} fld(\alpha) &= (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \dots (x - \sigma_n(\alpha)) \\ &= x^n - (\sigma_1(\alpha) + \sigma_2(\alpha) + \dots + \sigma_n(\alpha))x^{n-1} + (-1)^n (\sigma_1(\alpha)\sigma_2(\alpha) \dots \sigma_n(\alpha)) \end{aligned}$$

Vậy nên,

- nếu $\alpha \in K$ thì $fld(\alpha) \in Q[x] \Rightarrow tr(\alpha), N(\alpha) \in Q$

- nếu $\alpha \in D$ thì $fld(\alpha) \in Z[x] \Rightarrow tr(\alpha), N(\alpha) \in Z$

b) Hiển nhiên theo tính chất đồng cấu trường

c) + Giả sử rằng α là phân tử khả nghịch, khi đó có $\beta \in D$ thỏa $\alpha\beta = 1$.

$$\Rightarrow N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1.$$

Vì $N(\alpha), N(\beta) \in Z$ nên $N(\alpha) = \pm 1$

+ Bây giờ, gọi $\alpha \in D$ mà $N(\alpha) = \pm 1$ ta có

$$\sigma_1(\alpha)\sigma_2(\alpha) \dots \sigma_n(\alpha) = \pm 1$$

$$\Rightarrow \alpha.\sigma_2(\alpha) \dots \sigma_n(\alpha) = \pm 1$$

Đặt

$$\beta = \pm \sigma_2(\alpha) \dots \sigma_n(\alpha)$$

$$\Rightarrow \alpha\beta = 1 \quad (*)$$

$$\Rightarrow \beta = \frac{1}{\alpha} \in K$$

Do $\alpha \in D$ nên $fld(\alpha) \in Z[x]$, như vậy mỗi $\sigma_k(\alpha)$ là nghiệm của một đa thức đơn khởi với hệ số nguyên

$$\Rightarrow \sigma_k(\alpha) \in \Omega; k = 2, \dots, n$$

$$\Rightarrow \beta = \pm \sigma_2(\alpha) \dots \sigma_n(\alpha) \in \Omega$$

$$\Rightarrow \beta \in \Omega \cap K = D \quad (**)$$

Từ (*) và (**)

$\Rightarrow \alpha$ là phân tử khả nghịch.

d) Giả sử $\alpha \in D$, khi đó $N(\alpha) = \pm p$, với p là một số nguyên tố.

Rõ ràng $\alpha \neq 0$ vì $N(0) = 0$. Hơn nữa, α cũng không khả nghịch vì $N(\alpha) \neq \pm 1$.

Giả sử $\alpha = \beta\gamma; \gamma, \beta \in D$

$$\Rightarrow \pm p = N(\alpha) = N(\beta)N(\gamma)$$

Do $N(\beta), N(\gamma) \in Z$ và p là số nguyên tố

$$\Rightarrow N(\beta) \text{ hay } N(\gamma) = \pm 1$$

$\Rightarrow \beta$ hay γ khả nghịch.

Điều này chứng tỏ rằng α là phân tử bất khả quy của D .

e) Xét

$$fld(\alpha) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \dots (x - \sigma_n(\alpha))$$

$$irr_Q(\alpha) = x^m + b_{m-1}x^{m-1} + \dots + b_0 = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_m)$$

$$\Rightarrow fld(\alpha) = (irr_Q(\alpha))^s = (x - \alpha_1)^s (x - \alpha_2)^s \dots (x - \alpha_m)^s \text{ (theo 1.3.3b)}$$

$$\Rightarrow s = \frac{m}{n} \text{ hay } m \mid n$$

Ta có

$$irr_Q(\alpha) = x^m + b_{m-1}x^{m-1} + \dots + b_0 = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_m)$$

$$\Rightarrow b_0 = (-1)^m \alpha_1 \alpha_2 \dots \alpha_m$$

Do đó

$$N(\alpha) = \alpha_1(\alpha) \dots \sigma_n(\alpha) = (\alpha_1 \dots \alpha_m)^s = (\alpha_1 \dots \alpha_m)^{\frac{n}{m}} = \left((-1)^m b_0\right)^{\frac{n}{m}} = (-1)^n \cdot (b_0)^{\frac{n}{m}}$$

2.3.7 Định lý

Với $\alpha \in D$ ta có

$$N(\langle \alpha \rangle) = |N(\alpha)|$$

Chứng minh

Gọi $\{\omega_1, \dots, \omega_n\}$ là một cơ sở nguyên của K , khi đó $\{\alpha\omega_1, \dots, \alpha\omega_n\}$ là một cơ sở của $\langle \alpha \rangle$. Do đó

$$D(\langle \alpha \rangle) = \begin{vmatrix} \sigma_1(\alpha\omega_1) & \dots & \sigma_1(\alpha\omega_n) \\ \sigma_2(\alpha\omega_1) & \dots & \sigma_2(\alpha\omega_n) \\ \vdots & \dots & \vdots \\ \sigma_n(\alpha\omega_1) & \dots & \sigma_n(\alpha\omega_n) \end{vmatrix}^2$$

với $\sigma_k : K \rightarrow C (k=1, \dots, n)$ là n đơn cấu trường

$$= \begin{vmatrix} \sigma_1(\alpha)\sigma_1(\omega_1) & \dots & \sigma_1(\alpha)\sigma_1(\omega_n) \\ \sigma_2(\alpha)\sigma_2(\omega_1) & \dots & \sigma_2(\alpha)\sigma_2(\omega_n) \\ \vdots & \dots & \vdots \\ \sigma_n(\alpha)\sigma_n(\omega_1) & \dots & \sigma_n(\alpha)\sigma_n(\omega_n) \end{vmatrix}^2$$

$$= (\sigma_1(\alpha)\sigma_2(\alpha) \dots \sigma_n(\alpha))^2 \begin{vmatrix} \sigma_1(\omega_1) \dots \sigma_1(\omega_n) \\ \sigma_2(\omega_1) \dots \sigma_2(\omega_n) \\ \vdots & \dots & \vdots \\ \sigma_n(\omega_1) \dots \sigma_n(\omega_n) \end{vmatrix}^2$$

$$= N(\alpha)^2 \cdot d(K)$$

$$\Rightarrow N(\langle \alpha \rangle) = \sqrt{\frac{D(\langle \alpha \rangle)}{d(K)}} = \sqrt{(N(\alpha))^2} = |N(\alpha)|.$$

2.3.8 Bổ đề

Cho D là một vành Dedekind. Giả sử A là một ideal nguyên hoặc phân của D với $A \neq \langle 0 \rangle, \langle 1 \rangle$ và B là một ideal nguyên của D , $B \neq \langle 0 \rangle, \langle 1 \rangle$. Khi đó tồn tại phần tử $\gamma \in A$ thỏa

$$A = \langle \gamma \rangle + AB$$

Đồng thời, nếu như P_i là ideal nguyên tố của D có mặt trong sự phân tích của B thì $\text{ord}_{P_i}(A) = \text{ord}_{P_i}(\gamma)$

Chứng minh

Gọi $P_1, \dots, P_n$ là tập các ideal nguyên tố của D thỏa

$$\text{ord}_{P_i}(A) \neq 0 \text{ hay } \text{ord}_{P_i}(AB) \neq 0$$

Tập trên khác rỗng vì $A \neq D$. Theo 1.2.17, ta tìm được γ thuộc trường các thương của D sao cho

$$\text{ord}_{P_i}(\gamma) = \text{ord}_{P_i}(A) \quad ; i = 1, \dots, n$$

$$\text{ord}_P(\gamma) \geq 0 \quad ; P \neq P_1, \dots, P_n$$

Như vậy

$$\text{ord}_P(\gamma) \geq \text{ord}_P(A) \text{ với mọi ideal } P$$

Do đó

$$\langle \gamma \rangle \subset A$$

$$\Rightarrow \langle \gamma \rangle \subset A \Rightarrow \gamma \in A$$

+ Với mỗi $i = 1, \dots, n$ ta có

$$\begin{aligned} \text{ord}_{P_i}(\langle \gamma \rangle + AB) &= \min \{ \text{ord}_{P_i}(\langle \gamma \rangle), \text{ord}_{P_i}(AB) \} \\ &= \min \{ \text{ord}_{P_i}(\gamma), \text{ord}_{P_i}(A) + \text{ord}_{P_i}(B) \} \\ &= \min \{ \text{ord}_{P_i}(A), \text{ord}_{P_i}(A) + \text{ord}_{P_i}(B) \} \\ &= \text{ord}_{P_i}(A) \end{aligned}$$

+ Với ideal $P \neq P_i$; $i = 1, \dots, n$ thì $\text{ord}_P(A) = \text{ord}_P(AB) = 0$, do đó

$$\begin{aligned} \text{ord}_P(\langle \gamma \rangle + AB) &= \min \{ \text{ord}_P(\langle \gamma \rangle), \text{ord}_P(AB) \} \\ &= \min \{ \text{ord}_P(\langle \gamma \rangle), 0 \} \\ &= 0 \\ &= \text{ord}_P(A) \end{aligned}$$

Vậy

$$\text{ord}_P(\langle \gamma \rangle + AB) = \text{ord}_P(A) \text{ với mọi ideal nguyên tố } P$$

$$\Rightarrow A = \langle \gamma \rangle + AB.$$

Bây giờ, gọi P_i là ideal nguyên tố có mặt trong sự phân tích của B

Khi đó

$$\begin{aligned}
ord_{P_i}(A) &= ord_P(\langle \gamma \rangle + AB) \\
&= \min \{ ord_{P_i}(\langle \gamma \rangle), ord_{P_i}(AB) \} \\
&= \min \{ ord_{P_i}(\langle \gamma \rangle), ord_{P_i}(A) + ord_{P_i}(B) \} \quad (2)
\end{aligned}$$

Vì P_i là ideal nguyên tố có mặt trong sự phân tích của B nên $ord_{P_i}(B) > 0$

Do đó

$$\begin{aligned}
ord_{P_i}(A) + ord_{P_i}(B) &> ord_{P_i}(A) \\
\Rightarrow ord_{P_i}(A) &= ord_{P_i}(\gamma).
\end{aligned}$$

2.3.9 Định lý

Gọi A, B là các ideal nguyên khác không của D. Khi đó

$$N(AB) = N(A).N(B)$$

Chứng minh

Nếu $A = D$ hay $B = D$ thì kết quả định lý vẫn đúng vì $N(D) = |D/D| = 1$. Do đó có thể giả sử $A \neq D, B \neq D$. Đặt $k = N(A)$ và $l = N(B)$ thì theo định lý 2.3.4 ta có

$$|D/A| = N(A) = k$$

$$\Rightarrow D/A \text{ có } k \text{ phần tử, giả sử là } \alpha_1 + A, \dots, \alpha_k + A \quad (*)$$

$$\text{Cũng vậy, } D/B \text{ có } l \text{ phần tử là } \beta_1 + B, \dots, \beta_l + B \quad (**)$$

Theo bổ đề 2.3.8, có phần tử $\gamma \in A$ sao cho

$$A = \langle \gamma \rangle + AB$$

Nếu $\gamma = 0$ thì $A = AB$ suy ra $B = D$ mâu thuẫn việc $B \neq D$. Do đó $\gamma \neq 0$. Lấy $\delta \in D$, khi đó, theo (*) thì có duy nhất số nguyên i ($1 \leq i \leq k$) sao cho

$$\delta \equiv \alpha_i \pmod{A}$$

Vì

$$\delta - \alpha_i \in A = \langle \gamma \rangle + AB$$

nên có $\sigma \in D$ và $\tau \in AB$ sao cho

$$\delta - \alpha_i = \sigma \gamma + \tau$$

Tương tự, có duy nhất số nguyên j ($1 \leq j \leq l$) sao cho

$$\sigma \equiv \beta_j \pmod{B}$$

$$\Rightarrow \sigma - \beta_j \in B$$

Vì $\gamma \in A$

$$\Rightarrow (\sigma - \beta_j)\gamma \in AB$$

Do đó

$$\delta = \alpha_i + \sigma \gamma + \tau = \alpha_i + \beta_j \gamma + (\sigma - \beta_j)\gamma + \tau = \alpha_i + \beta_j \gamma \pmod{AB}$$

Điều này chứng tỏ rằng tập gồm $k l$ phần tử

$$\{\alpha_i + \beta_j \gamma + AB : i = 1, \dots, k; j = 1, \dots, l\}$$

là tập đại diện đầy đủ của D/AB . Ta chứng minh các $\alpha_i + \beta_j \gamma + AB$ đôi một phân biệt. Giả sử có

$$\begin{aligned} \alpha_i + \beta_j \gamma + AB &= \alpha_p + \beta_q \gamma + AB \\ \Rightarrow \alpha_i + \beta_j \gamma &\equiv \alpha_p + \beta_q \gamma \pmod{AB} \\ \Rightarrow \alpha_i - \alpha_p &\equiv (\beta_q - \beta_j) \gamma \pmod{AB} \quad (***) \end{aligned}$$

Vì $(\beta_q - \beta_j) \gamma \in \langle \gamma \rangle$, $A = \langle \gamma \rangle + AB$

$$\Rightarrow \alpha_i - \alpha_p \in A$$

$$\stackrel{(*)}{\Rightarrow} i = p$$

$$\stackrel{(***)}{\Rightarrow} \beta_j \gamma \equiv \beta_q \gamma \pmod{AB}$$

$$\Rightarrow (\beta_j - \beta_q) \gamma \in AB \quad (1)$$

Bây giờ, gọi P_i là các ideal nguyên tố có mặt trong sự phân tích của B với

$$B = \prod_{i=1}^h P_i^{b_i}; b_i > 0$$

Khi đó, theo bổ đề 2.3.8

$$\Rightarrow \text{ord}_{P_i}(A) = \text{ord}_{P_i}(\gamma); i = 1, \dots, h \quad (2)$$

Nếu $\beta_j - \beta_q \neq 0$, từ (1) ta có $(\beta_j - \beta_q) \gamma$ là phần tử khác không của AB nên với $i = 1, \dots, h$ ta được

$$\begin{aligned} \text{ord}_{P_i}((\beta_j - \beta_q) \gamma) &\geq \text{ord}_{P_i}(AB) \\ \Rightarrow \text{ord}_{P_i}(\beta_j - \beta_q) + \text{ord}_{P_i}(\gamma) &\geq \text{ord}_{P_i}(A) + \text{ord}_{P_i}(B) \\ \stackrel{(2)}{\Rightarrow} \text{ord}_{P_i}(\beta_j - \beta_q) &\geq \text{ord}_{P_i}(B) \\ \Rightarrow \beta_j - \beta_q &\in B \end{aligned}$$

và như vậy $j = q$ mâu thuẫn $\beta_j - \beta_q \neq 0$.

