TẠP CHÍ KHOA HỌC
TRƯỜNG ĐẠI HỌC SƯ PHẠM TP HỒ CHÍ MINH
Tập 23, Số 4 (2026): 944-954
Website: https://journal.hcmue.edu.vn
ISSN: 2734-9918

HO CHI MINH CITY UNIVERSITY OF EDUCATION
JOURNAL OF SCIENCE
Vol. 23, No. 4 (2026): 944-954
https://doi.org/10.54607/hcmue.js.23.4.5363(2026)

**Bài báo nghiên cứu**

# CẤU TRÚC NHÓM NHÂN CỦA VÀNH THƯƠNG CỦA VÀNH SỐ NGUYÊN ĐẠI SỐ $\mathbb{Z}[\sqrt{-6}]$

***Mỵ Vinh Quang, Nguyễn Cao Minh****

*Trường Đại học Sư phạm Thành phố Hồ Chí Minh, Việt Nam*

**Tác giả liên hệ: Nguyễn Cao Minh – Email: 4901101055@student.hcmue.edu.vn*

*Ngày nhận bài: 14-11-2025; Ngày nhận bài sửa: 20-11-2025; Ngày duyệt đăng: 15-12-2025*

**TÓM TẮT**

*Trong bài báo này, chúng tôi mô tả đầy đủ cấu trúc nhóm nhân của vành thương của vành các số nguyên đại số $\mathbb{Z}[\sqrt{-6}]$ theo các iđêan là luỹ thừa của iđêan nguyên tố. Từ đó, như là hệ quả, chúng tôi mô tả trọn vẹn cấu trúc nhóm nhân của vành thương của vành các số nguyên đại số $\mathbb{Z}[\sqrt{-6}]$ theo iđêan khác không bất kì. Cuối cùng, bài báo xây dựng một ví dụ minh họa được xem như là áp dụng các kết quả nghiên cứu trên trong trường hợp cụ thể.*

***Từ khoá:*** vành số nguyên đại số; vành thương; nhóm nhân của vành thương

## 1. Mở đầu

Xét một mở rộng đại số $F$ trên trường số hữu tỉ $\mathbb{Q}$ với bậc $[F:\mathbb{Q}] = n$. Gọi $D$ là vành các số nguyên đại số của $F$. Khi đó, ta có thể coi $D$ như một dạng mở rộng tự nhiên từ vành số nguyên $\mathbb{Z}$ (rõ ràng $D = \mathbb{Z}$ trong trường hợp $n = 1$). Với mỗi $I \lhd D$, kí hiệu $D/I$ là vành thương của $D$ theo $I$, vành này còn gọi là vành các lớp thặng dư modulo $I$, nhóm các phần tử khả nghịch (nhóm nhân) của vành thương này được định nghĩa bởi $\phi_D(I) = (D/I)^*$, trong khi số phần tử $|D/I|$ đại diện cho chuẩn $N_D(I)$ của iđêan $I$. Khi đó, đại lượng $\varphi_D(I) = |\phi_D(I)|$ chính là hàm Euler tổng quát trên $D$, xác định với mọi iđêan $I$ khác không thuộc $D$).

Việc nghiên cứu nhằm tường minh cấu trúc của vành thương cũng như nhóm nhân tương ứng trên vành các số nguyên đại số luôn là một hướng đi quan trọng và mang tính thời sự trong lí thuyết số. Dresden và Dymáček (2005) mô tả được cấu trúc vành thương của vành số nguyên Gauss (vành $\mathbb{Z}[\sqrt{-1}]$); Buçaj (2014) mô tả được cấu trúc vành thương của vành số nguyên Eisenstein (vành $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$). Gần đây, Greene và Jing (2024) mô tả được cấu trúc vành thương của vành các số nguyên đại số bậc hai mà là vành chính. Đối với cấu trúc nhóm nhân, Cross (1983) mô tả thành công cấu trúc nhóm nhân của vành thương của vành số

