ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC KHOA HỌC

-------ଌ*ଌ-------

HOÀNG VĂN ĐÔNG

VÀNH, TRƯỜNG BẬC HAI VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - 2015

ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC KHOA HỌC

-------ꕥ*ꕥ-------

HOÀNG VĂN ĐÔNG

VÀNH, TRƯỜNG BẬC HAI VÀ ỨNG DỤNG

Chuyên ngành: Phương pháp Toán sơ cấp

Mã số: 60 46 01 13

LUẬN VĂN THẠC SĨ TOÁN HỌC

Người hướng dẫn khoa học: PGS.TS. LÊ THỊ THANH NHÀN

Thái Nguyên - 2015

Mục lục

LỜI CẢM ƠN

Trong quá trình học tập và nghiên cứu tại Trường Đại học Khoa học - Đại học Thái Nguyên, tôi được nhận đề tài nghiên cứu "Vành, trường bậc hai và ứng dụng" dưới sự hướng dẫn của PGS.TS Lê Thị Thanh Nhàn. Đến nay, luận văn đã được hoàn thành. Có được kết quả này là do sự dạy bảo và hướng dẫn tận tình và nghiêm khắc của Cô. Tôi xin bày tỏ lòng biết ơn chân thành và sâu sắc tới Cô và gia đình!

Tôi cũng xin gửi lời cảm ơn chân thành đến Ban giám hiệu, Phòng Đào tạo và Khoa Toán - Tin của Trường Đại học Khoa học - Đại học Thái Nguyên đã tạo mọi điều kiện thuận lợi giúp đỡ tôi trong quá trình học tập tại Trường và trong thời gian nghiên cứu hoàn thành luận văn này. Sự giúp đỡ nhiệt tình và thái độ thân thiện của các thày cô giáo, các cán bộ thuộc Phòng Đào tạo, Khoa Toán - Tin đã để lại trong lòng mỗi chúng tôi những ấn tượng tốt đẹp.

Tôi xin cảm ơn Sở Giáo dục và Đào tạo Quảng Ninh, đặc biệt là Trung tâm HN&GDTX tỉnh - nơi tôi đang công tác đã tạo mọi điều kiện thuận lợi để tôi hoàn thành khóa học này.

Tôi xin cảm ơn gia đình, bạn bè, đồng nghiệp và các thành viên trong lớp cao học Toán K7Q (Khóa 2013-2015) đã quan tâm, tạo điều kiện, cổ vũ và động viên để tôi có thể hoàn thành nhiệm vụ của mình.

LỜI NÓI ĐẦU

Trong lý thuyết số đại số, một trường bậc hai được hiểu là một trường con của trường số phức $\mathbb{C}$ đồng thời là một mở rộng bậc hai của trường số hữu tỷ $\mathbb{Q}$ (tức là một $\mathbb{Q}$-không gian véc tơ chiều 2). Như vậy, nếu K là trường bậc hai thì tồn tại một hệ $\{\alpha_1, \beta\} \subseteq K$ (gọi là một *cơ sở* của K) sao cho mỗi phần tử của K đều biểu diễn được một cách duy nhất dạng $a\alpha + b\beta$ với $a, b \in \mathbb{Q}$. Với suy nghĩ tương tự, người ta giới thiệu khái niệm vành bậc hai, đó là một vành con của $\mathbb{C}$ đồng thời là một mở rộng bậc hai của vành số nguyên $\mathbb{Z}$. Cụ thể, nếu D là vành bậc hai thì tồn tại một hệ $\{\alpha, \beta\} \subseteq D$ (gọi là một *cơ sở* của D) sao cho mỗi phần tử của D đều biểu diễn được một cách duy nhất dạng $a\alpha + b\beta$ với $a, b \in \mathbb{Z}$. Các vành và trường bậc hai đã được quan tâm và nghiên cứu một cách sâu sắc với nhiều ứng dụng quan trọng trong toán sơ cấp. Chẳng hạn, chúng ta có thể dùng vành và trường bậc hai để chứng minh rằng không thể dựng bằng thước kẻ và compa số thực $\sqrt[3]{2}$, không thể "cầu phương một hình tròn" (dựng một hình vuông có diện tích bằng diện tích một hình tròn cho trước).