Điều này chứng tỏ $\beta_j - \beta_q = 0$ suy ra $j = q$.

Do đó $\{\alpha_i + \beta_j \gamma + AB : i = 1, \dots, k; j = 1, \dots, l\}$ là tập đầy đủ các đại diện riêng biệt của D/AB

$$\Rightarrow |D/AB| = k.l = |D/A| \cdot |D/B|$$

$$\Rightarrow N(AB) = N(A).N(B).$$

2.3.10 Định nghĩa

Cho A là một ideal phân khác không của D, khi đó có $\alpha \neq 0, \alpha \in D$ và ideal nguyên I của D sao cho

$$A = \frac{1}{\alpha} I$$

Ta định nghĩa chuẩn $N(A)$ của ideal phân A như sau

$$N(A) = \frac{N(I)}{N(\langle \alpha \rangle)}$$

Nhận xét

Định nghĩa trên hợp lý vì nếu các ideal nguyên I, J của D và α, β là các phần tử khác không của D sao cho

$$A = \frac{1}{\alpha} I = \frac{1}{\beta} J$$

Thì

$$\beta I = \alpha J$$

Theo định lý 2.3.9 ta có

$$N(\beta)N(I) = N(\beta I) = N(\alpha J) = N(\alpha)N(J)$$

$$\Rightarrow \frac{N(I)}{N(\langle \alpha \rangle)} = \frac{N(J)}{N(\langle \beta \rangle)}$$

2.3.11 Hệ quả

Nếu A, B là các ideal phân khác không của D thì

$$N(AB) = N(A).N(B)$$

Chứng minh

Vì A, B là các ideal phân khác không của D nên có các ideal nguyên I, J khác không của D và các phần tử khác không α, β của D sao cho

$$A = \frac{1}{\alpha} I, B = \frac{1}{\beta} J$$

Khi đó

$$AB = \frac{1}{\alpha} \frac{1}{\beta} IJ$$

$$\begin{aligned} \Rightarrow N(AB) &= \frac{N(IJ)}{N(\langle \alpha\beta \rangle)} \\ &= \frac{N(IJ)}{N(\langle \alpha \rangle \langle \beta \rangle)} \\ &= \frac{N(I)N(J)}{N(\langle \alpha \rangle)N(\langle \beta \rangle)} \\ &= \frac{N(I)}{N(\langle \alpha \rangle)} \cdot \frac{N(J)}{N(\langle \beta \rangle)} \\ &= N(A).N(B) \end{aligned}$$

2.3.12 Định lý

Cho P là một ideal nguyên tố của D . Khi đó, tồn tại duy nhất một số nguyên tố p thỏa $P \mid \langle p \rangle$

Chứng minh

Do P là ideal nguyên tố của D và $Z \subset D$ nên $P \cap Z$ là một ideal nguyên tố của D

Do Z là một vành chính

$\Rightarrow P \cap Z$ cũng là một ideal chính

$\Rightarrow P \cap Z = \langle p \rangle$, với p là một số nguyên tố

$\Rightarrow P \mid \langle p \rangle$

Ta chứng minh sự duy nhất của số nguyên tố p :

Giả sử q là số nguyên tố thỏa:

$P \mid \langle q \rangle$, $q \neq p$

$\Rightarrow \langle q \rangle \subseteq P$

$\Rightarrow \langle p, q \rangle \subseteq P$, do $\langle p \rangle \subseteq P$

Do p, q là nguyên tố cùng nhau

$\Rightarrow \exists a, b \in Z$ sao cho $ap + bq = 1$

$\Rightarrow 1 \in \langle p, q \rangle \subseteq P$

$\Rightarrow D \subseteq P$ (vô lý)

Vậy $q = p$; p là số nguyên tố duy nhất được xác định bởi $P \mid \langle p \rangle$

Lưu ý

Số nguyên tố p trong định lý trên gọi là số nguyên tố nằm dưới P vì $P \supseteq \langle p \rangle$. Hơn nữa, nếu cho trước một số nguyên tố p thì mọi ideal nguyên tố P thỏa $P \mid \langle p \rangle$ được gọi là ideal nằm trên p .

2.3.13 Định lý

Cho P là một ideal nguyên tố của D , gọi p là số nguyên tố nằm dưới P . Khi đó

$N(P) = p^f$ (f là một số nguyên dương nào đó thuộc $\{1; \dots; n\}$)

Chứng minh

Vì p nằm dưới P nên $P \mid \langle p \rangle$

$\Rightarrow \langle p \rangle = P.Q$; với Q là một ideal nguyên nào đó của D

$\Rightarrow N(\langle p \rangle) = N(P.Q) = N(P).N(Q)$

Do $p \in Z$ nên

$N(\langle p \rangle) = p^n$

$\Rightarrow p^n = N(P).N(Q)$

$\Rightarrow N(P) \mid p^n$

Vậy tồn tại số nguyên $f \in \{1; 2; \dots; n\}$ sao cho

$$N(P) = p^f$$

2.3.14 Định nghĩa

Cho p là một số nguyên tố nằm dưới P . Khi đó số nguyên dương f thỏa

$$N(P) = p^f$$

được gọi là bậc quán tính của P trong D , kí hiệu $f_k(P)$

2.3.15 Nhận xét

Theo các định lý 2.1.14 và 2.3.4 ta có

$$[D:P] = p^f$$

nên D/P là một trường số hữu hạn với p^f phần tử

Xét các phần tử có dạng

$$a + P \text{ với } a \in Z$$

của D , ta thấy nếu

$$a, a' \in Z \text{ mà } a \equiv a' \pmod{p}$$

$$\Rightarrow p \mid a - a'$$

$$\Rightarrow \langle p \rangle \mid \langle a - a' \rangle$$

$$\text{mà } P \mid \langle p \rangle$$

$$\Rightarrow P \mid \langle a - a' \rangle$$

$$\Rightarrow a \equiv a' \pmod{P} \text{ hay } a + P = a' + P$$

Ngược lại, giả sử rằng $a + P = a' + P$; $a, a' \in Z$

$$\Rightarrow a - a' \in P$$

$$\Rightarrow \langle a - a' \rangle \leq P \text{ hay } P \mid \langle a - a' \rangle$$

$$\Rightarrow \langle a - a' \rangle = P \cdot Q \text{ với } Q \text{ là một ideal nguyên nào đó của } D$$

Lấy chuẩn hai vế ta được

$$\Rightarrow |a - a'|^n = N(\langle a - a' \rangle) = N(P \cdot Q) = N(P) \cdot N(Q) = p^f \cdot N(Q)$$

$$\Rightarrow p^f \mid (a - a')^n$$

$$\Rightarrow p \mid a - a' ; \text{ do } p \text{ nguyên tố}$$

$$\Rightarrow a \equiv a' \pmod{p}$$

Từ hai kết quả trên ta có

$$a + P = a' + P \Leftrightarrow a \equiv a' \pmod{p} ; a, a' \in Z$$

Như vậy các lớp $a + P$; $a \in \{0; 1; \dots; p-1\}$ là phân biệt và trường nguyên tố của D/P là:

$$F = \{a + P \mid a = 0; 1; \dots; p-1\} \simeq Z/\langle p \rangle$$

Bậc quán tính $f = f_k(P)$ được cho bởi

$$f_k(P) = [D/P : F] = [D/P : Z/\langle p \rangle]$$

Nếu $f_k(P) = 1$ thì $[D/P : F] = 1$

$$\Rightarrow D/P = F = \{a + P \mid a = 0; 1; \dots; p-1\}$$

Lúc này lấy $\alpha \in D$ thì $\alpha + P \in D/P$ nên có $a \in \{0; 1; \dots; p-1\}$ thỏa

$$\alpha + P = a + P$$

$$\Rightarrow \alpha \equiv a \pmod{P}$$

Như vậy khi $f_k(P) = 1$ thì với α bất kỳ thuộc D , luôn tồn tại $a \in Z$ sao cho

$$\alpha \equiv a \pmod{P}$$

(hơn nữa $a \in \{0; 1; \dots; p-1\}$)

2.3.16 Định lý

Cho p là số nguyên tố. Giả sử rằng ideal chính $\langle p \rangle$ được phân tích trong D dưới dạng:

$\langle p \rangle = P_1^{e_1} \dots P_g^{e_g}$; P_i là các ideal nguyên tố phân biệt của D , e_i là các số nguyên dương

Đặt $f_i = f_K(P_i)$, khi đó:

$$e_1 f_1 + \dots + e_g f_g = n$$

Chứng minh

Do $f_i = f_K(P_i)$

$$\Rightarrow N(P_i) = p^{f_i}; i = 1; 2; \dots; g$$

Vì $\langle p \rangle = P_1^{e_1} \dots P_g^{e_g}$

$$\Rightarrow N(\langle p \rangle) = N(P_1^{e_1} \dots P_g^{e_g})$$

$$\Rightarrow p^n = N(P_1)^{e_1} \dots N(P_g)^{e_g} = (p^{f_1})^{e_1} \dots (p^{f_g})^{e_g}$$

$$\Rightarrow e_1 f_1 + \dots + e_g f_g = n$$

Nhận xét: được suy ra trực tiếp từ định lý

$$+ e_i \in \{1; 2; \dots; n\}; f_i \in \{1; 2; \dots; n\}; i = 1; 2; \dots; g$$

$$+ P^n | \langle p \rangle; P \text{ ideal nguyên tố}$$

$$\Rightarrow \langle p \rangle = P^n$$

2.3.17 Định nghĩa

Cho P là một ideal nguyên tố của D , gọi p là số nguyên tố nằm dưới P . Khi đó, số nguyên dương e duy nhất thỏa

$$P^e | \langle p \rangle \text{ và } P^{e+1} \nmid \langle p \rangle$$

được gọi là chỉ số rẽ nhánh của P trong K , kí hiệu $e_K(P)$

Từ định lý 2.1.15 ta có $e_K(P) \leq n$; $e_K(P_i) = e_i$; $f_K(P_i) = f_i$ và $g_K(p) = g$

2.3.18 Định nghĩa

Cho p là một số nguyên tố. Gọi $P_1, \dots, P_g$ là các ideal nguyên tố nằm trên p . Khi đó

$$\langle p \rangle = P_1^{e_1} \dots P_g^{e_g}; e_i = e_K(P_i); i = 1, \dots, g$$

nếu

+ có $e_i, i \in \{1, \dots, g\}$ sao cho $e_i > 1$ thì p gọi là rẽ nhánh trong K

+ $e_i = 1; \forall i = 1, 2, \dots, g$ thì p không rẽ nhánh trong K

2.3.19 Định lý

Gọi $I (\neq \langle 0 \rangle)$ là một ideal của D . Khi đó:

a) Nếu $N(I) = p$ với p là một nguyên tố thì I là một ideal nguyên tố

b) $N(I) \in I$

Chứng minh

a) Giả sử $N(I) = p$, p nguyên tố

Rõ ràng $I \neq \langle 1 \rangle$ vì $N(I) \neq 1$. Giả sử tồn tại các ideal nguyên tố P, Q mà PQ chia được I (hay $PQ \mid I$) P, Q có thể không phân biệt thì $I = PQA$; với A là một nguyên tố nào đó của D . Ta có:

$$p = N(I) = N(P) \cdot N(Q) \cdot N(A)$$

Đẳng thức này không thể xảy ra khi p là một số nguyên tố; $N(P), N(Q)$ là các số nguyên dương lớn hơn 1.

$\Rightarrow I$ phải là một ideal nguyên tố.

b) Chứng minh $N(I) \in I$

Ta có

$$N(I) = |D:I|$$

Do đó

$$N(I) \cdot (x + I) = 0 + I; \forall x \in D$$

hay

$$N(I) \cdot x \in I; \forall x \in D$$

Chọn $x = 1 \in D$ ta được $N(I) \in I$

2.4 HÀM EULER – CÁC TÍNH CHẤT CỦA HÀM EULER

2.4.1 Định nghĩa

Cho $A \triangle D$ ta nói rằng $(\bar{x}, A) = 1$ nếu $(x, A) = 1$.