***Cite this article as:*** My, V. Q., & Nguyen, C. M. (2026). The structure of the multiplicative group of the quotient ring of the ring of algebraic integers $\mathbb{Z}[\sqrt{-6}]$. *Ho Chi Minh City University of Education Journal of Science, 23*(4), 944-954. https://doi.org/10.54607/hcmue.js.23.4.5363(2026)

nguyên Gauss; My và Cao (2025) mô tả được cấu trúc nhóm nhân của vành thương của vành số nguyên Eisenstein. Bài báo này sẽ mô tả cấu trúc nhóm nhân của vành thương của vành các số nguyên đại số $\mathbb{Z}[\sqrt{-6}]$. Lưu ý rằng tất cả các kết quả kể trên của các tác giả trước đều áp dụng cho lớp các vành số nguyên đại số là vành chính. Trong các vành này, mỗi iđêan đều là iđêan chính và mọi phần tử khác không, không khả nghịch đều phân tích được duy nhất thành tích các phần tử bất khả quy. Tuy nhiên vành $\mathbb{Z}[\sqrt{-6}]$ không là vành nhân tử hóa, do đó trong vành này tồn tại các phần tử có thể có nhiều cách phân tích thành tích các phần tử bất khả quy. Mặt khác, vành $\mathbb{Z}[\sqrt{-6}]$ là vành Dedekind; vì vậy mọi iđêan khác 0, $\mathbb{Z}[\sqrt{-6}]$ của $\mathbb{Z}[\sqrt{-6}]$ đều phân tích được duy nhất thành tích các iđêan nguyên tố.

## 2. Kí hiệu và các kết quả mở đầu

Kí hiệu $D$ là vành các số nguyên đại số của trường $F = \mathbb{Q}(\sqrt{-6})$. Khi đó

$D = \mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$.

Nhóm các phần tử khả nghịch trong $D$ là $\{\pm 1\} = \langle -1\rangle$.

Các iđêan nguyên tố trong $D$ được mô tả thông qua định lí sau.

***Định lí 2.1.*** Trong vành $D$ có ba loại iđêan nguyên tố (khác 0) như sau:

1) $\alpha = \langle 2, \sqrt{-6}\rangle$ và $\beta = \langle 3, \sqrt{-6}\rangle$ là các iđêan nguyên tố đồng thời $\langle 2\rangle = \alpha^2$, $\langle 3\rangle = \beta^2$ và $N(\alpha) = 2, N(\beta) = 3$.

2) Nếu $p$ là số nguyên tố thỏa mãn $\left(\frac{-6}{p}\right) = -1$, thì $\langle p\rangle$ là iđêan nguyên tố trong $D$ và $N(\langle p\rangle) = p^2$.

3) Nếu $q$ là số nguyên tố thỏa mãn $\left(\frac{-6}{q}\right) = 1$, thì $\langle q\rangle$ có phân tích duy nhất dưới dạng $\langle q\rangle = \pi_q\overline{\pi_q}$, trong đó $\pi_q = \langle q, m + \sqrt{-6}\rangle$, $\overline{\pi_q} = \langle q, m - \sqrt{-6}\rangle$ ($m$ là số nguyên thỏa mãn $m^2 + 6$ chia hết cho $q$) là các iđêan nguyên tố khác nhau và $N(\pi_q) = N(\overline{\pi_q}) = q$.

Ngoài ra, bất kì iđêan nguyên tố khác 0 nào của $D$ cũng bằng với một trong ba loại iđêan nguyên tố nói trên.

Chứng minh của Định lí 2.1 này có thể tìm thấy trong (Alaca & Williams, 2004). Kể từ đây, ta kí hiệu $p$ là số nguyên tố thỏa mãn $\left(\frac{-6}{p}\right) = -1$, $q$ là số nguyên tố thỏa mãn $\left(\frac{-6}{q}\right) = 1$, $\alpha, \beta, \pi_q, \overline{\pi_q}$ là các iđêan nguyên tố như trên thỏa mãn $\langle q\rangle = \pi_q\overline{\pi_q}$.

