ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

o0o

ĐINH CAO THƯỢNG

PHÂN TÍCH VÀNH THƯƠNG TRONG VÀNH CÁC SỐ NGUYÊN EISENSTEIN $\mathbb{Z}[\omega]$

THÁI NGUYÊN, 05/2017

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

———————o0o———————

ĐINH CAO THƯỢNG

PHÂN TÍCH VÀNH THƯƠNG TRONG VÀNH CÁC SỐ NGUYÊN EISENSTEIN $\mathbb{Z}[\omega]$

CHUYÊN NGÀNH: PHƯƠNG PHÁP TOÁN SƠ CẤP
MÃ SỐ: 60 46 01 13

LUẬN VĂN THẠC SĨ TOÁN HỌC

GIÁO VIÊN HƯỚNG DẪN:
GS.TS. LÊ THỊ THANH NHÀN

THÁI NGUYÊN, 05/2017

Mục lục

Mục lục 2

Lời cảm ơn 3

Phần mở đầu 4

1 Vành các số nguyên Eisenstein 6

1.1 Tính chia hết và miền nhân tử hóa 6
1.2 Miền iđêan chính và miền Euclid 12
1.3 Iđêan nguyên tố và iđêan tối đại 17
1.4 Một số tính chất của kí hiệu Legendre 20
1.5 Căn nguyên thủy của đơn vị 24
1.6 Vành các số nguyên Eisenstein $\mathbb{Z}[\omega]$ 27

2 Số nguyên tố Eisenstein, vành thương của $\mathbb{Z}[\omega]$ và sự phân tích 32

2.1 Số nguyên tố Eisenstein và vành thương của vành $\mathbb{Z}[\omega]$ 32
2.2 Phân tích vành thương của vành $\mathbb{Z}[\omega]$ 41

Kết luận 47

Tài liệu tham khảo 48

LỜI CẢM ƠN

Trước hết, tôi xin gửi lời biết ơn chân thành đến GS. TS. Lê Thị Thanh Nhàn đã hướng dẫn tôi hoàn thành bản luận văn này. Khi bắt đầu nhận đề tài thực sự tôi cảm nhận đề tài mang nhiều nội dung mới mẻ. Hơn nữa với vốn kiến thức ít ỏi cùng với kinh nghiệm làm đề tài lớn không nhiều nên tôi chưa thực sự tự tin để tiếp cận đề tài. Mặc dù rất bận rộn trong công việc nhưng Cô vẫn dành nhiều thời gian và tâm huyết trong việc hướng dẫn, động viên khuyến khích tôi trong suốt thời gian tôi thực hiện đề tài. Trong quá trình tiếp cận đề tài đến quá trình hoàn thiện luận văn Cô luôn tận tình chỉ bảo và tạo điều kiện tốt nhất nhất cho tôi hoàn thành luận văn. Cho đến bây giờ luận văn thạc sĩ của tôi đã được hoàn thành, xin cảm ơn Cô đã đôn đốc nhắc nhở tôi.

Tôi xin trân trọng cảm ơn Ban Giám hiệu, Khoa Toán - Tin và Phòng Đào tạo của trường Đại học Khoa học - Đại học Thái Nguyên. Tôi xin trân trọng cảm ơn các Thầy, Cô đã tận tình truyền đạt những kiến thức quý báu cũng như tạo mọi điều kiện thuận lợi nhất để tôi hoàn thành luận văn này.

Tôi xin trân trọng cảm ơn Ban giám hiệu, các thầy cô giáo trường THPT Kim Sơn A - Ninh Bình nơi tôi công tác đã tạo điều kiện giúp đỡ tôi hoàn thành công việc chuyên môn tại nhà trường để tôi hoàn thành chương trình học tập cao học.

Cuối cùng, tôi xin chân thành bày tỏ lòng biết ơn đến gia đình, bạn bè, những người không ngừng động viên, hỗ trợ tạo mọi điều kiện tốt nhất cho tôi trong suốt quá trình học tập và thực hiện luận văn.