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

$$\Rightarrow x' - x \in A \Rightarrow (x', A) = (x, A) = 1$$

2.4.2 Định nghĩa

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

2.4.3 Mệnh đề

Cho $A \triangle D$, $(\bar{x}, A) = 1 \Leftrightarrow \bar{x}$ khả nghịch

Chứng minh

$+\Rightarrow$) :

$$(\bar{x}, A) = 1$$

ta suy ra

$$(x, A) = 1.$$

Điều này có nghĩa là

$$\langle x \rangle + A = D.$$

Từ đó $\exists x' \in D, a \in A$ để cho $x.x' + a = 1$

$$\Rightarrow \bar{x} \cdot \bar{x}' = \bar{1} \text{ hay } \bar{x} \text{ khả nghịch.}$$

$+\Leftarrow$) :

$\bar{x}$ khả nghịch

suy ra $\exists \bar{x}'$ sao cho $\bar{x} \cdot \bar{x}' = \bar{1}$

Hay

$$x \cdot x' - 1 \in A.$$

Từ đó

$$1 \in \langle x \rangle + A$$

có nghĩa là

$$\langle x \rangle + A = D$$

hay

$$(x, A) = 1.$$

Vậy

$$(D/A)^* = \{ \bar{x}/\bar{x} \text{ khả nghịch} \} = \{ \bar{x}/(x, A) = 1 \}.$$

2.4.4 Định nghĩa

Hàm $\varphi : \mathbf{P} \rightarrow \mathbf{N}^*$; $\mathbf{P}$ là tập các ideal của D .

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

2.4.5 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 :

- $(s, A) = 1 \quad \forall s \in T_A$
- $s, s' \in T_A$ và $s \neq s'$ thì $s \equiv s' \pmod{A}$
- $\forall a \in D$ mà $(a, A) = 1$ 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.

2.4.6 Mệnh đề

Hàm Euler có tính nhân tức là nếu $A, B \triangle D$ và $(A, B) = \langle 1 \rangle$ thì $\varphi(AB) = \varphi(A) \varphi(B)$.

Chứng minh

Do $(A, B) = \langle 1 \rangle$ nên có $a \in A, b \in B$ sao cho $a + b = 1$.

Giả sử γ sao cho $\gamma : A$ và $\gamma : B$ ta có

$$\begin{cases} \gamma : A \\ \gamma : B \end{cases} \Leftrightarrow \gamma = \gamma \cdot (a + b) = (\gamma a + \gamma b) : AB \text{ do } \gamma a \in AB \text{ và } \gamma b \in AB.$$

Xét tương ứng

$$\theta : (D/AB) \rightarrow (D/A) \times (D/B)$$

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

Ta chứng minh θ là một đẳng cấu

θ là một ánh xạ đồng thời là một đơn ánh vì:

$$x_1 + AB = x_2 + AB$$

$$\Leftrightarrow x_1 - x_2 : AB$$

$$\Leftrightarrow x_1 - x_2 : A, x_1 - x_2 : B$$

$$\Leftrightarrow x_1 + A = x_2 + A, x_1 + B = x_2 + B$$

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

. θ là một toàn ánh :

Thật vậy, lấy phần tử $(x + A, y + B) \in (D/A) \times (D/B)$.

Do $(A, B) = 1$

nên

$$A + B = D$$

suy ra tồn tại $a \in A, b \in B$ sao cho $a + b = 1$.

Xét phần tử

$$\alpha = bx + ay$$

thì rõ ràng

$$\begin{cases} x - \alpha = x - bx - ay = x(1 - b) - ay = ax - ay = (x - y)a \in A \\ y - \alpha = y - bx - ay = y(1 - a) - bx = by - bx = (y - x)b \in B \end{cases}$$

$$\Rightarrow \alpha \equiv x \pmod{A}, \alpha \equiv y \pmod{B}.$$

Từ đó ta có:

$$\theta(\alpha + AB) = (\alpha + A, \alpha + B) = (x + A, y + B).$$

Vậy θ là một song ánh.

Dễ thấy θ là một đồng cấu vành nên θ là đẳng cấu vành.

Hơn nữa, theo chứng minh trên thì

$$(x, AB) = 1 \Leftrightarrow \begin{cases} (x, A) = 1 \\ (x, B) = 1 \end{cases}$$

Nên θ cảm sinh đẳng cấu

$$(D/AB)^* \cong (D/A)^* \times (D/B)^*.$$

$$\Rightarrow |(D/AB)^*| = |(D/A)^*| \times |(D/B)^*|$$

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

2.4.7 Mệnh đề

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

Chứng minh

Xét $\theta : (D/B)^* \rightarrow (D/A)^*$

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

Ta thấy quy tắc θ không phụ thuộc vào phần tử đại diện.

Thật vậy với $x_1 + B = x_2 + B$

$$\Rightarrow x_1 - x_2 \in B$$

$$\Rightarrow x_1 - x_2 \in A$$

$$\Rightarrow x_1 + A = x_2 + A.$$

θ là ánh xạ vì $A|B$ nên $(x, B) = 1 \Rightarrow (x, A) = 1$.

Dễ thấy rằng θ là một đồng cấu nhóm.

Ta chứng minh θ là toàn cấu tức chứng minh $(D/A)^* \subset \text{im}\theta$.

Thật vậy, với mọi

$$x + A \in (D/A)^*$$

$$\Rightarrow (x, A) = 1.$$

Do $A | B$ nên có thể giả sử rằng P_i ($1 \leq i \leq k$) là các ideal nguyên tố mà $P_i | B$ nhưng $P_i \nmid A$

$$\Rightarrow (P_1 P_2 \dots P_k, A) = 1$$

$$\Rightarrow P + A = D \text{ với } P = \prod_{i=1}^k P_i.$$

Từ đó tồn tại $p \in P, a \in A$ để cho

$$p + a = 1$$

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

Do đó $(x', A) = (x, A) = 1$ và $(x', P) = 1$

suy ra

$$(x', AP) = 1.$$

Mà số các thừa số nguyên tố của B cũng giống như của AP . Vì thế

$$(x', B) = 1.$$

Do đó

$$x' + B \in (D/B)^*.$$

Rõ ràng

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

Vậy θ là toàn cấu.

Theo định lý Note ta có

$$\text{im}\theta \cong (D/B)^* / \ker \theta$$

hay

$$(D/A)^* \cong (D/B)^* / \ker \theta.$$

Suy ra

$$\varphi(A) | \varphi(B).$$

2.4.8 Mệnh đề

Với $n \in \mathbb{N}^*$, $A \Delta D$ 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

$$\theta : (D/A^n)^* \rightarrow (D/A)^*$$

$$(x, A^n) \mapsto (x, A)$$

Theo chứng minh ở 2.4.7, vì $A \mid A^n$ nên θ là một toàn cấu, ta có

$$\ker \theta = \{ \bar{x} \mid x \equiv 1 \pmod{A} \} = \{ \overline{1+a} \mid a \in A \}$$

Ta có $N(A^{n-1}) = N(A)^{n-1} = \left| \left(D/A^{n-1} \right)^* \right|$, gọi

$$S = \{a_1, a_2, \dots, a_{N(A)^{n-1}}\} \text{ là hệ thặng dư đầy đủ theo mod } A^{n-1}$$

Theo Bổ đề 2.3.8, có $\gamma \in A$ sao cho

$$A = \langle \gamma \rangle + AB; \text{ với } B = A^{n-1}$$

$$\Rightarrow A = \langle \gamma \rangle + A^n$$

Ta chứng minh

$$\ker \theta = H; \text{ với } H = \{ \overline{1+\gamma a_i} \pmod{A^n} \}$$

+ Chứng minh $H \subset \ker \theta$

$$\text{Lấy } \overline{1+\gamma a_i} \in H$$

Do

$$\theta(\overline{1+\gamma a_i}) = 1 + \gamma a_i + A = 1 + A = \bar{1} \text{ (vì } \gamma \in A)$$

$$\Rightarrow \overline{1+\gamma a_i} \in \ker \theta$$

$$\Rightarrow H \subset \ker \theta$$

+ Chứng minh $\ker \theta \subset H$

Lấy $\bar{x} = x + A^n \in \ker \theta$, ta chứng minh $\bar{x} = \overline{1+\gamma a_j}$, a_j nào đó thuộc S.

Do $x + A^n \in \ker \theta$

$$\Rightarrow \theta(\bar{x}) = x + A = \bar{1} = 1 + A$$

$$\Rightarrow x - 1 \in A = \langle \gamma \rangle + A^n$$

$$\Rightarrow x - 1 = \gamma y + a; a \in A^n$$

Do $S = \{a_1, a_2, \dots, a_{N(A)^{n-1}}\}$ là hệ thặng dư đầy đủ theo mod A^{n-1} nên có a_j sao cho

$$y \equiv a_j \pmod{A^{n-1}}$$

$$\Rightarrow y - a_j = b; b \in A^{n-1}$$

Ta được

$$\begin{aligned} x - 1 &= \gamma \cdot (b + a_j) + a; b \in A^{n-1}, a \in A^n, \gamma \in A \\ &= \gamma b + \gamma a_j + a \end{aligned}$$

Vì $\gamma b \in A^n$ và $a \in A^n$

$$\Rightarrow x - 1 \equiv \gamma a_j \pmod{A^n}$$

$$\Rightarrow \bar{x} = \overline{1+\gamma a_j} \pmod{A^n}$$

$$\Rightarrow \ker \theta \subset H$$

Do đó

$\ker \theta = H$; với $H = \{ \overline{1 + \gamma a_i} \bmod A^n \}$

+ Hơn nữa, các $\overline{1 + \gamma a_i}$ đôi một khác nhau

Thật vậy, giả sử như

$$\overline{1 + \gamma a_i} = \overline{1 + \gamma a_j}$$

$$\Rightarrow 1 + \gamma a_i + A^n = 1 + \gamma a_j + A^n$$

$$\Rightarrow \gamma(a_i - a_j) \in A^n$$

$$\Rightarrow \gamma(a_i - a_j) \in A^n$$

$$\Rightarrow \langle \gamma \rangle \subset a_i - a_j \subset A^n$$

$$\Rightarrow A \langle a_i - a_j \rangle = (\langle \gamma \rangle + A^n) \langle a_i - a_j \rangle = \langle \gamma \rangle \langle a_i - a_j \rangle + A^n \langle a_i - a_j \rangle \subset A^n$$

$$\Rightarrow A \langle a_i - a_j \rangle \subset A^n$$

$$\Rightarrow \langle a_i - a_j \rangle \subset A^{n-1}$$

$$\Rightarrow a_i \equiv a_j \pmod{A^{n-1}}$$

$$\Rightarrow a_i = a_j$$

Suy ra

$$|\ker \theta| = |H| = N(A)^{n-1}$$

Cuối cùng, do θ toàn cấu, theo định lý Note ta có

$$|(D/A)^*| = |\ker \theta| \cdot |(D/A^n)^*| = N(A)^{n-1} \cdot |(D/A^n)^*|$$

Vậy

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

2.4.9 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) Do $A = P^n$ nên do mệnh đề 2.4.8 ta có:

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

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 nên

$$\varphi(A) = \varphi(P_1^{k_1}) \dots \varphi(P_r^{k_r})$$

Mặt khác

$$\varphi(P_i^{k_i}) = N(P_i)^{k_i-1} [N(P_i) - 1] = N(P_i)^{k_i} \left[1 - \frac{1}{N(P_i)} \right]$$

nên

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

2.4.10 Mệnh đề

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

Chứng minh

+TH1: Với $A = P^n$

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

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

+TH2: Với $A = P_1^{\alpha_1} \dots P_r^{\alpha_r}$, khi đó

$$B|A \Leftrightarrow B = P_1^{a_1} \dots P_r^{a_r} \text{ với } 0 \leq a_i \leq \alpha_i, \forall i = \overline{1, r}$$

Ta có

$$N(A) = N \left[\prod_{i=1}^r P_i^{\alpha_i} \right] = \prod_{i=1}^r N(P_i^{\alpha_i})$$

Theo TH1 ta có

$$N(P_i^{\alpha_i}) = \sum_{C|N(P_i^{\alpha_i})} \varphi(C) = \sum_{0 \leq a_i \leq \alpha_i} \varphi(P_i^{a_i})$$

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

2.5 CÁC ĐỊNH LÝ SỐ HỌC TRÊN VÀNH D

2.5.1 Định lý Euler

Cho $a \in D$, $A \triangle D$ sao cho $(a, A) = 1$. 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 $(a, A) = 1$ nên theo mệnh đề 2.4.3 suy ra

$$\bar{a} \in (D/A)^*.$$

Từ đó cấp của $\bar{a}$ là ước của $\varphi(A)$.

Do vậy

$$\bar{a}^{\varphi(A)} \equiv \bar{1} \text{ hay } a^{\varphi(A)} \equiv 1 \pmod{A}.$$

Từ định lý Euler ta rút ra các hệ quả sau

2.5.2 Hệ quả

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

Chứng minh

Nếu $a \in P$

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

Hay

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

Nếu $(a, P) = 1$ 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

$$a^{\varphi(P)} \equiv a \pmod{P}$$

2.5.3 Hệ quả

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

2.5.4 Hệ quả

$A \triangle D$, $a \in D$ sao cho $(a, A) = 1$. Nếu $s \equiv t \pmod{\varphi(A)}$

thì

$$a^s \equiv a^t \pmod{A}$$

2.5.5 Định lý Wilson

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

Nếu

$\{\zeta_1, \dots, \zeta_s\}$ là hệ thặng dư thu gọn theo mod P thì

$$\zeta_1 \dots \zeta_s \equiv -1 \pmod{P}$$

Chứng minh

Trong trường D/P ta xét phương trình

$$x^s - \bar{1} = \bar{0} \quad (1)$$

với $i \in \{1, 2, \dots, s\}$ thì $\bar{\xi}_i \in (D/P)^*$.

