ĐẠI HỌC THÁI NGUYÊN
**TRƯỜNG ĐẠI HỌC KHOA HỌC**

**PHẠM THỊ NGÂN**

# VÀNH CÁC SỐ NGUYÊN ĐẠI SỐ

**LUẬN VĂN THẠC SĨ TOÁN HỌC**

**Thái Nguyên - 2016**

ĐẠI HỌC THÁI NGUYÊN
**TRƯỜNG ĐẠI HỌC KHOA HỌC**

**PHẠM THỊ NGÂN**

# VÀNH CÁC SỐ NGUYÊN ĐẠI SỐ

**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. NÔNG QUỐC CHINH**

**Thái Nguyên - 2016**

# Mục lục

**Mục lục** **i**

**Lời cảm ơn** **ii**

**Mở đầu** **1**

**1 Một số kiến thức chuẩn bị** **2**

1.1 Nhóm . . . . . 2

1.2 Vành và trường . . . . . 3

1.3 Đa thức . . . . . 6

1.4 Nhóm Abel tự do . . . . . 9

**2 Vành số nguyên đại số trên trường số** **13**

2.1 Số đại số và số nguyên đại số . . . . . 13

2.2 Các trường số . . . . . 20

2.3 Nhân tử hóa . . . . . 32

2.4 Các iđêan trong vành các số nguyên đại số . . . . . 41

**Kết luận** **53**

**Tài liệu tham khảo** **54**

# Lời cảm ơn

Luận văn này được hoàn thành tại trường Đại học Khoa học - Đại học Thái Nguyên. Tác giả xin bày tỏ lòng biết ơn sâu sắc với PGS.TS. Nông Quốc Chinh, đã trực tiếp hướng dẫn tận tình và động viên tác giả trong suốt thời gian nghiên cứu vừa qua.

Xin chân thành cảm ơn tới các thầy, cô giáo trong Khoa Toán - Tin, Phòng Đào tạo, các bạn học viên lớp Cao học Toán K7C trường Đại học Khoa học - Đại học Thái Nguyên, và các bạn đồng nghiệp đã tạo điều kiện thuận lợi, động viên tác giả trong quá trình học tập và nghiên cứu tại trường.

Tác giả cũng xin bày tỏ lòng biết ơn sâu sắc tới gia đình và người thân luôn khuyến khích, động viên tác giả trong suốt quá trình học tập và làm luận văn.

***Thái Nguyên, 2016*** **Phạm Thị Ngân**

*Học viên Cao học Toán K7C,*
*Trường ĐH Khoa học - ĐH Thái Nguyên*

# Mở đầu

Số học luôn được mệnh danh là nữ hoàng của toán học, bởi trong nó chứa đựng nhiều vẻ đẹp của tư duy logic. Số nguyên đại số là lĩnh vực được nhiều nhà toán học dành nhiều thời gian nghiên cứu. Việc nghiên cứu các tính chất của các số nguyên đại số luôn là một đề tài hấp dẫn đối với những người yêu toán xưa và nay. Vì những lý do như vậy nên chúng tôi chọn "Vành các số nguyên đại số" làm đối tượng nghiên cứu trong luận văn của mình.

Ngoài phần mở đầu và tài liệu tham khảo, luận văn gồm 2 chương với nội dung chính như sau.

Chương 1: Một số kiến thức chuẩn bị. Chương này trình bày các kiến thức cơ bản có liên quan cần sử dụng cho luận văn như: Các khái niệm vành, iđêan, iđêan chính, iđêan nguyên tố, iđêan tối đại, vành nhân tử hóa, vành Euclid; Đa thức, đa thức đối xứng, đa thức bất khả quy; Nhóm Abel tự do ...

Chương 2: Vành số nguyên đại số trên trường số. Nội dung chương 2 trình bày khái niệm, tính chất và các iđêan trong vành $\mathcal{O}_K$ các số nguyên đại số.

*Thái Nguyên, ngày 18 tháng 05 năm 2016*

**Phạm Thị Ngân**

Email: nganstar1821@gmail.com

# Chương 1

# Một số kiến thức chuẩn bị

## 1.1 Nhóm

**Định nghĩa 1.1.1.** Cho tập $X$ với phép toán nhân. Ta nói $(X, .)$ (gọi tắt là $X$) là:

(i) một *nửa nhóm* nếu phép toán nhân kết hợp trên $X$ $(X \neq \varnothing)$;

(ii) một *vị nhóm* nếu phép toán nhân kết hợp trên $X$ và phép toán có phần tử đơn vị trên $X$.

Một nửa nhóm được gọi là *giao hoán* hay *Abel* nếu phép toán tương ứng giao hoán.

**Định nghĩa 1.1.2.** *Nhóm* là một vị nhóm mà mọi phần tử đều có phần tử nghịch đảo. Nói cách khác, tập $G$ khác rỗng với phép toán nhân được gọi là một nhóm nếu các tính chất sau được thỏa mãn:

$(G_1)$ Với mọi $x, y, z \in G, (xy)z = x(yz)$;

$(G_2)$ Tồn tại $e \in G$ sao cho với mọi $x \in G, ex = xe = x$;

$(G_3)$ Với mọi $x \in G$, tồn tại $x^{-1} \in G$ sao cho $xx^{-1} = x^{-1}x = e$.