Hai định lí dưới đây mô tả các phần tử đại diện của vành thương và nhóm nhân của vành thương của $D$ theo iđêan lũy thừa của iđêan nguyên tố.

***Định lí 2.2.*** Ta có:

1) $D/_{\pi_q^n} = \{[a]: 0 \le a \le q^n - 1\}$.

2) $D/_{\langle p^n\rangle} = \{[a + b\sqrt{-6}]: 0 \le a, b \le p^n - 1\}$.

3) $D/_{\alpha^{2m}} = \{[a + b\sqrt{-6}]: 0 \le a, b \le 2^m - 1\}$.

$D/_{\alpha^{2m+1}} = \{[a + b\sqrt{-6}]: 0 \le a \le 2^{m+1} - 1, 0 \le b \le 2^m - 1\}$.

4) $D/_{\beta^{2m}} = \{[a + b\sqrt{-6}] : 0 \le a, b \le 3^m - 1\}$.

$D/_{\beta^{2m+1}} = \{[a + b\sqrt{-6}] : 0 \le a \le 3^{m+1} - 1, 0 \le b \le 3^m - 1\}$.

*Chứng minh.* Ta có vế phải là tập con của vế trái. Ta sẽ chứng minh các lớp tương đương ở vế phải đôi một khác nhau. Từ đó suy ra số phần tử của hai vế bằng nhau nên hai vế cũng bằng nhau.

Quy ước chung: Ở vế phải, các phần tử được lựa chọn đều đóng vai trò là đại diện cho những lớp tương đương tương ứng. Các kí hiệu $|_R$ và $\nmid_R$ lần lượt được sử dụng để mô tả quan hệ chia hết và không chia hết xét trong cấu trúc vành $R$.

1) Từ giả thiết $a \equiv b \pmod{\pi_q^n}$, ta thu được $\pi_q^n |_D \langle a - b \rangle$. Dẫn đến:

$\overline{\pi_q}^n = \overline{\pi_q^n} \,|_D \overline{\langle a - b \rangle} = \langle a - b \rangle$.

Mặt khác, do $\pi_q, \overline{\pi_q}$ nguyên tố cùng nhau trong $D$ nên $\pi_q^n \overline{\pi_q^n} \,|_D \langle a - b \rangle$, hay nói cách khác $\langle q^n \rangle \,|_D \, \langle a - b \rangle$, điều này kéo theo $q^n \,|_{\mathbb{Z}} (a - b)$, và vì vậy ta thu được $a = b$.

2) Giả sử $a + b\sqrt{-6} \equiv c + d\sqrt{-6} \pmod{p^n}$, hệ thức này tương đương với

$p^n |_D [(a - c) + (b - d)\sqrt{-6}]$.

Ta suy ra đồng thời $p^n |_{\mathbb{Z}} (a - c)$ và $p^n |_{\mathbb{Z}} (b - d)$ hay $a = c, b = d$.

3) Đối với trường hợp $D/_{\alpha^{2m}}$, do $\alpha^{2m} = (\alpha^2)^m = \langle 2^m \rangle$ trong $D$ nên ta chứng minh tương tự như (2).

Đối với $D/_{\alpha^{2m+1}}$ , ta có $\alpha^{2m+1} = \alpha^{2m}.\alpha = \langle 2^m \rangle \alpha$. Nếu

$a + b\sqrt{-6} \equiv c + d\sqrt{-6} \pmod{\alpha^{2m+1}}$

thì $\langle 2^m \rangle \alpha \,|_D \langle (a - c) + (b - d)\sqrt{-6} \rangle$. Khi đó $2^m \,|_D [(a - c) + (b - d)\sqrt{-6}]$ nên $2^m |_{\mathbb{Z}} (b - d)$, hay $b = d$. Ta suy ra $\langle 2^m \rangle \alpha \,|_D \, (a - c)$, do đó $N(2^m \alpha) \,|_{\mathbb{Z}} N(a - c)$, tức $2^{2m+1} \,|_{\mathbb{Z}} \, (a - c)^2$. Như vậy $2^{m+1} |_{\mathbb{Z}} (a - c)$, hay $a = c$.