Từ đó

$$(\xi_i, P) = 1.$$

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

$$\prod_{i=1}^s \bar{\xi}_i = (-1)^s (-\bar{1}) \quad (2).$$

Giả sử trường hữu hạn D/P có đặc số p . Khi đó

+Nếu $p = 2$: khi đó

$|D/P| = 2^n$ là số chẵn nên s lẻ nên từ (2) ta có

$$\prod_{i=1}^s \bar{\xi}_i = (-1)(-\bar{1}) = -\bar{1}$$

+Nếu $p > 2$: khi đó

$|D/P| = p^n$ là số lẻ nên s chẵn nên từ (2) ta có

$$\prod_{i=1}^s \bar{\xi}_i = (1)(-\bar{1}) = -\bar{1}.$$

Vậy

$$\prod_{i=1}^r \xi_i = -1 \pmod{P}$$

CHƯƠNG 3

SỰ PHÂN TÍCH MỘT IDEAL THÀNH TÍCH CÁC IDEAL NGUYÊN TỐ TRONG TRƯỜNG BẬC HAI

3.1 Định lý về sự mô tả $\mathcal{O}_K$ khi K là trường bậc hai

Trong tiết này ta kí hiệu K là một mở rộng bậc hai của $\mathbb{Q}$, $[K:\mathbb{Q}] = 2$, $D = \mathcal{O}_K$ là vành các số nguyên đại số của K . Ta có định lý mô tả về vành các số nguyên đại số của K . Trước hết ta xét mệnh đề

3.1.1 Mệnh đề

Tồn tại duy nhất số nguyên m , m không chia hết cho số chính phương khác 1, sao cho $K = \mathbb{Q}(\sqrt{m})$

Chứng minh

*Trước hết ta chứng minh sự tồn tại của m :

Lấy $\alpha \in K \setminus \mathbb{Q}$ thì $K = \mathbb{Q}(\alpha)$.

Do $[K:\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}] = 2$ nên $\text{irr}_{\mathbb{Q}}(\alpha) = x^2 + ax + b \in \mathbb{Q}[x]$ có 2 nghiệm

$$\alpha_1 = \frac{-a + \sqrt{a^2 - 4b}}{2}; \alpha_2 = \frac{-a - \sqrt{a^2 - 4b}}{2}$$

Suy ra $\alpha = \alpha_1$ hay $\alpha = \alpha_2$, vì $\alpha_1 + \alpha_2 = -a$ nên $\mathbb{Q}(\alpha_1) = \mathbb{Q}(-a - \alpha_2) = \mathbb{Q}(\alpha_2) = \mathbb{Q}(\alpha)$

Đặt $a^2 - 4b = \frac{p}{q} = \frac{pq}{q^2}$; $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$; $(p, q) = 1$.

Vì $\alpha \notin \mathbb{Q}$ nên pq không là số chính phương. Do đó $pq = k^2 m$ với $k \in \mathbb{N}^*$, m là số nguyên không chia hết cho số chính phương khác 1.

Như vậy

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}\left(\frac{-a + \sqrt{a^2 - 4b}}{2}\right) = \mathbb{Q}(\sqrt{a^2 - 4b}) = \mathbb{Q}\left(\sqrt{\frac{pq}{q^2}}\right) = \mathbb{Q}\left(\frac{1}{q}\sqrt{pq}\right) = \mathbb{Q}(\sqrt{m}).$$

*Sự duy nhất:

Giả sử rằng n là số nguyên không chính phương khác thỏa $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$

$$\Rightarrow \exists x, y \in \mathbb{Q} \text{ sao cho } m = x^2 + y^2 n + 2xy\sqrt{n}$$

Ta nhận thấy nếu $xy \neq 0 \Rightarrow \sqrt{n} = \frac{m - x^2 - y^2 n}{2xy} \in \mathbb{Q}$ mâu thuẫn cách chọn n không

chính phương. Do đó $xy = 0$. Lúc này, nếu $y = 0$ thì $m = x^2$ hay $\sqrt{m} = x \in \mathbb{Q}$ (vô lý). Suy ra $x=0$, dẫn đến $m = y^2 n$.

Vì $m, n \in \mathbb{Z}$ và m không chia hết cho số chính phương khác 1 nên $y^2 = 1$.

Vậy $n=m$.

3.1.2 Định lý

Cho $K=Q(\sqrt{m})$, m không chia hết cho số chính phương khác 1. Khi đó

$$D = \begin{cases} Z + Z\sqrt{m}; m \equiv 2, 3(\text{mod } 4) \\ Z + Z\frac{1+\sqrt{m}}{2}; m \equiv 1(\text{mod } 4) \end{cases}$$

Chứng minh

Ta chứng minh $Z + Z\sqrt{m} \subset D$

Với $\alpha = a + b\sqrt{m}; a, b \in Z$ thì α là nghiệm của đa thức

$$f(x) = (x - a - b\sqrt{m})(x - a + b\sqrt{m}) = x^2 - 2ax + a^2 - mb^2 \in Z[x] \Rightarrow \alpha \in D$$

Ta chứng minh $Z + Z\frac{1+\sqrt{m}}{2} \subset D$ khi $m \equiv 1(\text{mod } 4)$

Với $\alpha = a + b\frac{1+\sqrt{m}}{2}; a, b \in Z$ thì α là nghiệm của

$$g(x) = [x - (a + \frac{b}{2}) - \frac{b\sqrt{m}}{2}][x - (a + \frac{b}{2}) + \frac{b\sqrt{m}}{2}] = x^2 - (2a+b)x + a^2 + ab - \frac{(m-1)b^2}{4}$$

Do $m \equiv 1(\text{mod } 4)$ nên $g(x) \in Z[x] \Rightarrow \alpha \in D$

Ta chứng minh $D \subset \begin{cases} Z + Z\sqrt{m}; \text{ khi } m \equiv 2, 3(\text{mod } 4) \\ Z + Z\frac{1+\sqrt{m}}{2}; \text{ khi } m \equiv 1(\text{mod } 4) \end{cases}$

Với $\alpha \in D; \alpha = a + b\sqrt{m}; a, b \in Q$. Gọi $f(x)$ là đa thức tối thiểu của α trên Q thì $f(x) \in Z[x]$. Xét 2 trường hợp

*TH1: $b=0 \Rightarrow f(x) = x - a \in Z[x] \Rightarrow a \in Z \Rightarrow \alpha \in Z \Rightarrow D \subset \text{Vế phải(VP)}$

TH2: $b \neq 0 \Rightarrow f(x) = x^2 - 2ax + a^2 - mb^2 \in Z[x] \Rightarrow \begin{cases} 2a \in Z \\ a^2 - mb^2 \in Z \end{cases} ()$

Vì $2a \in Z \Rightarrow 2a \in 2Z$ hay $2a \in 2Z+1$

+ Xét trường hợp $2a \in 2Z$, khi đó $a \in Z \Rightarrow mb^2 \in Z$, ta đặt

$$b = \frac{k}{l}; (k, l) = 1; k, l \in Z \Rightarrow mb^2 = m \frac{k^2}{l^2} \in Z \Rightarrow m : l^2$$

Do m không chia hết cho số chính phương khác 1 nên $l^2 = 1$ hay $l = \pm 1$, suy ra $b \in Z$

Vậy $\alpha = a + b\sqrt{m} \in Z + Z\sqrt{m} \subset \text{VP}$.

+ Xét trường hợp $2a \in 2Z+1$

Từ (*) ta có $a^2 - mb^2 \in Z \Rightarrow 4a^2 - 4mb^2 \in Z \Rightarrow 4mb^2 \in Z \Rightarrow 4b^2 \in Z$ (vì m không chia hết cho số chính phương khác 1).

Ta có $4b^2 \in Z$ dẫn đến $2b \in Z$, từ đó $2b \in 2Z$ hay $2b \in 2Z+1$

Nếu $2b \in 2Z \Rightarrow b \in Z \Rightarrow mb^2 \in Z \Rightarrow a^2 \in Z \Rightarrow a \in Z \Rightarrow 2a \in 2Z$ (vô lý).

Vậy $2b \in 2Z+1$.

Bây giờ, do $2a$ và $2b$ thuộc $2\mathbb{Z}+1$ nên có thể đặt $2a=2u+1$; $2b=2v+1$; $u, v \in \mathbb{Z}$
Do $a^2 - mb^2 \in \mathbb{Z}$ suy ra

$$\left(\frac{2u+1}{2}\right)^2 - m\left(\frac{2v+1}{2}\right)^2 = u^2 - mv^2 + u - mv - \frac{m-1}{4} \in \mathbb{Z}$$

$$\Rightarrow m \in \mathbb{Z} \Rightarrow m \equiv 1 \pmod{4}.$$

Cuối cùng

$$\begin{aligned}\alpha &= a + b\sqrt{m} = \left(\frac{2u+1}{2}\right) + \left(\frac{2v+1}{2}\right)\sqrt{m} \\ &= \left(\frac{2u+1}{2}\right) + \left(\frac{2v+1}{2}\right)(\sqrt{m}+1) - \left(\frac{2v+1}{2}\right) = (u-v) + (2v+1)\frac{1+\sqrt{m}}{2} \\ \Rightarrow \alpha &\in \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{m}}{2} \Rightarrow D \subset \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{m}}{2} \text{ khi } m \equiv 1 \pmod{4}.\end{aligned}$$

Vậy định lý đã được chứng minh.

3.1.3 Định lý

Cho $K=\mathbb{Q}(\sqrt{m})$, m không chia hết cho số chính phương khác 1. Khi đó

a) Nếu $m \equiv 5 \pmod{8}$ thì

$$\langle 2 \rangle \text{ là ideal nguyên tố của } D; N(\langle 2 \rangle) = 4$$

b) Nếu $m \equiv 1 \pmod{8}$ thì

$$\langle 2 \rangle = M_2 \cdot \overline{M_2} \text{ với } M_2 = \left\langle 2, \frac{1+\sqrt{m}}{2} \right\rangle, \overline{M_2} = \left\langle 2, \frac{1-\sqrt{m}}{2} \right\rangle \text{ là các ideal}$$

nguyên tố phân biệt của D và $N(\langle M_2 \rangle) = N(\langle \overline{M_2} \rangle) = 2$.

c) Nếu $m \equiv 2 \pmod{4}$ thì

$$\langle 2 \rangle = (M_2)^2 \text{ với } M_2 = \langle 2, \sqrt{m} \rangle \text{ là ideal nguyên tố của } D \text{ và } N(M_2)=2.$$

d) Nếu $m \equiv 3 \pmod{4}$ thì

$$\langle 2 \rangle = (M_2)^2 \text{ với } M_2 = \langle 2, 1 + \sqrt{m} \rangle \text{ là ideal nguyên tố của } D \text{ và } N(M_2)=2$$

Chứng minh

a) Trường hợp $m \equiv 5 \pmod{8}$

Giả sử rằng $\langle 2 \rangle = P_1 \cdot P_2$ ($P_1 \neq P_2$) hay $\langle 2 \rangle = P_1^2$; P_1, P_2 là các ideal nguyên tố

$$\Rightarrow N(P_1) = 2$$

$$\Rightarrow f_k(P_1) = 1$$

$$\Rightarrow \frac{D}{P_1} = \{ a + P_1 \mid a = 0; 1; \dots; p-1 \}$$

$$\text{Khi } m \equiv 5 \pmod{8} \Rightarrow D = \left\{ a + b \cdot \frac{1+\sqrt{m}}{2} \mid a, b \in \mathbb{Z} \right\}$$

$$\text{Với } \frac{1+\sqrt{m}}{2} \in D \text{ thì } \exists a \in \mathbb{Z} \text{ thỏa } \frac{1+\sqrt{m}}{2} \equiv a \pmod{P_1}$$

$$\Rightarrow \frac{1-\sqrt{m}}{2} = 1 - \frac{1+\sqrt{m}}{2} \equiv 1-a \pmod{P_1}$$

$$\Rightarrow \frac{1-m}{4} = \frac{1+\sqrt{m}}{2} \cdot \frac{1-\sqrt{m}}{2} \equiv a \cdot (1-a) \pmod{P_1}$$

Hơn nữa, do $\frac{1-m}{4} \in \mathbb{Z}$ (vì $m \equiv 5 \pmod{8}$); $a \cdot (1-a) \in \mathbb{Z}$ và $P_1 \nmid \langle 2 \rangle$

$$\Rightarrow \frac{1-m}{4} \equiv a \cdot (1-a) \pmod{2}$$

Do $a \in \mathbb{Z}$ nên $a \cdot (1-a) \equiv 0 \pmod{2}$

$$\Rightarrow \frac{1-m}{4} \equiv 0 \pmod{2}$$

$\Rightarrow m \equiv 1 \pmod{8}$ trái giả thiết $m \equiv 5 \pmod{8}$

Vậy $\langle 2 \rangle$ là ideal nguyên tố.

