ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

PHẠM XUÂN HÙNG

PHÂN TÍCH VÀNH THƯƠNG CỦA VÀNH CÁC SỐ NGUYÊN GAUSS

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2017

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

PHẠM XUÂN HÙNG

PHÂN TÍCH VÀNH THƯƠNG CỦA VÀNH CÁC SỐ NGUYÊN GAUSS

LUẬN VĂN THẠC SĨ TOÁN HỌC

Chuyên ngành: Phương pháp Toán sơ cấp
Mã số: 60 46 01 13

NGƯỜI HƯỚNG DẪN KHOA HỌC
GS.TS. LÊ THỊ THANH NHÀN

THÁI NGUYÊN - 2017

Mục lục

Lời cảm ơn

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 luân tận tình chỉ bảo và tạo điều kiện tốt nhất cho tôi. 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 quí báu cũng như tạo mọi điều kiện thuận lợi nhất để tôi hoàn thành luận văn này.

Cuối cùng, tôi xin chân thành bày tỏ lòng biết ơn đến gia đình, bạn bè, những người đã 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.

Lời nói đầu

Các số phức có dạng $a + bi$ với $a, b \in \mathbb{Z}$ được gọi là *các số nguyên Gauss*. Tập các số nguyên Gauss làm thành một vành với phép cộng và nhân các số phức. Vành này được kí hiệu là $\mathbb{Z}[i]$, và được gọi là *vành các số nguyên Gauss*.

Chú ý rằng mỗi vành thương của $\mathbb{Z}$ có dạng $\mathbb{Z}/m\mathbb{Z}$ với $m > 0$. Vành thương này có thể đồng nhất với vành $\mathbb{Z}_m$. Một kết quả quen biết về phân tích vành $\mathbb{Z}_m$ thành tổng trực tiếp như sau: Nếu $m = p_1^{t_1} \ldots p_k^{t_k}$ là phân tích tiêu chuẩn của m thì $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{t_1}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{t_k}}$. Mục tiêu của luận văn là phát triển kết quả trên cho vành thương của vành các số nguyên Gauss. Chúng tôi trình bày lại chi tiết các kết quả trong bài báo của G. Dresden, W. Dymacek (2005), *"Finding factors of factor rings over the Gaussian Integers"* đăng trên tạp chí "American Math. Monthly" về phân tích vành thương của vành $\mathbb{Z}[i]$. Chúng tôi cũng quan tâm khai thác các ứng dụng của vành các số nguyên Gauss để giải những bài toán sơ cấp cổ điển như bài toán tìm điều kiện để một số tự nhiên là tổng của hai số chính phương, bài toán tìm các bộ số Pythagore.

Luận văn gồm 2 Chương. Trong Chương 1, Tiết 1.1 dành để nhắc lại một số khái niệm về miền phân tích duy nhất, miền iđêan chính và miền Euclid. Tiết tiếp theo trình bày sự phân tích vành thương của vành $\mathbb{Z}$ các số nguyên thành tổng trực tiếp của những vành đơn giản hơn (Mệnh đề 1.2.5). Phần cuối Chương 1 trình bày một số kết quả về vành $\mathbb{Z}[i]$ các số nguyên Gauss, trong đó quan tâm đặc biệt đến việc xác định các phần tử khả nghịch (Bổ đề 1.3.2), chứng minh $\mathbb{Z}[i]$ là miền Euclid (Định lí 1.3.4), và đặc trưng phần tử nguyên tố trong vành các số nguyên Gauss (Định lí 1.3.5).

Trong Chương 2, phần đầu Chương trình bày bài toán phân tích vành thương của vành $\mathbb{Z}[i]$ thành tổng trực tiếp của những vành đơn giản hơn. Hai tiết còn lại (Tiết 2.2 và Tiết 2.3) dành để khai thác các kết quả của vành $\mathbb{Z}[i]$ để giải quyết hai bài toán sơ cấp kinh điển: tìm điều kiện để một số tự nhiên là tổng của hai số chính phương (Định lí 2.2.1, Định lí 2.2.5), bài toán tìm các bộ số Pythagore (Định lí 2.3.4).

Chương 1

Vành các số nguyên Gauss

Các số phức có dạng $a + bi$ với $a, b \in \mathbb{Z}$ được gọi là *các số nguyên Gauss* (Carl Friedrich Gauss là người đầu tiên nghiên cứu các số phức này). Tập các số nguyên Gauss làm thành một vành, được kí hiệu là $\mathbb{Z}[i]$, và được gọi là *vành các số nguyên Gauss*.