PHẦN MỞ ĐẦU

Như chúng ta đã biết, vành các số nguyên $\mathbb{Z}$ là một miền Euclid, và do đó nó là một miền nhân tử hóa và là miền iđêan chính. Các iđêan của $\mathbb{Z}$ có dạng

$$m\mathbb{Z} = \{km \mid \ k \in \mathbb{Z}\} = (m)$$

với $m \in \mathbb{Z}, m \geq 0$. Nếu $m > 0$ thì vành thương của $\mathbb{Z}$ có dạng $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$, được gọi là vành các số nguyên modulo m. Trong vành các số nguyên $\mathbb{Z}$, mọi phần tử khác 0 và không khả nghịch đều phân tích thành tích các phần tử nguyên tố. Phân tích này là duy nhất nếu không kể đến thứ tự các nhân tử nguyên tố và các nhân tử là ước của đơn vị. Do $\mathbb{Z}$ là miền iđêan chính nên mọi iđêan I của $\mathbb{Z}$ đều là iđêan chính. Giả sử $I = (m)$ là iđêan sinh bởi $m > 0$. Nếu $m = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ là phân tích tiêu chuẩn của m thành tích các thừa số nguyên tố thì theo Định lý Trung Hoa ta có phân tích duy nhất

$$\mathbb{Z}_m \cong \mathbb{Z}/I = \mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p_t^{\alpha_t}}.$$

Cho $\omega = \dfrac{-1 + i\sqrt{3}}{2}$ là một căn nguyên thủy bậc ba của đơn vị. Đặt

$$\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}.$$

Khi đó $\mathbb{Z}[\omega]$ cùng với hai phép toán cộng và nhân

$$(a + b\omega) + (c + d\omega) = (a + c) + (b + d)\omega,$$

$$(a + b\omega)(c + d\omega) = (ac - bd) + (ad + bc - bd)\omega$$

là một miền nguyên, được gọi là *vành các số nguyên Eisenstein.*

Cấu trúc của vành $\mathbb{Z}[\omega]$ và vành thương của nó được nghiên cứu bởi M. Misaghian trong bài báo [Mi]: "*Factor rings and their decompositions in the Eisenstein integer ring* $\mathbb{Z}[\omega]$" xuất bản năm 2013. Mục đích của luận văn này là trình bày lại các kết quả trong bài báo trên. Luận văn quan tâm khai thác tính chất Euclid của vành $\mathbb{Z}[\omega]$, xác định các số nguyên tố Eisenstein, phân tích các số nguyên Eisenstein thành thừa số nguyên tố Eisenstein và cấu trúc của vành thương của vành $\mathbb{Z}[\omega]$.

Luận văn chia làm hai chương.

Chương 1 trình bày một số kiến thức cơ bản về miền nhân tử hóa, miền iđêan chính, miền Euclid và mối quan hệ giữa chúng. Hơn thế nữa, luận văn trình bày một số tính chất của kí hiệu Legendre, căn nguyên thủy của đơn vị. Đặc biệt phát biểu và chứng minh tính chất Euclid của vành các số nguyên Eisenstein $\mathbb{Z}[\omega]$.

Chương 2 gồm hai phần. Phần đầu trình bày tính chất của số nguyên tố Eisentein và cấu trúc vành thương của vành $\mathbb{Z}[\omega]$, thể hiện trong Định lý 2.1.8 và Định lý 2.1.12. Phần cuối luận văn trình bày sự phân tích vành thương của vành $\mathbb{Z}[\omega]$ (xem Định lý 2.2.4), đồng thời đưa ra một số ví dụ minh họa. Nếu phân tích của vành thương của vành $\mathbb{Z}$ là duy nhất thì Ví dụ 2.2.6 chỉ ra rằng sự phân tích của vành thương của vành các số nguyên Eisenstein $\mathbb{Z}[\omega]$ không duy nhất.

Chương 1

Vành các số nguyên Eisenstein

Mục đích của chương này là trình bày các tính chất cơ sở của vành các số nguyên Eisenstein. Tài liệu tham khảo chính của Chương là [H], [N], [M], [Mi].

1.1 Tính chia hết và miền nhân tử hóa

Trong suốt mục này ta luôn xét D là một miền nguyên.

1.1.1 Định nghĩa. Cho a, b là hai phần tử của D

(i) Cho $b \neq 0$. Ta nói b là một *ước* của a (hay a là bội của b), kí hiệu là $b|a$, nếu tồn tại $q \in D$ sao cho $a = bq$. Nếu b là ước của a thì ta còn nói b *chia hết* a hoặc a *chia hết cho* b.

(ii) Nếu tồn tại $q \in D$ để $1 = bq$ thì ta nói b là *ước của đơn vị*.

(iii) Cho $0 \neq a$ và $0 \neq b$. Ta nói a liên kết b, kí hiệu là $a \sim b$, nếu $a|b$ và $b|a$. Nếu a không liên kết với b thì ta kí hiệu $a \nsim b$.