4) Chứng minh tương tự như (3). ■

***Định lí 2.3.*** Với $a, b \in \mathbb{Z}$, ta có:

1) $\phi_D(\pi_q^n) = \{[a] \mid 1 \le a \le q^n - 1, q \nmid_{\mathbb{Z}} a\}$.

2) $\phi_D(\langle p^n \rangle) = \{[a + b\sqrt{-6}] : 0 \le a, b \le p^n - 1, p \nmid_{\mathbb{Z}} a \text{ hoặc } p \nmid_{\mathbb{Z}} b\}$.

3) $\phi_D(\alpha^{2m}) = \{[a + b\sqrt{-6}] : 0 \le a, b \le 2^m - 1, 2 \nmid_{\mathbb{Z}} a\}$.

$\phi_D(\alpha^{2m+1}) = \{[a + b\sqrt{-6}] : 0 \le a \le 2^{m+1} - 1, 0 \le b \le 2^m - 1, 2 \nmid_{\mathbb{Z}} a\}$.

4) $\phi_D(\beta^{2m}) = \{[a + b\sqrt{-6}] : 0 \le a, b \le 3^m - 1, 3 \nmid_{\mathbb{Z}} a\}$.

$\phi_D(\beta^{2m+1}) = \{[a + b\sqrt{-6}] : 0 \le a \le 3^{m+1} - 1, 0 \le b \le 3^m - 1, 3 \nmid_{\mathbb{Z}} a\}$.

*Chứng minh.* Trước hết ta có nhận xét sau: Cho $\gamma \in D$ và $I \lhd D$, khi đó $[\gamma]$ khả nghịch trong $D/I$ khi và chỉ khi $([\gamma], I) = D$ hay $\langle \gamma \rangle + I = D$.

Thật vậy nếu $[\gamma]$ khả nghịch trong $D/I$ thì tồn tại $[\delta] \in D/I$ sao cho $[\gamma].[\delta] = \overline{1}$ hay $\gamma\delta - 1 = \theta \in I$, do đó $1 = \gamma\delta - \theta \in \langle \gamma \rangle + I$. Suy ra $\langle \gamma \rangle + I = D$. Ngược lại, nếu $\langle \gamma \rangle + I = D$ thì $1 = \gamma\delta + \theta$ với $\delta \in I$ và $\theta \in I$. Do đó $[\gamma].[\delta] = \overline{1}$.

Trường hợp đặc biệt, khi $I = P^m$ với $P$ là iđêan nguyên tố, ta có $[\gamma]$ khả nghịch trong $D/P^m$ khi và chỉ khi $([\gamma], P^m) = D$ hay $([\gamma], P) = D$ khi và chỉ khi $P \nmid_D \langle\gamma\rangle$ hay $\gamma \notin P$.

Như một hệ quả trực tiếp, lấy hai phần tử $a, b \in \mathbb{Z}$:

1) $[a]$ khả nghịch trong vành $D/_{\pi_q^n}$ khi và chỉ khi $\pi_q \nmid_D \langle a\rangle$. Thật vậy, ta có

$\pi_q \nmid_D \langle a\rangle \Rightarrow \langle q\rangle = \pi_q\overline{\pi_q} \nmid_D \langle a\rangle \Rightarrow q \nmid_{\mathbb{Z}} a$;

và

$\pi_q \mid_D \langle a\rangle \Rightarrow \overline{\pi_q} \mid_D \overline{\langle a\rangle} = \langle a\rangle \Rightarrow \langle q\rangle = \pi_q\overline{\pi_q} \mid_D a \Rightarrow q \mid_{\mathbb{Z}} a$.

Vì vậy $\pi_q \nmid_D \langle a\rangle$ khi và chỉ khi $q \nmid_{\mathbb{Z}} a$.

2) $\left[a + b\sqrt{-6}\right]$ khả nghịch trong vành $D/_{\langle p^n\rangle}$ khi và chỉ khi $p \nmid_D \left(a + b\sqrt{-6}\right)$, điều này dẫn đến điều kiện đồng thời $p \nmid_{\mathbb{Z}} a$ hoặc $p \nmid_{\mathbb{Z}} b$.