Mục tiêu của Chương 1 là trình bày các tính chất cơ sở của vành các số nguyên Gauss. Phần đầu Chương nhắc lại một số khái niệm về miền phân tích duy nhất, miền iđêan chính và miền Euclid. Phần tiếp theo trình bày sự phân tích vành thương của vành $\mathbb{Z}$ các số nguyên thành tổng trực tiếp của những vành đơn giản hơn. Phần cuối trình bày về vành $\mathbb{Z}[i]$ các số nguyên Gauss, trong đó quan tâm đặc biệt đến việc xác định các phần tử khả nghịch, việc chứng minh $\mathbb{Z}[i]$ là miền Euclid, và việc đặc trưng các số nguyên tố Gauss.

Carl Friedrich Gauss (sinh ngày 30 tháng 4 năm 1777, mất ngày 23 tháng 2 năm 1855) là một nhà Toán học và là nhà Khoa học thiên tài người Đức. Ông có những đóng góp lớn cho Khoa học, đặc biệt là trong Lí thuyết số, Giải tích, Hình học vi phân, Khoa học trắc địa, Từ học, Tĩnh điện học, Thiên văn học và Quang học. Với những ảnh hưởng sâu sắc trong Khoa học, đặc biệt là trong Toán học, Carl Friedrich Gauss được xếp ngang với những thiên tài Leonhard Euler, Isaac Newton và

Archimedes - những nhà Toán học vĩ đại nhất của lịch sử.

1.1 Miền phân tích duy nhất

Chúng ta đều biết rằng, trong miền nguyên $\mathbb{Z}$, mỗi số nguyên dương $n > 1$ đều có một phân tích tiêu chuẩn $n = p_1^{r_1} \ldots p_k^{r_k}$, trong đó $p_1, \ldots, p_k$ là những số nguyên tố đôi một phân biệt và $r_1, \ldots, r_k$ là những số nguyên dương. Sự phân tích tiêu chuẩn của n là duy nhất nếu không kể đến thứ tự của các nhân tử. Vấn đề đặt ra là những miền nguyên nào có tính chất phân tích duy nhất tương tự như vành các số nguyên $\mathbb{Z}$? Mục đích của tiết này là giải quyết vấn đề trên. Những miền nguyên có tính chất này được gọi là *miền phân tích duy nhất* - Unique Factorization Domain (UFD) hay *miền nhân tử hóa*. Đôi khi miền phân tích duy nhất còn được gọi là *miền Gauss*, vì Carl Friedrich Gauss là người đầu tiên nghiên cứu loại miền nguyên này. Ông cũng là người có đóng góp rất quan trọng trong việc phát triển lí thuyết chia hết từ vành các số nguyên $\mathbb{Z}$ sang các miền phân tích duy nhất.

Trong Chương I, luôn giả thiết D là một miền nguyên, tức D là vành giao hoán khác $\{0\}$ và nếu $a, b \neq 0$ là hai phần tử của D thì $ab \neq 0$. Trước khi trình bày khái niệm miền phân tích duy nhất, chúng ta nhắc lại một số khái niệm về ước, bội, phần tử nguyên tố, phần tử bất khả quy.

1.1.1 Định nghĩa. Cho $a, b \in D$, $b \neq 0$. Ta nói b là *ước* của a (hay a là *bội* của b), nếu tồn tại $q \in D$ sao cho $a = bq$. Nếu tồn tại $q \in D$ để $1 = bq$ thì ta nói b là *phần tử khả nghịch* hay b *là ước của đơn vị*. Ta nói a và b là *liên kết,* viết là $a \sim b$, nếu đồng thời a là ước của b và b là ước của a. Nếu b là ước của a và a không là ước của b thì ta nói b là *ước thực sự của a*.

Chú ý rằng a và b liên kết với nhau nếu và chỉ nếu chúng chỉ khác nhau một nhân tử là ước của đơn vị, tức là tồn tại một phần tử khả nghịch $u \in D$ sao cho $a = bu$.

1.1.2 Định nghĩa. Cho $p \in D$. Ta nói p là *phần tử bất khả quy* nếu p khác 0, không khả nghịch và có ước thực sự. Ta nói p là *phần tử nguyên tố* nếu p khác 0, không khả nghịch và nếu p là ước của tích ab thì p là ước của a hoặc p là ước của b với mọi $a, b \in D$.