Mục tiêu đầu tiên của luận văn là nghiên cứu các trường bậc hai và các vành bậc hai. Mục tiêu tiếp theo là làm rõ cấu trúc của vành các số nguyên đại số trong một trường bậc hai, chúng tôi chỉ ra rằng đây là một loại vành bậc hai rất đặc biệt. Chẳng hạn, các iđêan của nó đều có một hệ sinh gồm một hoặc hai phần tử, mỗi phần tử của nó đều có sự phân tích thành nhân tử bất khả quy. Chúng tôi cũng chỉ ra một số lớp vành bậc hai có sự phân tích duy nhất. Mục tiêu thứ ba của luận văn là áp dụng những kết quả về vành và trường bậc hai để giải quyết một số dạng bài toán sơ cấp.

Luận văn được viết chủ yếu dựa theo 4 tài liệu sau đây.

1. Daniel A. Marcus, *Number Fields*, Springer New York, 1977.

2. J. Rotman, *Galois theory*, Second edition, Springer, 1998.

3. David Anthony Santos, *Number Theory for mathematical contests*, GNU Free Documentation License, October, 2007.

4. Victor V. Prasolov, *Polynomials*, Springer, 2004 (second edition).

Phần mở rộng vành và trường được tham khảo từ các tài liệu 1 và 2. Khái niệm và một số kết quả về vành và trường bậc hai được tham khảo từ tài liệu 1. Phần ứng dụng giải toán sơ cấp trong Chương 3 được tham khảo từ tài liệu 3, 4 và một tài liệu về toán sơ cấp của PGS.TS. Đàm Văn Nhỉ.

Luận văn chia làm 3 chương. Chương 1 trình bày những kiến thức cơ bản về vành, trường, đồng cấu, mở rộng trường, cơ sở và bậc của mở rộng vành và trường, số đại số, số nguyên đại số. Trong Chương 2, chúng tôi chỉ ra cấu trúc của trường bậc hai, vành bậc hai, vành các số nguyên đại số trong trường bậc hai, iđêan trong vành bậc hai, sự phân tích duy nhất trong vành bậc hai. Chương 3 trình bày những ứng dụng của vành và trường bậc hai trong việc giải toán sơ cấp. Chương chia làm 3 tiết nhỏ. Tiết 3.1 là các bài toán giải được bằng cách sử dụng trường bậc hai. Tiết 3.2 là các bài toán sử dụng chuẩn trong vành bậc hai. Tiết 3.3 dành để trình bày các bài toán sử dụng sự phân tích duy nhất trong vành bậc hai.

Chương 1

Kiến thức cơ bản về mở rộng vành và trường

1.1 Kiến thức cơ bản

Để bắt đầu chúng ta sẽ nhắc lại các định nghĩa cơ bản sau.

1.1.1 Định nghĩa. *Một vành* là một tập V cùng với 2 phép toán $+$ (phép cộng) và . (phép nhân) thỏa mãn các điều kiện sau:
(i) Phép cộng kết hợp: $\forall x, y, z \in$ V ta có $(x + y) + z = x + (y + z)$.
(ii) Có phần tử không: $\exists 0 \in V$ sao cho $\forall x \in V$ ta có $0 + x = x + 0 = x$.
(iii) Có phần tử đối: $\forall x \in V, \exists -x \in V$ sao cho $x + (-x) = (-x) + x = 0$.
(iv) Phép cộng giao hoán: $\forall x, y \in V$ ta có $x + y = y + x$.
(v) Phép nhân kết hợp: $\forall x, y, z \in V$ ta có $(xy)z = x(yz)$.
(vi) Có phần tử đơn vị: $\exists 1 \in V$ sao cho $1.x = x.1 = x, \forall x \in V$.
(vii) Tính phân phối: $\forall x, y, z \in V$ sao cho $x(y + z) = xy + xz$.