(iv) Cho b là một ước của a. Ta nói b là *ước thực sự* của a, kí hiệu $b \,||\, a$, nếu $b \nsim 1$ và $b \nsim a$. Các ước của a liên kết với 1 hoặc liên kết với a được gọi là các ước tầm thường của a.

1.1.2 Mệnh đề. *Cho $0 \neq a$, $b \in D$. Khi đó a liên kết b khi và chỉ khi chúng chỉ sai khác nhau bởi một nhân tử là ước của đơn vị.*

Chứng minh. Giả sử a và b là liên kết. Khi đó tồn tại $c, d \in D$ sao cho $a = cb$ và $b = da$. Suy ra $a = cb = cda$. Do D là miền nguyên và $a \neq 0$ nên $1 = cd$. Vậy cả c và d là ước của đơn vị và do đó a và b chỉ khác nhau một nhân tử là ước của đơn vị. Ngược lại, giả sử $a = cb$ với c là một ước của đơn vị. Khi đó $b|a$. Do $c|1$ nên tồn tại $d \in D$ sao cho $1 = cd$. Vì thế ta có $ad = b(cd) = b$. Suy ra $a|b$. Vậy a và b liên kết với nhau. $\square$

1.1.3 Định nghĩa. Cho $p \in D$ là một phần tử khác không và khác ước của đơn vị.

(i) p được gọi là *phần tử bất khả quy* nếu p không có ước thực sự.

(ii) p được gọi là *phần tử nguyên tố* nếu $p|ab$ kéo theo $p|a$ hoặc $p|b$ với mọi $a, b \in D$.

Trong vành $\mathbb{Z}$ các số nguyên, các khái niệm phần tử bất khả quy và phần tử nguyên tố là tương đương. Trong trường hợp tổng quát, nhìn chung hai khái niệm này không tương đương. Tuy nhiên ta có tính chất sau đây.

1.1.4 Mệnh đề. *Mọi phần tử nguyên tố đều bất khả quy.*

Chứng minh. Giả sử $a|p$. Khi đó tồn tại $b \in D$ để $p = ab$. Suy ra $p|ab$. Do p nguyên tố nên $p|a$ hoặc $p|b$. Nếu $p|a$ thì $a \sim p$. Nếu $p|b$ thì $p \sim b$ và do đó p và b chỉ sai khác nhau nhân tử là ước của đơn vị, tức là a là ước của đơn vị. $\square$

Ví dụ sau đây chỉ ra rằng điều ngược lại của Mệnh đề 1.1.4 là không đúng.

1.1.5 Ví dụ. Lấy $D = \{a + b\sqrt{-5} \,|\, a, b \in \mathbb{Z}\}$. Vì D là vành con của trường số phức nên D là một miền nguyên. Ta khẳng định các phần tử $2, 3, 1 + \sqrt{-5}$ và $1 - \sqrt{-5}$ là bất khả quy nhưng không là phần tử nguyên tố. Thật vậy, với mỗi $r = a + b\sqrt{-5} \in D$, gọi $\overline{r}$ là số phức liên hợp với r. Ta định nghĩa *chuẩn* của r, kí hiệu là $N(r)$ là số $N(r) = r\overline{r} = a^2 + 5b^2$. Do liên hợp của tích hai số phức bằng tích các liên hợp nên ta có $N(rs) = rs.\overline{rs} = r\overline{r}s\overline{s} = N(r)N(s)$. Ta có $6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Trước hết ta chứng minh số 2 là phần tử bất khả quy nhưng không nguyên tố. Giả sử $r = a + b\sqrt{-5}$ là một ước của 2. Khi đó tồn tại $s \in D$ sao cho $2 = rs$. Suy ra $4 = N(2) = N(r)N(s)$. Do đó $N(r)$ chỉ có thể là $1, 2, 4$. Nếu $N(r) = 1 = a^2 + 5b^2$ thì $a = \pm 1$ và $b = 0$, do đó r là ước của đơn vị. Nếu $N(r) = 2$ thì $a^2 + 5b^2 = 2$. Rõ ràng không xảy ra trường hợp này. Nếu $N(r) = 4 = a^2 + 5b^2$ thì $a = \pm 2$ và $b = 0$, do đó r liên kết với 2. Vậy số 2 là phần tử bất khả quy. Bây giờ ta chứng minh số 2 không là phần tử nguyên tố. Thật vậy, giả sử số 2 là phần tử nguyên tố. Vì $2|(1 + \sqrt{-5})(1 - \sqrt{-5})$ nên 2 là ước của một trong hai thừa số đó. Giả sử 2 là ước của $1 + \sqrt{-5}$. Khi đó tồn tại $r = a + b\sqrt{-5} \in D$ sao cho $2r = 1 + \sqrt{-5}$. Suy ra