b) Trường hợp $m \equiv 1 \pmod{8}$

Đặt $M_2 = \langle 2, \frac{1+\sqrt{m}}{2} \rangle$, $\overline{M}_2 = \langle 2, \frac{1-\sqrt{m}}{2} \rangle$, ta có

$$\begin{aligned} M_2 \cdot \overline{M}_2 &= \langle 2, \frac{1+\sqrt{m}}{2} \rangle \cdot \langle 2, \frac{1-\sqrt{m}}{2} \rangle = \langle 4, 2 \cdot \frac{1+\sqrt{m}}{2}, 2 \cdot \frac{1-\sqrt{m}}{2}, \frac{1-m}{4} \rangle \\ &= \langle 2 \rangle \cdot I \text{ với } I = \langle 2, \frac{1+\sqrt{m}}{2}, \frac{1-\sqrt{m}}{2}, \frac{1-m}{8} \rangle \end{aligned}$$

$$\text{Do } 1 = \frac{1+\sqrt{m}}{2} + \frac{1-\sqrt{m}}{2} \in I \Rightarrow I = \langle 1 \rangle$$

$$\Rightarrow M_2 \cdot \overline{M}_2 = \langle 2 \rangle$$

+ Ta chứng minh $M_2, \overline{M}_2 \neq D$

Thật vậy, nếu $M_2 = D$, do $m \equiv 1 \pmod{8} \Rightarrow D = \{ a + b \cdot \frac{1+\sqrt{m}}{2} \mid a, b \in \mathbb{Z} \}$

$$\Rightarrow M_2 \cdot \overline{M}_2 = D \cdot \langle 2, \frac{1-\sqrt{m}}{2} \rangle = \langle 2 \rangle$$

$$\Rightarrow \langle 2 \rangle \cdot \langle 1, \frac{1-\sqrt{m}}{4} \rangle = \langle 2 \rangle$$

$$\Rightarrow \langle 1, \frac{1-\sqrt{m}}{4} \rangle = \{ a + b \cdot \frac{1+\sqrt{m}}{2} \mid a, b \in \mathbb{Z} \}$$

$$\Rightarrow \exists a, b \in \mathbb{Z} \text{ sao cho } \frac{1-\sqrt{m}}{4} = a + b \cdot \frac{1+\sqrt{m}}{2}$$

$$\Rightarrow \frac{b}{2} = \frac{-1}{4} \text{ hay } b = \frac{-1}{2} \text{ (vô lý)}$$

$$\Rightarrow M_2 \neq D, \text{ và tương tự } \overline{M}_2 \neq D.$$

+ Ta cũng có $M_2 \neq \overline{M}_2$ vì nếu $M_2 = \overline{M}_2 \Rightarrow 1 = \frac{1+\sqrt{m}}{2} + \frac{1-\sqrt{m}}{2} \in M_2$ (vô lý)

+ Bây giờ, do $M_2 \cdot \overline{M_2} = \langle 2 \rangle$

$$\Rightarrow N(M_2) \cdot N(\overline{M_2}) = N(M_2 \cdot \overline{M_2}) = N(\langle 2 \rangle) = 4$$

$$\Rightarrow N(M_2) = N(\overline{M_2}) = 2 \text{ vì } M_2, \overline{M_2} \neq D$$

$\Rightarrow M_2, \overline{M_2}$ là các ideal nguyên tố.

c) Trường hợp $m \equiv 2 \pmod{4}$

Đặt $M_2 = \langle 2, \sqrt{m} \rangle$, khi đó

$$M_2^2 = \langle 2, \sqrt{m} \rangle \cdot \langle 2, \sqrt{m} \rangle$$

$$= \langle 4, 2\sqrt{m}, m \rangle = \langle 2 \rangle \cdot I \text{ với } I = \langle 2, \sqrt{m}, m/2 \rangle$$

Do $m \equiv 2 \pmod{4}$ nên $m/2$ là số lẻ, đặt $m/2 = 2k+1, k \in \mathbb{Z}$

$$\Rightarrow 1 = (-k) \cdot 2 + 1 \cdot (m/2) \in I$$

$$\Rightarrow I = \langle 1 \rangle$$

$$\Rightarrow \langle 2 \rangle = M_2^2$$

Hơn nữa

$$N(M_2)^2 = N(M_2^2) = N(\langle 2 \rangle) = 4$$

$$\Rightarrow N(M_2) = 2$$

$\Rightarrow M_2$ là ideal nguyên tố.

d) Trường hợp $m \equiv 3 \pmod{4}$

Đặt $M_2 = \langle 2, 1 + \sqrt{m} \rangle$

Vì $1 - \sqrt{m} = 2 - (1 + \sqrt{m}) \in M_2$

Nên $M_2 = \langle 2, 1 + \sqrt{m}, 1 - \sqrt{m} \rangle$, khi đó

$$M_2^2 = \langle 2, 1 + \sqrt{m} \rangle \cdot \langle 2, 1 - \sqrt{m} \rangle = \langle 4, 2(1 + \sqrt{m}), 2(1 - \sqrt{m}), 1 - m \rangle$$

$$= \langle 2 \rangle \cdot I$$

với $I = \langle 2, (1 + \sqrt{m}), (1 - \sqrt{m}), \frac{1-m}{2} \rangle$

Vì $m \equiv 3 \pmod{4}$ nên $\frac{1-m}{2}$ là số lẻ suy ra $(2, \frac{1-m}{2}) = 1$, do đó có $x, y \in \mathbb{Z}$

sao cho

$$1 = x \cdot 2 + y \left(\frac{1-m}{2} \right) \in I$$

$$\Rightarrow I = \langle 1 \rangle \Rightarrow M_2^2 = \langle 2 \rangle$$

$$\Rightarrow N(M_2)^2 = N(M_2^2) = N(\langle 2 \rangle) = 4$$

$$\Rightarrow N(M_2) = 2 \Rightarrow M_2 \text{ là ideal nguyên tố.}$$

Ta chứng minh xong định lý 3.1.3

Tóm lại

$$\langle 2 \rangle = \begin{cases} \langle 2 \rangle & m \equiv 5 \pmod{8} \\ \left\langle 2, \frac{1+\sqrt{m}}{2} \right\rangle \cdot \left\langle 2, \frac{1-\sqrt{m}}{2} \right\rangle & m \equiv 1 \pmod{8} \\ \langle 2, \sqrt{m} \rangle^2 & m \equiv 2 \pmod{8} \\ \langle 2, 1+\sqrt{m} \rangle^2 & m \equiv 3 \pmod{8} \end{cases} \quad \text{khi}$$

Trong đó các ideal ở vế phải trong từng trường hợp tương ứng như $\langle 2 \rangle; \left\langle 2, \frac{1+\sqrt{m}}{2} \right\rangle; \left\langle 2, \frac{1-\sqrt{m}}{2} \right\rangle; \langle 2, \sqrt{m} \rangle; \langle 2, 1+\sqrt{m} \rangle$ đều là các ideal nguyên tố của D.

3.1.4 Định lý

Cho $K = \mathbb{Q}(\sqrt{m})$, m không chia hết cho số chính phương khác 1. Với p là số nguyên tố lẻ bất kỳ. Khi đó

a) nếu $p \mid m$ thì

$$\langle p \rangle = (M_p)^2 \text{ với } M_p = \langle p, \sqrt{m} \rangle \text{ là ideal nguyên tố của D và } N(M_p) = p.$$

b) nếu $\left(\frac{m}{p}\right) = 1$ thì $\langle p \rangle = M_p \cdot \overline{M_p}$ với $M_p = \langle p, a + \sqrt{m} \rangle, \overline{M_p} = \langle p, a - \sqrt{m} \rangle$,

$a^2 \equiv m \pmod{p}$, là các ideal nguyên tố phân biệt của D

$$\text{và } N(\langle M_p \rangle) = N(\langle \overline{M_p} \rangle) = p.$$

c) nếu $\left(\frac{m}{p}\right) = -1$ thì $\langle p \rangle$ là ideal nguyên tố của D và $N(\langle p \rangle) = p^2$

Chứng minh

a) Giả sử $p \mid m$

Đặt $M_p = \langle p, \sqrt{m} \rangle$, khi đó

$$M_p^2 = \langle p, \sqrt{m} \rangle \langle p, \sqrt{m} \rangle$$

$$= \langle p^2, p\sqrt{m}, m \rangle = \langle p \rangle \cdot I \quad \text{với } I = \langle p, \sqrt{m}, \frac{m}{p} \rangle$$

Do $m \not\equiv p^2, p \mid m$

$$\Rightarrow \left(p, \frac{m}{p}\right) = 1$$

Vì thế có $x, y \in \mathbb{Z}$ thỏa $1 = xp + y\left(\frac{m}{p}\right) \in I$

$$\Rightarrow I = \langle 1 \rangle$$

$$\Rightarrow \langle p \rangle = M_p^2.$$

$$\Rightarrow N(M_p)^2 = N(M_p)N(M_p) = N(M_p^2) = N(\langle p \rangle) = p^2$$

$$\Rightarrow N(M_p) = p \Rightarrow M_p \text{ là ideal nguyên tố.}$$

TH1 rơi vào phần a/

b) Giả sử $\left(\frac{m}{p}\right) = 1$

+ Do $\left(\frac{m}{p}\right) = 1$ nên có $a \in \mathbb{Z}$ thỏa $a^2 \equiv m \pmod{p}$. Vì $p^2 \nmid m$ nên $p \nmid a$. Ta đặt

$$M_p = \langle p, a + \sqrt{m} \rangle ; \overline{M_p} = \langle p, a - \sqrt{m} \rangle$$

Trước hết, ta chỉ ra rằng $M_p \neq \overline{M_p}$.

Giả sử $M_p = \overline{M_p}$,

khi đó

$$2a = (a + \sqrt{m}) + (a - \sqrt{m}) \in M_p \Rightarrow 2a \in M_p \cap \mathbb{Z} \Rightarrow p \mid 2a \Rightarrow p \mid a \text{ do } p > 2$$

Điều này trái giả thiết.

$\Rightarrow M_p, \overline{M_p}$ phân biệt.

+ Tiếp theo ta chứng minh $\langle p \rangle = M_p \overline{M_p}$, ta có

$$\begin{aligned} M_p \overline{M_p} &= \langle p, a + \sqrt{m} \rangle \langle p, a - \sqrt{m} \rangle \\ &= \langle p^2, p(a + \sqrt{m}), p(a - \sqrt{m}), a^2 - m \rangle \\ &= \langle p \rangle \left\langle p, (a + \sqrt{m}), (a - \sqrt{m}), \frac{a^2 - m}{p} \right\rangle \\ &= \langle p \rangle \cdot I \text{ với } I = \left\langle p, (a + \sqrt{m}), (a - \sqrt{m}), \frac{a^2 - m}{p} \right\rangle \end{aligned}$$

Do $(2a, p) = 1$ nên tồn tại $x, y \in \mathbb{Z}$ sao cho $x.p + y.(2a) = 1$

$$\Rightarrow 1 = x.p + y.(2a) = xp + y(a + \sqrt{m}) + y(a - \sqrt{m}) \in I$$

$$\Rightarrow I = \langle 1 \rangle.$$

Điều này chứng tỏ rằng $\langle p \rangle = M_p \overline{M_p}$

+ $M_p, \overline{M_p}$ là các ideal nguyên tố. Thật vậy

$$M_p = \langle p, a + \sqrt{m} \rangle = \langle \overline{p}, a - \sqrt{m} \rangle = \overline{\langle p, a - \sqrt{m} \rangle} = \overline{(\overline{M_p})}$$

$$\Rightarrow N(M_p) = N(\overline{(\overline{M_p})}) = N(\overline{M_p})$$

Mà

$$N(M_p).N(\overline{M_p}) = N(M_p \overline{M_p}) = N(\langle p \rangle) = p^2$$

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

$\Rightarrow M_p, \overline{M_p}$ là các ideal nguyên tố.

c) Trường hợp $\left(\frac{m}{p}\right) = -1$

Giả sử $\langle p \rangle$ không là ideal nguyên tố của D nguyên tố, khi đó

$$\langle p \rangle = P_1 P_2 \ (P_1 \neq P_2) \text{ hay } \langle p \rangle = (P_1)^2.$$

Trong mỗi trường hợp trên đều dẫn đến $f_k(P_1) = 1 \Rightarrow N(P_1) = p$.

Suy ra

$$D/P_1 = \{ a + P_1 \mid a = 0; 1; \dots; p-1 \} \text{ (theo định nghĩa 2.3.14)}$$

Với

$$\sqrt{m} \in D \Rightarrow \sqrt{m} + P_1 \in D/P_1$$

$$\Rightarrow \exists a \in \mathbb{Z} \text{ sao cho } \sqrt{m} \equiv a \pmod{P_1} \Rightarrow m \equiv a^2 \pmod{P_1}$$

Do $m \in \mathbb{Z}$, $a^2 \in \mathbb{Z}$, $P_1 \mid \langle p \rangle$ nên $m \equiv a^2 \pmod{p}$ trái giả thiết $\left(\frac{m}{p}\right) = -1$.

Vậy $\langle p \rangle$ là ideal nguyên tố của D .