3) $\left[a + b\sqrt{-6}\right]$ khả nghịch trong vành $D/_{\alpha^n}$ khi và chỉ khi $a + b\sqrt{-6} \notin \alpha$. Do $b\sqrt{-6} \in \alpha$ nên $a + b\sqrt{-6} \notin \alpha$ tương đương với $a \notin \alpha$ hay $2 \nmid_{\mathbb{Z}} a$.

4) $\left[a + b\sqrt{-6}\right]$ khả nghịch trong vành $D/_{\beta^n}$ khi và chỉ khi $a + b\sqrt{-6} \notin \beta$. Do $b\sqrt{-6} \in \beta$ nên $a + b\sqrt{-6} \notin \beta$ tương đương với $a \notin \beta$ hay $3 \nmid_{\mathbb{Z}} a$. ■

***Hệ quả 2.4.*** Giá trị $\varphi$ −hàm Euler cho các lũy thừa iđêan nguyên tố trong $D$ với $n \geq 1$ là:

1) $\varphi_D\left(\pi_q^n\right) = q^{n-1}(q-1)$.
2) $\varphi_D(\langle p^n\rangle) = p^{2n-2}(p^2-1)$.
3) $\varphi_D(\alpha^n) = 2^{n-1}$.
4) $\varphi_D(\beta^n) = 2.3^{n-1}$.

## 3. Các kết quả chính

### *3.1. Một số bổ đề*

Cho số tự nhiên $n \geq 1$ và $r$ là số nguyên tố, ta kí hiệu $v_r(n)$ là số mũ của $r$ trong phân tích tiêu chuẩn của $n$ (nếu $r \nmid n$ thì quy ước $v_r(n) = 0$).

***Bổ đề 3.1.*** **(Định lí Kummer)** Cho $r$ là số nguyên tố và $k$ là số nguyên dương. Khi đó

$v_r\left(C_{rk}^i\right) = k - v_r(i)$.

C*hứng minh.* Bổ đề 3.1 có thể tìm thấy trong (Andreescu et al., 2017).

***Bổ đề 3.2.*** Với $n$ là số nguyên dương, ta có:

1) $\left(1 + p\sqrt{-6}\right)^{p^{n-1}} \equiv 1 + p^n\sqrt{-6} \pmod{p^{n+1}}$.
2) $\left(1 + \sqrt{-6}\right)^{2^n} \equiv 1 + 2^n\sqrt{-6} \pmod{2^{n+1}}$ với $n \geq 2$.
3) $\left(1 + \sqrt{-6}\right)^{3^n} \equiv 1 + 2.3^n\sqrt{-6} \pmod{3^{n+1}}$.

*Chứng minh.*

1) Ta có

$$\left(1 + p\sqrt{-6}\right)^{p^{n-1}} = 1 + p^n\sqrt{-6} + \sum_{i=2}^{p^{n-1}} C_{p^{n-1}}^i\, p^i\left(\sqrt{-6}\right)^i.$$

Theo Bổ đề 3.1 thì $v_p\left(C_{p^{n-1}}^{i}\right) = n - 1 - v_p(i)$, mặt khác, dễ thấy với $i \geq 2$ thì $i - v_p(i) \geq 2$, do đó ta luôn có $v_p\left(C_{p^{n-1}}^{i} p^i\right) = n - 1 + i - v_p(i) \geq n + 1, \forall i \geq 2$. Do đó

$\left(1 + p\sqrt{-6}\right)^{p^{n-1}} \equiv 1 + p^n\sqrt{-6} \pmod{p^{n+1}}$.

2) Ta chứng minh quy nạp theo $n$

Với $n = 2$, ta có $\left(1 + \sqrt{-6}\right)^4 = 1 - 20\sqrt{-6} \equiv 1 + 4\sqrt{-6}\ (mod\ 8)$.