$$4(a^2 + 5b^2) = N(2)N(r) = N(2r) = N(1 + \sqrt{-5}) = 6$$

Điều này là vô lý vì trong vành số nguyên, 4 không thể là ước của 6. Tương tự nếu 2 là ước của $1 - \sqrt{-5}$ thì ta cũng suy ra điều vô lý. Vậy 2 không là phần tử nguyên tố.

Bằng cách tương tự, ta có thể kiểm tra được các phần tử $2, 1 - \sqrt{-5}, 1 + \sqrt{-5}$ cũng là bất khả quy nhưng không nguyên tố.

1.1.6 Định nghĩa. Một miền nguyên D được gọi là *miền nhân tử hóa* (vành nhân tử hóa) nếu mỗi phần tử khác 0 và khác ước của đơn vị của D đều phân tích được thành tích những phần tử bất khả quy và sự phân tích đó là duy nhất nếu không kể đến thứ tự và các nhân tử là ước của đơn vị.

Ví dụ đơn giản nhất cho miền nhân tử hóa là vành $\mathbb{Z}$ các số nguyên. Từ đầu thế kỉ 19, nhà toán học người Đức C. F. Gauss đã chứng minh được rằng các vành đa thức nhiều biến $\mathbb{Z}[x_1, \ldots, x_n]$ và $\mathbb{Q}[x_1, \ldots, x_n]$ có hệ số tương ứng trong vành số nguyên và trường số hữu tỉ đều là những miền nhân tử hóa. Chính vì vậy, nhiều tài liệu đại số đã gọi miền nhân tử hóa là vành Gauss.

Cho $a, b \in D$. Phần tử $0 \neq d \in D$ được gọi là một ước chung lớn nhất của a và b nếu d là một ước chung của a, b và là bội của mọi ước chung khác của a, b. Chú ý rằng với d, d' là hai ước chung lớn nhất của a và b, thì tồn tại phần tử khả nghịch $u \in D$ sao cho $d = d'u$. Đặc biệt, trong vành $\mathbb{Z}$ các số nguyên, nếu d là ước chung lớn nhất của a, b thì $-d$ cũng là ước chung lớn nhất của a, b.

Miền nguyên D được gọi là thỏa mãn điều kiện có ước chung lớn nhất nếu hai phần tử bất kỳ của D không đồng thời bằng 0 đều có ước chung lớn nhất. Chẳng hạn, vành các số nguyên $\mathbb{Z}$ thỏa mãn điều kiện có ước chung lớn nhất.

Miền nguyên D được gọi là thỏa mãn điều kiện dãy dừng các ước thực sự nếu với mọi phần tử $a_1, a_2, a_3, \ldots$ trong D thỏa mãn điều kiện $a_2|a_1, a_3|a_2, \ldots$ đều phải dừng. Chẳng hạn, vành các số nguyên $\mathbb{Z}$ thỏa mãn điều kiện dãy dừng những ước thực sự.

Tiếp theo là một số tính chất của miền nguyên thỏa mãn điều kiện có ước chung lớn nhất và điều kiện dãy dừng các ước thực sự.

1.1.7 Bổ đề. *Cho D là miền nguyên thỏa mãn điều kiện dãy dừng các ước thực sự. Khi đó các phát biểu sau là đúng:*

(i) Mọi phần tử khác không và không khả nghịch đều có một ước bất khả quy.

(ii) Mọi phần tử khác không và không khả nghịch đều phân tích được thành tích các nhân tử bất khả quy.

Chứng minh. (i). Cho $a \in D$ là phần tử khác không và không khả nghịch. Nếu a là bất khả quy thì a chính là ước bất khả quy của a. Nếu a không là bất khả quy thì a có ước thực sự là a_1. Nếu a_1 là bất khả quy thì ta có điều cần chứng minh. Nếu a_1 không bất khả quy thì a_1 có ước thực sự là a_2. Tiếp tục quá trình trên ta được một dãy các ước thực sự. Dãy này phải dừng nên a có ước bất khả quy.