Nếu phép toán trên $G$ là phép toán cộng thì các tính chất trên trở thành:

$(G_1)$ Với mọi $x, y, z \in G, (x + y) + z = x + (y + z)$;

$(G_2)$ Tồn tại $e \in G$ sao cho với mọi $x \in G, 0 + x = x + 0 = x$;

$(G_3)$ Với mọi $x \in G$, tồn tại $-x \in G$ sao cho $x + (-x) = (-x) + x = 0$.

Trường hợp phép toán trên nhóm $G$ giao hoán thì ta nói $G$ là *nhóm giao hoán* hay *nhóm Abel*.

Nhóm $G$ được gọi là *nhóm hữu hạn* khi tập hợp $G$ hữu hạn. Khi đó số phần tử của $G$ được gọi là *chỉ số* của nhóm $G$. Nếu nhóm $G$ không hữu hạn thì ta nói $G$ là *nhóm vô hạn*.

**Định nghĩa 1.1.3.** *Nhóm con* $H$ của nhóm $G$ là một tập con ổn định của nhóm $G$ sao cho cùng với phép toán cảm sinh $H$ là một nhóm. Ký hiệu $H \leq G$ để chỉ $H$ là một nhóm con của $G$.

**Định lí 1.1.4.** *Cho $H$ là một tập con khác rỗng của nhóm $(G, .)$. Các mệnh đề sau tương đương:*

*(i)* $H \leq G$;

*(ii) Với mọi* $x, y \in H, xy \in H$ *và* $x^{-1} \in H$;

*(iii) Với mọi* $x, y \in H, x^{-1}y \in H$.

**Định nghĩa 1.1.5.** Cho $S$ là một tập con của nhóm $G$. *Nhóm con sinh bởi S* là nhóm con nhỏ nhất của $G$ chứa $S$ và được kí hiệu là $\langle S \rangle$. Tập $S$ được gọi là *tập sinh* của nhóm $\langle S \rangle$. Nếu $S$ hữu hạn $S = \{x_1, x_2, \ldots, x_n\}$ thì ta nói $\langle S \rangle$ là *nhóm hữu hạn sinh* với các phần tử sinh $x_1, \ldots, x_n$ mà ta thường kí hiệu nhóm là $\langle x_1, \ldots, x_n \rangle$.

## 1.2 Vành và trường

**Định nghĩa 1.2.1.** *Vành* là một tập $R$ cùng với hai phép toán cộng và nhân thỏa mãn các tính chất sau:

$(R_1)$ $(R, +)$ là nhóm Abel;

$(R_2)$ $(R, .)$ là nửa nhóm;

$(R_3)$ Phép nhân phân phối đối với phép cộng, nghĩa là với mọi $x, y, z \in R$,

ta có

$$x(y+z) = xy + xz;$$

$$(y+z)x = yx + zx.$$

Phần tử đơn vị của phép cộng được gọi là *phần tử không*, ký hiệu là $0$; phần tử nghịch đảo của phần tử $x \in R$ là *phần tử đối* của $x$ ký hiệu là $-x$. Nếu phép nhân giao hoán thì ta nói vành $R$ *giao hoán*; nếu phép nhân có phần tử đơn vị thì vành $R$ được gọi là *vành có đơn vị*. Phần tử đơn vị được ký hiệu là $e$ hay $1$.

**Định nghĩa 1.2.2.** Cho $R$ là một vành.

(i) Tập con $A$ khác rỗng của $R$ được gọi là một *vành con* của $R$ nếu $A$ ổn định đối với hai phép toán trong vành $R$ và $A$ cùng với hai phép toán cảm sinh là một vành.

(ii) Vành con $I$ của $R$ được gọi là một *iđêan trái* (tương ứng *iđêan phải*) của $R$ nếu với mọi $r \in R$ và $x \in I$ ta có $rx \in I$ (tương ứng $xr \in I$). Ta nói $I$ là một *iđêan* của $R$ nếu $I$ vừa là iđêan trái vừa là iđêan phải của $R$.

**Định lí 1.2.3** (Đặc trưng của vành con)**.** *Cho $A$ là một tập con khác rỗng của vành $R$. Các mệnh đề sau là tương đương:*

*(i) $A$ là một vành con của $R$;*

*(ii) Với mọi $x, y \in A, x + y \in A, xy \in A, -x \in A$;*

*(iii) Với mọi $x, y \in A, x - y \in A$ và $xy \in A$.*

**Định lí 1.2.4** (Đặc trưng của iđêan)**.** *Cho $I$ là một tập con khác rỗng của vành $R$. Các mệnh đề sau là tương đương:*

*(i) $I$ là một iđêan của $R$;*

*(ii) Với mọi $x, y \in I$ và $r \in R, x + y \in I, -x \in I, rx \in I$ và $xr \in I$;*

*(iii) Với mọi $x, y \in I$ và $r \in R, x - y \in I, xr \in I$ và $rx \in I$.*

**Định nghĩa 1.2.5.** Cho $S$ là một tập con khác rỗng của vành $R$. Ta định nghĩa:

(i) Giao của tất cả các vành con của $R$ có chứa $S$ là vành con *sinh bởi* $S$.