Trong miền nguyên $\mathbb{Z}$, các phần tử bất khả quy là và chỉ là các số nguyên tố. Trong miền nguyên D bất kì, nếu p là phần từ nguyên tố thì p là bất khả quy. Tuy nhiên, điều ngược lại không đúng. Chẳng hạn, xét miền nguyên

$$D = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}.$$

Các phần tử $2, 3, 1 + i\sqrt{5}$ và $1 - i\sqrt{5}$ là bất khả quy nhưng không là phần tử nguyên tố, vì ta có phân tích

$$6 = 2.3 = (1 + i\sqrt{5})(1 - i\sqrt{5}),$$

trong đó $2, 3$ là ước của tích $(1 + i\sqrt{5})(1 - i\sqrt{5})$ nhưng 2 và 3 không là ước của $1 + i\sqrt{5}$ và cũng không là ước của $1 - i\sqrt{5}$. Tương tự, $1 + i\sqrt{5}$ và $1 - i\sqrt{5}$ là ước của tích 2.3, nhưng $1 + i\sqrt{5}$ và $1 - i\sqrt{5}$ không là ước của 2 và cũng không là ước của 3.

1.1.3 Định nghĩa. Miền nguyên D được gọi là *miền phân tích duy nhất* nếu mỗi phần tử khác 0 và không khả nghịch 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 các nhân tử và cũng không kể đến các nhân tử là ước của đơn vị. Miền phân tích duy nhất (Unique Factorization Domain) còn được gọi là *miền nhân tử hoá* hay *miền Gauss.*

Ví dụ đơn giản cho miền phân tích duy nhất là miền nguyên $\mathbb{Z}$. Miền phân tích duy nhất tiếp theo là *vành các số nguyên Gauss* $\mathbb{Z}[i]$ (sẽ được nghiên cứu trong Tiết 2.3), được giới thiệu và khám phá bởi nhà toán học người Đức Carl Friedrich Gauss trong bài báo năm 1828 của ông nói về các thặng dư bậc hai.

Để trình bày đặc trưng của miền phân tích duy nhất, chúng ta cần đến điều kiện dãy dừng các ước thực sự và điều kiện có ước chung lớn nhất.

1.1.4 Định nghĩa. Cho $a_1, a_2, a_3, \ldots$ là dãy các phần tử của D sao cho a_{i+1} là ước của a_i với mọi $i \geq 1$. Ta nói $a_1, a_2, a_3, \ldots$ là *dãy dừng* nếu tồn tại một số tự nhiên n_0 sao cho a_n liên kết với a_{n_0} với mọi $n \geq n_0$. Miền nguyên D được gọi là *thoả mãn điều kiện dãy dừng những ước thực sự* nếu mọi dãy $a_1, a_2, a_3, \ldots$ những phần tử của D thỏa mãn tính chất a_{i+1} là ước của a_i với mọi i đều là dãy dừng.

Miền nguyên $\mathbb{Z}$ thoả mãn điều kiện dãy dừng những ước thực sự. Giả sử D là miền nguyên thoả mãn điều kiện dãy dừng những ước thực sự. Khi đó mỗi phần tử khác 0 và không khả nghịch của D đều có ít nhất một ước bất khả quy. Hơn nữa, mỗi phần tử khác 0 và không khả nghịch của D đều phân tích được thành tích những nhân tử bất khả quy.

1.1.5 Định nghĩa. Cho $a_1, \ldots, a_n \in D$. Một ước chung $d \in D$ của $a_1, \ldots, a_n$ được gọi là một *ước chung lớn nhất* nếu nó là bội của mọi ước chung khác của $a_1, \ldots, a_n$. Nếu 1 là một ước chung lớn nhất của $a_1, \ldots, a_n$ thì ta nói $a_1, \ldots, a_n$ là *nguyên tố cùng nhau*. Một bội chung $m \in D$ của $a_1, \ldots, a_n$ được gọi là một *bội chung nhỏ nhất* nếu m là ước của mọi bội chung khác của $a_1, \ldots, a_n$.

Chú ý rằng nếu $d, d' \in D$ là hai ước chung lớn nhất của $a_1, \ldots, a_n$, thì d và d' là liên kết với nhau, tức là tồn tại một phần tử khả nghịch