Giả sử $\left(1 + \sqrt{-6}\right)^{2^n} \equiv 1 + 2^n\sqrt{-6} \pmod{2^{n+1}}$. Khi đó

$\left(1 + \sqrt{-6}\right)^{2^n} = 1 + 2^n\sqrt{-6} + 2^{n+1}\delta, \delta \in D$.

Dẫn đến

$\left(1 + \sqrt{-6}\right)^{2^{n+1}} = \left(1 + 2^n\sqrt{-6} + 2^{n+1}\delta\right)^2 \equiv 1 + 2^{n+1}\sqrt{-6}\ (mod\ 2^{n+2})$.

Vậy (2) đã được chứng minh.

3) Ta chứng minh quy nạp theo $n$

Với $n = 1$, ta có $\left(1 + \sqrt{-6}\right)^3 = -17 - 3\sqrt{-6} \equiv 1 + 6\sqrt{-6}\ (mod\ 9)$.

Giả sử $\left(1 + \sqrt{-6}\right)^{3^n} \equiv 1 + 2.3^n\sqrt{-6} \pmod{3^{n+1}}$. Khi đó

$\left(1 + \sqrt{-6}\right)^{3^n} = 1 + 2.3^n\sqrt{-6} + 3^{n+1}\delta, \delta \in D$.

Dẫn đến

$\left(1 + \sqrt{-6}\right)^{3^{n+1}} = \left(1 + 2.3^n\sqrt{-6} + 3^{n+1}\delta\right)^3 \equiv 1 + 2.3^{n+1}\sqrt{-6}\ (mod\ 3^{n+2})$.

Vậy (3) đã được chứng minh. ■

***Bổ đề 3.3.*** Với $m, n \geq 1$, ta có:

1) $\left[1 + p\sqrt{-6}\right]$ có cấp $p^{n-1}$ trong $\phi_D(\langle p^n \rangle)$.
2) $\left[1 + \sqrt{-6}\right]$ có cấp $2^m$ trong $\phi_D(\alpha^{2m})$ và $\phi_D(\alpha^{2m+1})$ với $m \geq 2$.
3) $\left[1 + \sqrt{-6}\right]$ có cấp $3^m$ trong $\phi_D(\beta^{2m})$ và $\phi_D(\beta^{2m+1})$.

*Chứng minh.*

1) Theo Bổ đề 3.2, ta có:

$\left(1 + p\sqrt{-6}\right)^{p^{n-1}} \equiv 1 + p^n\sqrt{-6} \pmod{p^{n+1}}$;

do đó $\left(1 + p\sqrt{-6}\right)^{p^{n-1}} \equiv 1\ (mod\ p^n)$.

Vẫn theo Bổ đề 3.2:

$\left(1 + p\sqrt{-6}\right)^{p^{n-2}} \equiv 1 + p^{n-1}\sqrt{-6} \not\equiv 1 \pmod{p^n}$;

do đó cấp của $\left[1 + p\sqrt{-6}\right]$ trong $\phi_D(\langle p^n \rangle)$ là $p^{n-1}$.

2) Đối với $\phi_D(\alpha^{2m})$, ta có $\alpha^{2m} = \langle 2^m \rangle$, theo Bổ đề 3.2, ta có

$\left(1 + \sqrt{-6}\right)^{2^m} \equiv 1 + 2^m\sqrt{-6} \pmod{2^{m+1}}$;

do đó $\left(1+\sqrt{-6}\right)^{2^m} \equiv 1 \pmod{2^m}$.

Vẫn theo Bổ đề 3.2:

$\left(1+\sqrt{-6}\right)^{2^{m-1}} \equiv 1+2^{m-1}\sqrt{-6} \not\equiv 1 \pmod{2^m}$;

do đó cấp của $\left[1+\sqrt{-6}\right]$ trong $\phi_D(\alpha^{2m})$ là $2^m$.

Đối với $\phi_D(\alpha^{2m+1})$, ta có $\alpha^{2m+1} = \langle 2^m\rangle\alpha$, theo Bổ đề 3.2, ta có

$\left(1+\sqrt{-6}\right)^{2^m} \equiv 1+2^m\sqrt{-6} \pmod{2^{m+1}}$;

do $\alpha \mid \sqrt{-6}$ nên $\left(1+\sqrt{-6}\right)^{2^m} \equiv 1 \pmod{\alpha^{2m+1}}$.