Vành V gọi là *vành giao hoán* nếu phép nhân có tính giao hoán, tức là $ab = ba$ với mọi $a, b \in V$. Cho V là một vành. Một tập con A của V được gọi là một *vành con* của V nếu 2 phép toán trong vành V là đóng trong A (tức là $a + b, ab \in A$ với mọi $a, b \in A$) và A cùng với hai phép toán cảm sinh là một vành.

1.1.2 Ví dụ. (i) Tập hợp các số nguyên $\mathbb{Z}$ với phép cộng và phép nhân thông

thường là vành giao hoán, gọi là *vành các số nguyên*. Tương tự ta có vành các số hữu tỷ $\mathbb{Q}$, vành các số thực $\mathbb{R}$, vành các số phức $\mathbb{C}$.

(ii) Tập $\mathbb{Z}_n = \{\bar{x} \mid x \in \mathbb{Z}\}$ các số nguyên modulo n là một vành với phép cộng và phép nhân như sau: $\bar{x} + \bar{y} = \overline{x+y}$ và $\bar{x}\bar{y} = \overline{xy}$ với mọi $\bar{x}, \bar{y} \in \mathbb{Z}_n$. Vành $\mathbb{Z}_m$ được gọi là *vành các số nguyên modulo* m hay *vành các lớp thặng dư theo môđun* m.

(iii) Cho V là một vành giao hoán. Kí hiệu $V[x]$ là tập các đa thức một biến x với hệ số trong V. Mỗi phần tử của $V[x]$ được viết dưới dạng $f(x) = a_n x^n + \ldots + a_1 x + a_0$ với $a_i \in V, \forall i$. Ta cũng viết $f(x)$ dưới dạng $f(x) = \sum a_i x^i$, trong đó $a_i = 0$ với mọi $i > n$. Khi đó $V[x]$ là một vành với phép cộng $f(x) + g(x) = \sum (a_i + b_i)x^i$ và phép nhân $f(x)g(x) = \sum c_k x^k$, trong đó $c_k = \sum_{i+j=k} a_i b_j$ với $f(x) = \sum a_i x^i$ và $g(x) = \sum b_i x^i$. Vành $V[x]$ được gọi là *vành đa thức một biến* x *với hệ số trong* V.

1.1.3 Định nghĩa. Cho V là một vành. Tập con I của V được gọi là một *iđêan* của V nếu các điều kiện sau thỏa mãn

(i) Phép cộng đóng trong I, tức là $x + y \in I, \forall x, y \in I$.

(ii) I chứa phần tử không: $0 \in I$.

(iii) Có phần tử đối: $-x \in I$ với mọi $\forall x \in I$.

(iv) $ax, xa \in I$ với mọi $a \in I, x \in V$.

1.1.4 Ví dụ. (i) $0 = \{0\}$ là iđêan bé nhất và V là iđêan lớn nhất của V.

(ii) I là iđêan của vành $\mathbb{Z}$ khi và chỉ khi I có dạng $n\mathbb{Z}$ với $n \in \mathbb{N}$.

Cho V là một vành. Phần tử $a \in V$ được gọi là phần tử *khả nghịch* nếu tồn tại $b \in V$ sao cho $ab = 1$. Chú ý rằng nếu I là iđêan của V thì các phát biểu sau là tương đương:

(i) $I = V$;

(ii) I chứa một phần tử khả nghịch;

(iii) I chứa phần tử đơn vị.

1.1.5 Định nghĩa. Cho I là một iđêan của vành V. Với $x \in V$, đặt $x+I = \{x+a \mid a \in I\}$. Ta gọi $x+I$ là *lớp ghép trái của I ứng với x*. Chú ý rằng $x+I = y+I$ khi và chỉ khi $x-y \in I$. Đặt $V/I = \{x+I \mid x \in V\}$ là tập các lớp ghép trái của I. Khi đó V/I là một vành với phép cộng $(x+I)+(y+I) = (x+y)+I$ và phép nhân $(x+I)(y+I) = xy+I$. Vành V/I được gọi là *vành thương của V ứng với I*.

Chẳng hạn, vành thương $\mathbb{Z}/\mathfrak{m}\mathbb{Z}$ của vành $\mathbb{Z}$ theo iđêan $m\mathbb{Z}$ chính là vành $\mathbb{Z}_m$ các số nguyên modulo m.