(ii) Giao của tất cả các iđêan của R có chứa $S$ là *iđêan sinh bởi* $S$, ký hiệu là $\langle S\rangle$.

**Định nghĩa 1.2.6.** Cho $S$ là một tập con của vành $R$ và $I = \langle S\rangle$. Ta nói $I$ *được sinh ra bởi S* và $S$ là *tập sinh* của $I$. Nếu $S$ hữu hạn thì ta nói *I hữu hạn sinh*. Đặc biệt, nếu $S = \{a\}$ thì ta viết $I = \langle a\rangle$, gọi là *iđêan chính sinh bởi a*.

**Định nghĩa 1.2.7.** Cho $R$ là vành giao hoán, có đơn vị 1.

1) Iđêan $P$ của $R$ được gọi là *iđêan nguyên tố* nếu $P \neq R$ và từ $ab \in P$ suy ra $a \in P$ hoặc $b \in P$ với mọi $a, b \in R$.

2) Iđêan $M$ được gọi là *iđêan tối đại* của $R$ nếu $M \neq R$ và nếu với bất kỳ iđêan $B$ của $R$ thỏa mãn $M \subset B \subset R$ thì $B = R$ hoặc $B = M$.

**Định nghĩa 1.2.8.** (i) Cho $R$ là một vành giao hoán. Phần tử $x \in R\backslash\{0\}$ được gọi là *ước của 0* nếu tồn tại $y \in R\backslash\{0\}$ sao cho $xy = 0$.

(ii) Một vành giao hoán, có đơn vị, có nhiều hơn một phần tử và không có ước của không được gọi là *miền nguyên*.

(iii) Một vành giao hoán, có đơn vị, có nhiều hơn một phần tử trong đó một phần tử khác không đều khả nghịch được gọi là một *trường*.

**Định lí 1.2.9.** *(i) Mọi trường đều là miền nguyên.*

*(ii) Mọi miền nguyên hữu hạn đều là trường.*

**Định nghĩa 1.2.10.** Cho $R$ là một trường và $I$ là một tập con khác rỗng, ổn định đối với hai phép toán trong $R$. Ta nói $I$ là một *trường con* của $R$ nếu $I$ với hai phép toán cảm sinh từ $R$ cũng là một trường.

**Định lí 1.2.11** (Đặc trưng của trường con)**.** *Cho $R$ là một trường và $I$ là tập con của $R$ có chứa ít nhất hai phần tử. Các mệnh đề sau tương đương:*

*(i) $I$ là một trường con của $R$;*

*(ii) Với mọi $x, y \in I, x + y \in I, xy \in I, -x \in I$ và hơn nữa, nếu $x \neq 0$ thì $x^{-1} \in I$;*

*(iii) Với mọi $x, y \in I, x - y \in I$ và hơn nữa, nếu $x \neq 0$ thì $x^{-1}y \in I$.*

Một hàm Euclid $\phi$ trên miền nguyên $R$ là hàm $\phi : R\backslash\{0\} \to \mathbb{Z}$ với các tính chất

- $\phi(a) \geq 0$ với mọi $a \in \mathbb{R}, a \neq 0$, và
- nếu $a, b \in R$ với $a \neq 0$ thì $a|b$ hoặc tồn tại $c \in R$ với $\phi(b - ac) < \phi(a)$.

Một miền nguyên $R$ là một *miền Euclid* nếu tồn tại một hàm Euclid trên $R$.

**Bổ đề 1.2.12.** *Giả sử $R$ là một miền Euclid. Khi đó mỗi iđêan trong $R$ là iđêan chính.*

## 1.3 Đa thức

Cho $R$ là một vành (giao hoán) có đơn vị là 1, kí hiệu $R[X]$ là vành đa thức biến $X$ với các hệ số trong $R$. Nếu $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ với $a_n \neq 0$ thì $n$ là *bậc* của $f$, $a_n$ là *hạng tử cao nhất* của $f$ và $a_nX^n$ là *số hạng cao nhất* của $f$. Bậc của $f$ kí hiệu là $\deg(f)$. Một đa thức được gọi là *đa thức monic* nếu hệ số cao nhất bằng 1.

**Nhận xét 1.3.1.** Nếu $R$ là một miền nguyên thì $\deg(fg) = \deg(f) + \deg(g)$, trong đó $f$ và $g$ là hai đa thức khác không trong $R[X]$. Đặc biệt $fg \neq 0$ và do vậy $R[X]$ cũng là một miền nguyên.

**Mệnh đề 1.3.2** (Thuật toán chia)**.** *Cho $K$ là một trường và $f, g \in K[X]$ với $g \neq 0$. Khi đó, tồn tại duy nhất các đa thức $q, r \in K[X]$ sao cho*