Tóm lại, với số nguyên tố lẻ p ta có

$$\langle p \rangle = \begin{cases} \langle p, \sqrt{m} \rangle^2 & p \mid m \\ \langle p, a + \sqrt{m} \rangle \cdot \langle p, a - \sqrt{m} \rangle & \text{khi } p \nmid m, \left(\frac{m}{p}\right) = 1, a^2 \equiv m \pmod{p} \\ \langle p \rangle & p \nmid m, \left(\frac{m}{p}\right) = -1 \end{cases}$$

3.2 Ideal liên hợp

Khi $K = \mathbb{Q}(\sqrt{m})$, m không chia hết số chính phương khác 1, có đúng 2 đơn cấu trường

$$1, \sigma : K \rightarrow \mathbb{C}$$

với

$$1(a + b\sqrt{m}) = a + b\sqrt{m}$$

$$\sigma(a + b\sqrt{m}) = a - b\sqrt{m}$$

Gọi I là một ideal của D . Do I được sinh bởi nhiều nhất 2 phần tử nên ta có thể giả sử $I = \langle \alpha \rangle$ hay $I = \langle \alpha, \beta \rangle$. Ta định nghĩa ideal liên hợp của I như sau

$$\bar{I} = \sigma(I) = \langle \sigma(\alpha) \rangle \text{ hay } \langle \sigma(\alpha), \sigma(\beta) \rangle \text{ một cách tương ứng.}$$

Ta cũng kí hiệu $\bar{\alpha} = \sigma(\alpha)$

$$\text{Do } \overline{(\bar{\alpha})} = \sigma^2(\alpha) = \alpha \Rightarrow \overline{(\bar{I})} = I$$

Ta có

$$\begin{cases} \overline{(\alpha + \beta)} = \sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) = \bar{\alpha} + \bar{\beta} \\ \overline{(\alpha\beta)} = \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \bar{\alpha}\bar{\beta} \end{cases}; \forall \alpha, \beta \in K.$$

Từ những tính chất trên chúng ta kiểm chứng được rằng nếu $I = \langle \alpha_1, \dots, \alpha_n \rangle$ thì $\bar{I} = \langle \bar{\alpha}_1, \dots, \bar{\alpha}_n \rangle$.

3.2.1 Định lý

Cho I, J là các ideal của D . Khi đó $\overline{(IJ)} = \bar{I}\bar{J}$

Chứng minh

Vì $\langle \alpha \rangle = \langle \alpha, \alpha \rangle$ nên chúng ta có thể giả sử cả I, J đều được sinh bởi 2 phần tử

$$I = \langle \alpha, \beta \rangle; J = \langle \gamma, \delta \rangle$$

Khi đó

$$IJ = \langle \alpha, \beta \rangle \cdot \langle \gamma, \delta \rangle = \langle \alpha\gamma, \beta\gamma, \alpha\delta, \beta\delta \rangle$$

$$\Rightarrow \overline{IJ} = \langle \overline{\alpha\gamma}, \overline{\beta\gamma}, \overline{\alpha\delta}, \overline{\beta\delta} \rangle = \langle \bar{\alpha}\bar{\gamma}, \bar{\beta}\bar{\gamma}, \bar{\alpha}\bar{\delta}, \bar{\beta}\bar{\delta} \rangle = \langle \bar{\alpha}, \bar{\beta} \rangle \cdot \langle \bar{\gamma}, \bar{\delta} \rangle = \bar{I}\bar{J}$$

3.2.2 Định lý

$$\langle N(I) \rangle = I\bar{I}$$

Chứng minh

Do định lý đúng khi $I = \langle 0 \rangle, \langle 1 \rangle$ nên có thể giả sử $I \neq \langle 0 \rangle, \langle 1 \rangle$. Đặt

$$I = (P_1^{a_1} \bar{P}_1^{b_1} \dots P_r^{a_r} \bar{P}_r^{b_r}) (Q_1^{c_1} \dots Q_s^{c_s}) (R_1^{d_1} \dots R_t^{d_t}) \quad (*)$$

với P_i, Q_i, R_i là các ideal trong sự phân tích của I trong D , cụ thể hơn

+ $P_1 \dots P_r$ là các ideal nguyên tố phân biệt thỏa

$$P_i \cdot \bar{P}_i = \langle p_i \rangle; N(P_i) = N(\bar{P}_i) = p_i; P_i \neq \bar{P}_i$$

+ $Q_1 \dots Q_s$ là các ideal nguyên tố phân biệt thỏa $Q_i = \bar{Q}_i = \langle q_i \rangle; N(Q_i) = q_i^2$.

+ $R_1 \dots R_t$ là các ideal nguyên tố phân biệt thỏa $R_i = \bar{R}_i, R_i^2 = \langle r_i \rangle, N(R_i) = r_i$

và p_i, q_i, r_i là các số nguyên tố.

Theo 3.2.1 ta có

$$\begin{aligned} I &= (\bar{P}_1^{a_1} P_1^{b_1} \dots \bar{P}_r^{a_r} P_r^{b_r}) (Q_1^{c_1} \dots Q_s^{c_s}) (R_1^{d_1} \dots R_t^{d_t}) \\ \Rightarrow I\bar{I} &= (\bar{P}_1^{a_1+b_1} P_1^{a_1+b_1} \dots \bar{P}_r^{a_r+b_r} P_r^{a_r+b_r}) (Q_1^{2c_1} \dots Q_s^{2c_s}) (R_1^{2d_1} \dots R_t^{2d_t}) \\ &= \langle p_1 \rangle^{a_1+b_1} \dots \langle p_r \rangle^{a_r+b_r} \cdot \langle q_1 \rangle^{2c_1} \dots \langle q_s \rangle^{2c_s} \cdot \langle r_1 \rangle^{d_1} \dots \langle r_t \rangle^{d_t} \\ &= \langle p_1^{a_1+b_1} \dots p_r^{a_r+b_r} \cdot q_1^{2c_1} \dots q_s^{2c_s} \cdot r_1^{d_1} \dots r_t^{d_t} \rangle \end{aligned}$$

Hơn nữa, lấy chuẩn hai vế (*) ta thấy

$$N(I) = N(P_1)^{a_1} N(\bar{P}_1)^{b_1} \dots N(P_r)^{a_r} N(\bar{P}_r)^{b_r} N(Q_1)^{c_1} \dots N(Q_s)^{c_s} N(R_1)^{d_1} \dots N(R_t)^{d_t}$$

$$= p_1^{a_1} p_1^{b_1} \dots p_r^{a_r} p_r^{b_r} \cdot q_1^{2c_1} \dots q_s^{2c_s} \cdot r_1^{d_1} \dots r_t^{d_t}$$

Từ hai kết quả trên ta có kết quả cần chứng minh.

$$\langle N(I) \rangle = I \bar{I}.$$

3.3.3 Hệ quả

$$N(I) = N(\bar{I})$$

Chứng minh

Với I là ideal khác $\langle 0 \rangle$ của D ta có

$$\langle N(I) \rangle = I \bar{I} = \bar{I} I = \bar{I} (\bar{\bar{I}}) = \langle N(\bar{I}) \rangle$$

$\Rightarrow N(I) = \varepsilon N(\bar{I})$, với ε là một phần tử khả nghịch của D .

Do $N(I), N(\bar{I})$ là những số nguyên dương nên $\varepsilon = \pm 1$

$$\Rightarrow N(I) = N(\bar{I}).$$

Kết quả vẫn đúng khi $I = \langle 0 \rangle$.

3.3 Số học trên vành $D = \{ a + b\sqrt{-10} \mid a, b \in \mathbb{Z} \}$

Theo định lý 3.1.2 ta thấy $D = \{ a + b\sqrt{-10} \mid a, b \in \mathbb{Z} \}$ chính là vành các số nguyên đại số của trường $K = \mathbb{Q}(\sqrt{-10})$. Trong tiết này ta kí hiệu

$K = \mathbb{Q}(\sqrt{-10})$ và D là vành các số nguyên đại số của trường K . Ta có mệnh đề

3.3.1 Mệnh đề

Nếu $\alpha = a + b\sqrt{-10} \in D$ thì $N(\langle \alpha \rangle) = N(\alpha) = a^2 + 10b^2$.

Chứng minh

Xét hai trường hợp

. nếu $\alpha \in \mathbb{Q}$ thì $b=0$ và $\text{irr}_Q(\alpha) = x - \alpha$

$$\Rightarrow N(\alpha) = \alpha^2 = a^2 + 10b^2$$

. nếu $\alpha \notin \mathbb{Q}$ thì $\deg \text{irr}_Q(\alpha) = 2$ suy ra $\text{irr}_Q(\alpha) = (x - \alpha)(x - \bar{\alpha})$

$$\Rightarrow N(\alpha) = \alpha \cdot \bar{\alpha} = (a + b\sqrt{-10})(a - b\sqrt{-10}) = a^2 + 10b^2$$

Do $N(\langle \alpha \rangle) = |N(\alpha)|$

$$\Rightarrow N(\langle \alpha \rangle) = N(\alpha) = a^2 + 10b^2.$$

3.3.2 Ví dụ

Sự phân tích phần tử $10 \in D$ thành tích các phần tử bất khả quy là không duy nhất.

Ta thấy $10 = 2 \cdot 5 = -\sqrt{-10} \cdot \sqrt{-10}$, với $2, 5, \sqrt{-10}$ là các phần tử bất khả quy của D . Thật vậy

. Giả sử $2 = \alpha \cdot \beta$; $\alpha, \beta \in D$

$$\Rightarrow N(\alpha) \cdot N(\beta) = N(\alpha \beta) = N(2) = 4, \text{ khi đó có thể xảy ra các trường hợp sau}$$

- + nếu $N(\alpha)=4, N(\beta)=1 \Rightarrow \beta$ khả nghịch (theo định lý 2.3.6c)
- + nếu $N(\beta)=4, N(\alpha)=1 \Rightarrow \alpha$ khả nghịch.
- + nếu $N(\alpha) = N(\beta) = 2 \Rightarrow a^2+10b^2=2$ không thể xảy ra với $a,b \in \mathbb{Z}$.

Vậy 2 là phần tử bất khả quy.

. Giả sử $5 = \alpha \cdot \beta; \alpha, \beta \in D$

$$\Rightarrow N(\alpha) \cdot N(\beta) = N(\alpha \beta) = N(5) = 25$$

Khi đó có thể xảy ra các trường hợp sau

- + nếu $N(\alpha) = 25, N(\beta) = 1 \Rightarrow \beta$ khả nghịch
- + nếu $N(\beta) = 25, N(\alpha) = 1 \Rightarrow \alpha$ khả nghịch.
- + nếu $N(\alpha) = N(\beta) = 5 \Rightarrow a^2+10b^2=5$ không thể xảy ra với $a,b \in \mathbb{Z}$.

Vậy 5 là phần tử bất khả quy.

. Giả sử $\sqrt{-10} = \alpha \cdot \beta; \alpha, \beta \in D$

$\Rightarrow N(\alpha) \cdot N(\beta) = N(\alpha \beta) = N(\sqrt{-10}) = 10$, khi đó có thể xảy ra các trường hợp sau

- + nếu $N(\alpha)=10, N(\beta)=1 \Rightarrow \beta$ khả nghịch.
- + nếu $N(\beta)=10, N(\alpha)=1 \Rightarrow \alpha$ khả nghịch.
- + nếu $N(\alpha)=5, N(\beta)=2 \Rightarrow a^2+10b^2=2$ không thể xảy ra với $a,b \in \mathbb{Z}$.
- + nếu $N(\alpha)=2, N(\beta)=5$ không thể xảy ra.

Vậy $\sqrt{-10}$ là phần tử bất khả quy.

Qua ví dụ trên ta có thể nói D không phải là vành Gauss vì sự phân tích một phần tử thành tích các phần tử bất khả quy là không duy nhất.

3.3.3 Định lý

Với số nguyên tố p bất kỳ, ta có sự phân tích ideal chính $\langle p \rangle$ thành tích các ideal nguyên tố của D như sau:

a/

. nếu $p=2$ thì $\langle 2 \rangle = (M_2)^2$ với $M_2 = \langle 2, \sqrt{-10} \rangle, N(M_2) = 2$

. nếu $p=5$ thì $\langle 5 \rangle = (M_5)^2$ với $M_5 = \langle 5, \sqrt{-10} \rangle, N(M_5) = 5$

b/

. nếu p có dạng $40k+1, 40k+7, 40k+9, 40k+11, 40k+13, 40k+19, 40k+23$ và $40k+37$ thì

$$\langle p \rangle = M_p \cdot \overline{M_p} \text{ với } M_p = \langle p, a + \sqrt{-10} \rangle, \overline{M_p} = \langle p, a - \sqrt{-10} \rangle, a^2 + 10 \equiv 0 \pmod{p},$$

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

c/

. nếu p có dạng $40k+3, 40k+17, 40k+21, 40k+27, 40k+29, 40k+31, 40k+33$ và $40k+39$ thì $\langle p \rangle$ là ideal nguyên tố của D .

Chứng minh

Áp dụng định lý 3.1.3 khi $m = -10$, phần a/ được chứng minh trực tiếp, phần b/ ta chỉ cần chứng tỏ các số nguyên tố đó thỏa $\left(\frac{-10}{p}\right)=1$ và phần c/ tương ứng là $\left(\frac{-10}{p}\right)=-1$.