1.1.6 Định nghĩa. Một ánh xạ f từ vành V vào vành V' được gọi là một *đồng cấu vành* nếu f bảo toàn các phép toán, nghĩa là

$$f(x+y) = f(x)+f(y) \text{ và } f(xy) = f(x)f(y)$$

với mọi $x, y \in V$. Một đồng cấu từ vành V vào V được gọi là một *tự đồng cấu* của V. Một đồng cấu đồng thời là đơn ánh (toàn ánh, song ánh) được gọi là *đơn cấu* (*toàn cấu, đẳng cấu*). Nếu f là một tự đồng cấu và là song ánh thì ta nói f là một *tự đẳng cấu*.

1.1.7 Ví dụ. (i) Giả sử A là một vành con của vành V. Khi đó ánh xạ nhúng $i_A : A \to V$ xác định bởi $i_A(x) = x$ là một đơn cấu, gọi là *đơn cấu chính tắc* hay *đơn cấu nhúng*.
(ii) Giả sử I là một iđêan của vành V. Khi đó ánh xạ $p : A \to V/I$ xác định bởi: $p(x) = x+I$ là một toàn cấu, gọi là *toàn cấu chính tắc* hay *phép chiếu tự nhiên*.

1.1.8 Định nghĩa. (i) Cho V là một vành giao hoán. Phần tử $a \in V$ được gọi là một *ước của không* nếu $a \neq 0$ và tồn tại $b \in V, b \neq 0$ sao cho $ab = 0$.
(ii) Một vành giao hoán khác $\{0\}$ và không có ước của không được gọi là một *miền nguyên*.

(ii) Một trường là một vành giao hoán khác 0 và mọi phần tử khác 0 đều khả nghịch. Cho K là một trường và T là một tập con khác rỗng của K ổn định với hai phép toán trong K. Ta nói T là một *trường con* của K nếu T cùng với hai phép toán cảm sinh từ K cũng là một trường.

$\mathbb{Z}$ là miền nguyên, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ là trường. Chú ý rằng mỗi trường là một miền nguyên, và mỗi miền nguyên hữu hạn là một trường. Tuy nhiên miền nguyên vô hạn không nhất thiết là trường, chẳng hạn như miền nguyên $\mathbb{Z}$.

Chú ý rằng mỗi trường có đúng hai iđêan là $\{0\}$ và chính nó. Tổng quát hơn, nếu $V \neq \{0\}$ là vành giao hoán thì các phát biểu sau là tương đương:
(i) V là một trường;
(ii) V chỉ có đúng hai iđêan là $\{0\}$ và V.
(iii) Mọi đồng cấu từ V đến một vành giao hoán khác $\{0\}$ đều là đơn cấu.

1.2 Mở rộng vành và trường

1.2.1 Định nghĩa. (i) Cho F là một trường và K là một trường chứa F. Khi đó $F \subset K$ được gọi là một *mở rộng trường* và ta nói K là một *mở rộng* của trường F. Mở rộng trường $F \subset K$ được kí hiệu là K/F.
(ii) Cho A là một vành và V là một vành chứa A. Khi đó $A \subset V$ được gọi là một *mở rộng vành* và ta nói V là một *mở rộng* của vành A. Mở rộng vành $A \subset V$ được kí hiệu là V/A.

Chú ý rằng nếu A là vành con của vành V và $A \neq V$ thì A không bao giờ là iđêan của V. Vì thế chúng ta không sợ nhầm lẫn giữa kí hiệu của mở rộng vành V/A với kí hiệu cho một vành thương nào đó của V.

1.2.2 Ví dụ. (i) $\mathbb{Q} \subset \mathbb{C}, \mathbb{Q} \subset \mathbb{R}, \mathbb{R} \subset \mathbb{C}$ là các mở rộng trường.
(ii) $\mathbb{Z} \subset \mathbb{Q}, \mathbb{Z} \subset \mathbb{R}, \mathbb{R} \subset \mathbb{C}$ là các mở rộng vành.