Cụ thể như sau:

a/

. Do $p=2$ và $-10 \equiv 2 \pmod{4} \Rightarrow \langle 2 \rangle = (M_2)^2$ với $M_2 = \langle 2, \sqrt{-10} \rangle$, $N(M_2) = 2$

. Do $5|-10$ và $p=5 > 2 \Rightarrow \langle 5 \rangle = (M_5)^2$ với $M_5 = \langle 5, \sqrt{-10} \rangle$, $N(M_5) = 5$

b/

Theo kết quả của công thức Legendre ta có

$$\left(\frac{-10}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) \left(\frac{5}{p}\right)$$

$$\text{Với } \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}; \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}; \left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$$

$$\text{Nên } \left(\frac{-10}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} \cdot \left(\frac{p}{5}\right) = (-1)^{\frac{p^2+4p-5}{8}} \left(\frac{p}{5}\right)$$

Bây giờ ta xét các trường hợp cụ thể của p

+ Khi $p = 40k + 1$ hay $40k + 11$ ta có

$$\frac{p^2+4p-5}{8} \text{ chẵn, } \left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1 \Rightarrow \left(\frac{-10}{p}\right) = 1$$

+ Khi $p = 40k + 7$ hay $40k + 37$ ta có

$$\frac{p^2+4p-5}{8} \text{ lẻ, } \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1 \Rightarrow \left(\frac{-10}{p}\right) = 1$$

+ Khi $p = 40k + 9$ hay $40k + 19$ ta có

$$\frac{p^2+4p-5}{8} \text{ chẵn, } \left(\frac{p}{5}\right) = \left(\frac{-1}{5}\right) = (-1)^{\frac{5-1}{2}} = 1 \Rightarrow \left(\frac{-10}{p}\right) = 1$$

+ Khi $p = 40k + 13$ hay $40k + 23$ ta có

$$\frac{p^2+4p-5}{8} \text{ lẻ, } \left(\frac{p}{5}\right) = \left(\frac{-2}{5}\right) = \left(\frac{-1}{5}\right) \left(\frac{2}{5}\right) = (1)(-1) = -1 \Rightarrow \left(\frac{-10}{p}\right) = 1$$

Vậy các số nguyên tố ở phần b/ thỏa $\left(\frac{-10}{p}\right)=1$.

c/ Ta chứng minh các số nguyên tố ở phần b/ thỏa $\left(\frac{-10}{p}\right) = -1$

+ Khi $p = 40k + 3$ hay $40k + 33$ ta có

$$\frac{p^2 + 4p - 5}{8} \text{ chẵn, } \left(\frac{p}{5}\right) = \left(\frac{-2}{5}\right) = -1 \Rightarrow \left(\frac{-10}{p}\right) = -1$$

+ Khi $p = 40k + 17$ hay $40k + 27$ ta có

$$\frac{p^2 + 4p - 5}{8} \text{ chẵn, } \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1 \Rightarrow \left(\frac{-10}{p}\right) = -1$$

+ Khi $p = 40k + 21$ hay $40k + 31$ ta có

$$\frac{p^2 + 4p - 5}{8} \text{ lẻ, } \left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1 \Rightarrow \left(\frac{-10}{p}\right) = -1$$

+ Khi $p = 40k + 29$ hay $40k + 39$ ta có

$$\frac{p^2 + 4p - 5}{8} \text{ lẻ, } \left(\frac{p}{5}\right) = \left(\frac{-1}{5}\right) = 1 \Rightarrow \left(\frac{-10}{p}\right) = -1$$

Vậy các số nguyên tố ở phần c/ thỏa $\left(\frac{-10}{p}\right) = -1$.

Ta **chứng minh** xong định lý.

3.3.5 Một số ví dụ

1/ Phân tích $\alpha = \langle 26 + 65\sqrt{-10} \rangle$ thành tích các ideal nguyên tố, tính $\varphi(\alpha)$.

Ta có $\alpha = \langle 13 \rangle . \langle 2 + 5\sqrt{-10} \rangle$

+ 13 có dạng $40k + 13$

nên $\langle 13 \rangle = M_{13} \overline{M_{13}}$; $M_{13} = \langle 13, 4 + \sqrt{-10} \rangle$, $\overline{M_{13}} = \langle 13, 4 + \sqrt{-10} \rangle$,

$N(M_{13}) = N(\overline{M_{13}}) = 13$

+ Đặt $\beta = \langle 2 + 5\sqrt{-10} \rangle \Rightarrow N(\beta) = 2^2 + 10 \cdot 5^2 = 254 = 2 \cdot 127$

. $\langle 2 \rangle = M_2^2$, $M_2 = \langle 2, \sqrt{-10} \rangle$, $N(M_2) = 2$

. 127 có dạng $40k + 7$

$\Rightarrow \langle 127 \rangle = \langle 127, 25 + \sqrt{-10} \rangle \langle 127, 25 - \sqrt{-10} \rangle = M_{127} \overline{M_{127}}$,

$N(M_{127}) = N(\overline{M_{127}}) = 127$

. Theo định lý 3.2.2 ta có $\beta \overline{\beta} = \langle N(\beta) \rangle = \langle 2 \rangle . \langle 127 \rangle = M_2^2 . M_{127} \overline{M_{127}}$

và $2 + 5\sqrt{-10} = 127 - 5(25 - \sqrt{-10}) \in \overline{M_{127}}$

nên $\beta = M_2 . \overline{M_{127}}$

$$+ \text{Vậy } \alpha = M_2 M_{13} \overline{M_{13}} \overline{M_{127}}$$

$$\Rightarrow \varphi(\alpha) = \varphi(M_2) \varphi(M_{13}) \varphi(\overline{M_{13}}) \varphi(\overline{M_{127}})$$

$$= (2-1).(13-1).(13-1).(127-1)=18144.$$

2/ Phân tích $\alpha = \langle 32395 + 6479\sqrt{-10} \rangle$ thành tích các ideal nguyên tố, tính $\varphi(\alpha)$.

$$\alpha = \langle 11 \rangle \langle 19 \rangle \langle 31 \rangle \langle 5 + \sqrt{-10} \rangle$$

+ 11 có dạng $40k + 11$

$$\text{nên } \langle 11 \rangle = M_{11} \overline{M_{11}}; M_{11} = \langle 11, 1 + \sqrt{-10} \rangle, \overline{M_{11}} = \langle 11, 1 - \sqrt{-10} \rangle,$$

$$N(M_{11}) = N(\overline{M_{11}}) = 11$$

+ 19 có dạng $40k + 19$

$$\text{nên } \langle 19 \rangle = M_{19} \overline{M_{19}}; M_{19} = \langle 19, 3 + \sqrt{-10} \rangle, \overline{M_{19}} = \langle 19, 3 - \sqrt{-10} \rangle,$$

$$N(M_{19}) = N(\overline{M_{19}}) = 19$$

+ 31 có dạng $40k + 31$ nên $\langle 31 \rangle = M_{31}$ là ideal nguyên tố, $N(M_{31}) = 31^2$

$$+ \text{Đặt } \beta = \langle 5 + \sqrt{-10} \rangle \Rightarrow N(\beta) = 5^2 + 10 = 35 = 5.7$$

$$\cdot \langle 5 \rangle = M_5^2, M_5 = \langle 5, \sqrt{-10} \rangle, N(M_5) = 5$$

$$\cdot \langle 7 \rangle = M_7 \overline{M_7}; M_7 = \langle 7, 2 + \sqrt{-10} \rangle, \overline{M_7} = \langle 7, 2 - \sqrt{-10} \rangle,$$

$$N(M_7) = N(\overline{M_7}) = 7$$

$$\cdot \text{Do } \beta \overline{\beta} = \langle N(\beta) \rangle = \langle 5 \rangle \langle 7 \rangle = M_5^2 \cdot M_7 \overline{M_7}$$

$$\text{và } 5 + \sqrt{-10} = 7 - (2 - \sqrt{-10}) \in \overline{M_7}$$

$$\text{nên } \beta = M_5 \cdot \overline{M_7}$$

$$+ \text{Vậy } \alpha = M_5 \overline{M_7} M_{11} \overline{M_{11}} M_{19} \overline{M_{19}} M_{31}$$

$$\Rightarrow \varphi(\alpha) = \varphi(M_5) \varphi(\overline{M_7}) \varphi(M_{11}) \varphi(\overline{M_{11}}) \varphi(M_{19}) \varphi(\overline{M_{19}}) \varphi(M_{31})$$

$$= (5-1).(7-1)(11-1).(11-1).(19-1).(19-1).(31^2-1)$$

$$= 746496000$$

3/ Phân tích $\alpha = \langle 12341 + 5289\sqrt{-10} \rangle$ thành tích các ideal nguyên tố, tính $\varphi(\alpha)$.

$$\alpha = \langle 41 \rangle \langle 43 \rangle \langle 7 + 3\sqrt{-10} \rangle$$

+ 41 có dạng $40k + 1$

$$\text{nên } \langle 41 \rangle = M_{41} \overline{M_{41}}; M_{41} = \langle 41, 20 + \sqrt{-10} \rangle, \overline{M_{41}} = \langle 41, 20 - \sqrt{-10} \rangle,$$

$$N(M_{41}) = N(\overline{M_{41}}) = 41$$

+ 43 có dạng $40k+3$ nên $\langle 43 \rangle = M_{43}$ là ideal nguyên tố, $N(M_{43}) = 43^2$
 + Đặt $\beta = \langle 7+3\sqrt{-10} \rangle \Rightarrow N(\beta) = 7^2+10.3^2 = 139$, vì 139 là số nguyên tố
 nên β là ideal nguyên tố của D, ta đưa β về dạng $M_p, \overline{M_p}$

. 139 có dạng $40k + 19$ nên $\langle 139 \rangle = M_{139} \overline{M_{139}}$; $M_{139} = \langle 139, 44 + \sqrt{-10} \rangle$,
 $\overline{M_{139}} = \langle 139, 44 - \sqrt{-10} \rangle$, $N(M_{139}) = N(\overline{M_{139}}) = 41$

. Do $\beta \overline{\beta} = \langle N(\beta) \rangle = \langle 139 \rangle = M_{139} \overline{M_{139}}$

và $7+3\sqrt{-10} = 139 - 3.(44 - \sqrt{-10}) \in \overline{M_{139}}$

nên $\beta = \overline{M_{139}}$

$\Rightarrow \alpha = M_{41} \overline{M_{41}} M_{43} \overline{M_{139}}$

$\Rightarrow \varphi(\alpha) = \varphi(M_{41})\varphi(\overline{M_{41}})\varphi(M_{43})\varphi(\overline{M_{139}})$
 $= (41-1)(41-1)(43^2-1)(139-1) = 408038400$

3.4 Số học trên vành $D = \{ a + b. \frac{1+\sqrt{-15}}{2} \mid a, b \in \mathbb{Z} \}$

Theo định lý 3.1.2 ta thấy $D = \{ a + b. \frac{1+\sqrt{-15}}{2} \mid a, b \in \mathbb{Z} \}$ chính là vành các số nguyên đại số của trường $K = \mathbb{Q}(\sqrt{-15})$. Trong tiết này ta kí hiệu $K = \mathbb{Q}(\sqrt{-15})$ và D là vành các số nguyên đại số của trường K. Ta có mệnh đề

3.4.1 Mệnh đề

Nếu $\alpha = a + b \frac{1+\sqrt{-15}}{2} \in D$ thì $N(\langle \alpha \rangle) = N(\alpha) = a^2 + ab + 4b^2$.

Chứng minh

Xét hai trường hợp

. nếu $\alpha \in \mathbb{Q}$ thì $b=0$ và $\text{irr}_{\mathbb{Q}}(\alpha) = x - \alpha$

$\Rightarrow N(\alpha) = \alpha^2 = a^2 = a^2 + ab + 4b^2$

. nếu $\alpha \notin \mathbb{Q}$ thì $\deg \text{irr}_{\mathbb{Q}}(\alpha) = 2$ suy ra $\text{irr}_{\mathbb{Q}}(\alpha) = (x - \alpha)(x - \overline{\alpha})$

$\Rightarrow N(\alpha) = \alpha \cdot \overline{\alpha} = (a + b \frac{1+\sqrt{-15}}{2}) \cdot (a + b \frac{1-\sqrt{-15}}{2}) = a^2 + ab + 4b^2$.

Do $N(\langle \alpha \rangle) = |N(\alpha)|$

$\Rightarrow N(\langle \alpha \rangle) = N(\alpha) = a^2 + ab + 4b^2$.

3.4.2 Ví dụ

1) Các phần tử 3; 5; $\sqrt{-15}$ là các phần tử bất khả quy của D.

Thật vậy

. Giả sử $3 = \alpha \cdot \beta$; $\alpha, \beta \in D$

$\Rightarrow N(\alpha) \cdot N(\beta) = N(\alpha\beta) = N(3) = 9$, khi đó có thể xảy ra các trường hợp sau
 + nếu $N(\alpha) = \pm 9$; $N(\beta) = \pm 1 \Rightarrow \beta$ khả nghịch.
 + nếu $N(\beta) = \pm 9$; $N(\alpha) = \pm 1 \Rightarrow \alpha$ khả nghịch.
 + nếu $N(\alpha) = N(\beta) = 3 \Rightarrow a^2 + ab + 4b^2 = 3$ không thể xảy ra với $a, b \in \mathbb{Z}$.
 + nếu $N(\alpha) = N(\beta) = -3 \Rightarrow a^2 + ab + 4b^2 = 3$ không thể xảy ra với $a, b \in \mathbb{Z}$.
 Vậy 3 là phần tử bất khả quy.

. Giả sử $5 = \alpha \cdot \beta$; $\alpha, \beta \in D$

$\Rightarrow N(\alpha) \cdot N(\beta) = N(\alpha\beta) = N(5) = 25$, khi đó có thể xảy ra các trường hợp sau

+ nếu $N(\alpha) = \pm 25$; $N(\beta) = \pm 1 \Rightarrow \beta$ khả nghịch.
 + nếu $N(\beta) = \pm 25$; $N(\alpha) = \pm 1 \Rightarrow \alpha$ khả nghịch.
 + nếu $N(\alpha) = N(\beta) = 5 \Rightarrow a^2 + ab + 4b^2 = 5$ hay $(2a+b)^2 + 15b^2 = 20$ không thể xảy ra với $a, b \in \mathbb{Z}$.
 + nếu $N(\alpha) = N(\beta) = -5 \Rightarrow a^2 + ab + 4b^2 = -5$ không thể xảy ra với $a, b \in \mathbb{Z}$.
 Vậy 5 là phần tử bất khả quy.

. Giả sử $\sqrt{-15} = \alpha \cdot \beta$; $\alpha, \beta \in D$

$\Rightarrow N(\alpha) \cdot N(\beta) = N(\alpha\beta) = N(\sqrt{-15}) = 15$, khi đó có thể xảy ra các trường hợp sau

+ nếu $N(\alpha) = \pm 15$; $N(\beta) = \pm 1 \Rightarrow \beta$ khả nghịch.
 + nếu $N(\beta) = \pm 15$; $N(\alpha) = \pm 1 \Rightarrow \alpha$ khả nghịch.
 + nếu $N(\alpha) = \pm 5$; $N(\beta) = \pm 3$ không thể xảy ra
 + nếu $N(\alpha) = \pm 3$; $N(\beta) = \pm 5$ không thể xảy ra

Vậy 3 là phần tử bất khả quy.

2) Trong D ta có sự phân tích

$$15 = 3 \cdot 5 = -\sqrt{-15} \cdot \sqrt{-15}$$

Qua ví dụ trên ta có thể nói D không phải là vành Gauss vì sự phân tích một phần tử thành tích các phần tử bất khả quy là không duy nhất.

3.4.3 Định lý

Với số nguyên tố p bất kỳ, ta có sự phân tích ideal chính $\langle p \rangle$ thành tích các ideal nguyên tố của D như sau:

a/

. nếu $p=2$ thì $\langle 2 \rangle = M_2 \overline{M_2}$ với $M_2 = \left\langle 2, \frac{1+\sqrt{-15}}{2} \right\rangle$, $\overline{M_2} = \left\langle 2, \frac{1-\sqrt{-15}}{2} \right\rangle$ là ideal

nguyên tố của D ; $N(M_2) = N(\overline{M_2}) = 2$

. nếu $p=3$ thì $\langle 3 \rangle = (M_3)^2$ với $M_3 = \langle 3, \sqrt{-15} \rangle$ là ideal nguyên tố của D ,

$$N(M_3) = 3$$

. nếu $p=5$ thì $\langle 5 \rangle = (M_5)^2$ với $M_5 = \langle 5, \sqrt{-15} \rangle$ là ideal nguyên tố của D ,

$$N(M_5) = 5$$

b/

. nếu p có dạng $15k+1, 15k+2, 15k+4, 15k+8$ thì

$$\langle p \rangle = M_p \cdot \overline{M_p} \text{ với } M_p = \langle p, a + \sqrt{-15} \rangle, \overline{M_p} = \langle p, a - \sqrt{-15} \rangle, N(M_p) = N(\overline{M_p}) = p,$$

$$a^2 + 15 \equiv 0 \pmod{p}$$

c/

. nếu p có dạng $15k+7, 15k+11, 15k+13, 15k+14$ thì $\langle p \rangle = M_p$ là ideal nguyên tố của D ; $N(M_p) = p^2$.

Chứng minh

Áp dụng định lý 3.1.3 khi $m = -15$, phần a/ được chứng minh trực tiếp, phần

b/ ta chỉ cần chứng tỏ các số nguyên tố đó thỏa $\left(\frac{-15}{p}\right) = 1$ và phần c/ tương

ứng là $\left(\frac{-15}{p}\right) = -1$.

Cụ thể như sau:

a/

. Do $p=2$ và $-15 \equiv 1 \pmod{8} \Rightarrow \langle 2 \rangle = M_2 \overline{M_2}$ với $M_2 = \left\langle 2, \frac{1+\sqrt{-15}}{2} \right\rangle$,

$\overline{M_2} = \left\langle 2, \frac{1-\sqrt{-15}}{2} \right\rangle$ là ideal nguyên tố của D ; $N(M_2) = N(\overline{M_2}) = 2$

. Do $p=3 \mid -15 \Rightarrow \langle 3 \rangle = (M_3)^2$ với $M_3 = \langle 3, \sqrt{-15} \rangle$ là ideal nguyên tố của D ,

$$N(M_3) = 3$$

. Do $p=5 \mid -15 \Rightarrow \langle 5 \rangle = (M_5)^2$ với $M_5 = \langle 5, \sqrt{-15} \rangle$ là ideal nguyên tố của D ,

$$N(M_5) = 5$$

Tiếp theo ta chứng minh b) và c).

Theo kết quả của công thức Legendre ta có

$$\left(\frac{-15}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) \left(\frac{5}{p}\right)$$

$$\text{Với } \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}; \left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{3}\right); \left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$$

Nên $\left(\frac{-15}{p}\right) = \left(\frac{p}{3}\right) \left(\frac{p}{5}\right)$; p là số nguyên tố lẻ.

Bây giờ ta xét các trường hợp cụ thể của p

+ Khi $p = 15k+1$ ta có

$$\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1; \left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1 \Rightarrow \left(\frac{-15}{p}\right) = 1$$

+ Khi $p = 15k + 2$ ta có

$$\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1; \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1 \Rightarrow \left(\frac{-15}{p}\right) = 1$$

+ Khi $p = 15k + 4$ ta có

$$\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1; \left(\frac{p}{5}\right) = \left(\frac{-1}{5}\right) = (-1)^{\frac{5-1}{2}} = 1 \Rightarrow \left(\frac{-15}{p}\right) = 1$$

+ Khi $p =$ ta có

$$\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1; \left(\frac{p}{5}\right) = \left(\frac{-2}{5}\right) = \left(\frac{-1}{5}\right)\left(\frac{2}{5}\right) = 1 \cdot (-1) = -1 \Rightarrow \left(\frac{-15}{p}\right) = 1$$

Vậy các số nguyên tố ở phần b/ thỏa $\left(\frac{-15}{p}\right) = 1$.

c/

Ta chứng minh các số nguyên tố ở phần c/ thỏa $\left(\frac{-15}{p}\right) = -1$

+ Khi $p = 15k+7$ ta có

$$\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1, \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1 \Rightarrow \left(\frac{-15}{p}\right) = -1$$

+ Khi $p = 15k + 11$ ta có

$$\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1, \left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1 \Rightarrow \left(\frac{-15}{p}\right) = -1$$

+ Khi $p = 15k + 13$ ta có

$$\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1, \left(\frac{p}{5}\right) = \left(\frac{-2}{5}\right) = -1 \Rightarrow \left(\frac{-15}{p}\right) = -1$$

+ Khi $p = 15k + 14$ ta có

$$\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1, \left(\frac{p}{5}\right) = \left(\frac{-1}{5}\right) = 1 \Rightarrow \left(\frac{-15}{p}\right) = -1$$

Vậy các số nguyên tố ở phần c/ thỏa $\left(\frac{-15}{p}\right) = -1$.

Ta **chứng minh** xong định lý.

3.4.5 Một số ví dụ

1/ Phân tích $\alpha = \left\langle \frac{15+5\sqrt{-15}}{2} \right\rangle$ thành tích các ideal nguyên tố, tính $\varphi(\alpha)$.

Ta có $\alpha = \langle 5 \rangle \cdot \left\langle \frac{3+\sqrt{-15}}{2} \right\rangle$

+ $\langle 5 \rangle = (M_5)^2$ với $M_5 = \langle 5, \sqrt{-15} \rangle$; $N(M_5) = 5$

+ Đặt $\beta = \left\langle \frac{3+\sqrt{-15}}{2} \right\rangle$

$\Rightarrow N(\beta) = 6$

$\Rightarrow \beta \bar{\beta} = \langle N(\beta) \rangle = \langle 6 \rangle = \langle 2 \rangle \cdot \langle 3 \rangle$

$\sqcup \langle 2 \rangle = M_2 \bar{M}_2 = \left\langle 2, \frac{1+\sqrt{-15}}{2} \right\rangle \cdot \left\langle 2, \frac{1-\sqrt{-15}}{2} \right\rangle$; $N(M_2) = N(\bar{M}_2) = 2$

$\sqcup \langle 3 \rangle = (M_3)^2 = \langle 3, \sqrt{-15} \rangle^2$, $N(M_3) = 3$

$\sqcup \frac{3+\sqrt{-15}}{2} = 2 - \frac{1-\sqrt{-15}}{2} \in \bar{M}_2$

$\Rightarrow \beta = \bar{M}_2 M_3$

$\Rightarrow \alpha = \bar{M}_2 M_3 (M_5)^2$

$\Rightarrow \varphi(\alpha) = (N(\bar{M}_2) - 1) \cdot (N(M_3) - 1) \cdot N(M_5) \cdot (N(M_5) - 1) = (2 - 1) \cdot (3 - 1) \cdot 5 \cdot (5 - 1) = 40$

2/ Phân tích $\alpha = \langle 84 - 42\sqrt{-15} \rangle$ thành tích các ideal nguyên tố, tính $\varphi(\alpha)$.

Ta có $\alpha = \langle 2 \rangle \langle 3 \rangle \langle 7 \rangle \cdot \langle 2 - \sqrt{-15} \rangle$

+ $\langle 2 \rangle = M_2 \bar{M}_2 = \left\langle 2, \frac{1+\sqrt{-15}}{2} \right\rangle \cdot \left\langle 2, \frac{1-\sqrt{-15}}{2} \right\rangle$; $N(M_2) = N(\bar{M}_2) = 2$

+ $\langle 3 \rangle = (M_3)^2 = \langle 3, \sqrt{-15} \rangle^2$, $N(M_3) = 3$

+ $\langle 7 \rangle = M_7$ là ideal nguyên tố.

+ Đặt $\beta = \langle 2 - \sqrt{-15} \rangle = \left\langle 3 - 2 \cdot \frac{1+\sqrt{-15}}{2} \right\rangle$

$\Rightarrow N(\beta) = 19$ (β là ideal nguyên tố)

$\Rightarrow \beta \bar{\beta} = \langle N(\beta) \rangle = \langle 19 \rangle = M_{19} \bar{M}_{19} = \langle 19; 2 + \sqrt{-15} \rangle \cdot \langle 19; 2 - \sqrt{-15} \rangle$

$\Rightarrow \beta = \bar{M}_{19}$

$\Rightarrow \alpha = M_2 \bar{M}_2 (M_3)^2 M_7 \bar{M}_{19}$

$\Rightarrow \varphi(\alpha) = (N(M_2) - 1)(N(\bar{M}_2) - 1) \cdot N(M_3)(N(M_3) - 1) \cdot N(M_7) \cdot (N(\bar{M}_{19}) - 1)$

$= (2 - 1) \cdot (2 - 1) \cdot 3 \cdot (3 - 1) \cdot (7^2 - 1) \cdot (19 - 1)$

$= 5184.$

KẾT LUẬN

Cho K là một trường mở rộng hữu hạn của Q và D là vành các số nguyên đại số của K . Sau quá trình nghiên cứu tính chất các ideal của vành D , chúng tôi đã thu được một số kết quả sau:

1/ Trong D , mọi ideal thật sự đều có thể biểu diễn được dưới dạng tích các ideal nguyên tố của D . Hơn nữa, tập các ideal khác không của D còn lập thành một nhóm Abel.

2/ Dựa vào sự phân tích thành tích các ideal nguyên tố, chúng tôi đã xây dựng được một số hàm số học cùng với các công thức tính của chúng. Cụ thể như sau:

- Hàm Euler $\varphi : P \rightarrow N^*$

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

- Định lý Euler

$$\text{Cho } a \in D, A \triangle D \text{ sao cho } (a, A) = 1. \text{ Khi đó}$$

$$a^{\varphi(A)} \equiv 1 \pmod{A}$$

- Hệ quả

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

- Định lý Wilson

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

$$\text{Nếu } \{\zeta_1, \dots, \zeta_s\} \text{ là hệ thặng dư thu gọn theo mod } P \text{ thì}$$

$$\zeta_1 \dots \zeta_s \equiv -1 \pmod{P}$$

3/ Dựa vào sự mô tả các ideal tối đại của vành D khi K là một trường bậc hai, chúng tôi đã xây dựng được thuật toán phân tích một phần tử của D thành tích các ideal tối đại.

Để minh họa cho các kết quả trên, chúng tôi đã khảo sát và áp dụng trong hai trường hợp cụ thể:

$$D = \{ a + b \cdot \sqrt{-10} \mid a, b \in \mathbb{Z} \}$$

và

$$D = \{ a + b \cdot \frac{1 + \sqrt{-15}}{2} \mid a, b \in \mathbb{Z} \}.$$

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. My Vinh Quang – Bài tập Đại số đại cương – NXB Giáo dục - 1999
2. Hoàng Xuân Sính – Số đại số Tập I- NXB Giáo dục – 2002
3. Hoàng Xuân Sính – Số đại số Tập II- NXB Đại học Sư Phạm – 2003

Tiếng Anh

1. L. Fuchs – Abelian Groups Pergamon Press – Oxford-London- NewYork- Pari -1960.
2. Saban Alaca and Kenneth S.William, Introductory Algebraic Number Thoery- Cambridge University Press-2004.
3. Z.I Borevich and I.R Shafarevich, Number Thoery- Academic Press- 1989.