Vẫn theo Bổ đề 3.2:

$\left(1+\sqrt{-6}\right)^{2^{m-1}} \equiv 1+2^{m-1}\sqrt{-6} \not\equiv 1 \pmod{2^m\alpha}$;

do đó cấp của $\left[1+\sqrt{-6}\right]$ trong $\phi_D(\alpha^{2m+1})$ là $2^m$.

3) Đối với $\phi_D(\beta^{2m})$, ta có $\beta^{2m} = \langle 3^m\rangle$, theo Bổ đề 3.2, ta có

$\left(1+\sqrt{-6}\right)^{3^m} \equiv 1+2.3^m\sqrt{-6} \pmod{3^{m+1}}$;

do đó $\left(1+\sqrt{-6}\right)^{3^m} \equiv 1 \pmod{3^m}$.

Vẫn theo Bổ đề 3.2:

$\left(1+\sqrt{-6}\right)^{3^{m-1}} \equiv 1+2.3^{m-1}\sqrt{-6} \not\equiv 1 \pmod{3^m}$;

do đó cấp của $\left[1+\sqrt{-6}\right]$ trong $\phi_D(\beta^{2m})$ là $3^m$.

Đối với $\phi_D(\beta^{2m+1})$, ta có $\beta^{2m+1} = \langle 3^m\rangle\beta$, theo Bổ đề 3.2, ta có

$\left(1+\sqrt{-6}\right)^{3^m} \equiv 1+2.3^m\sqrt{-6} \pmod{3^{m+1}}$;

do $\beta \mid \sqrt{-6}$ nên $\left(1+\sqrt{-6}\right)^{3^m} \equiv 1 \pmod{\beta^{2m+1}}$.

Vẫn theo Bổ đề 3.2:

$\left(1+\sqrt{-6}\right)^{3^{m-1}} \equiv 1+2.3^{m-1}\sqrt{-6} \not\equiv 1 \pmod{3^m\beta}$;

do đó cấp của $\left[1+\sqrt{-6}\right]$ trong $\phi_D(\beta^{2m+1})$ là $3^m$. ■

***Bổ đề 3.4.*** Cho $H, K$ là các nhóm con của nhóm Abel. Nếu $H = \langle a\rangle$ là nhóm con cyclic cấp $p^k (k \geq 1)$ và $a^{p^{k-1}} \notin K$ thì $H \cap K = \{e\}$.

*Chứng minh.* Ta có tập các nhóm con của $H$ là $\left\{\left\langle a^{p^i}\right\rangle;\ 0 \leq i \leq k\right\}$.

Do đó $H \cap K = \left\langle a^{p^j}\right\rangle$ với $0 \leq j \leq k$, nếu $j \leq k-1$ thì $a^{p^{k-1}} \in K$ trái so với giả thiết, dẫn đến $j = k$ và $H \cap K = \{e\}$. ■

### *3.2. Cấu trúc của nhóm $\phi_D(\pi_q^n)$*

***Định lí 3.5.*** Với $n \in \mathbb{N}, n \geq 1$, ta có

$\phi_D(\pi_q^n) \cong \mathbb{Z}_{q^n-q^{n-1}}$.

*Chứng minh.* Theo Định lí 2.3:

$\phi_D(\pi_q^n) = \{[a]: 1 \le a < q^n, \gcd(a,q) = 1\}$.

Lúc này, ánh xạ

$\phi_{\mathbb{Z}}(q^n) \to \phi_D(\pi_q^n), [a] \mapsto [a]$

là một đồng cấu, ngoài ra nếu như $[a] = [b]$ trong $\phi_D(\pi_q^n)$ hay $a \equiv b \pmod{\pi_q^n}$ thì theo chứng minh ở Định lí 2.1 ta có $q^n \mid_{\mathbb{Z}} (a-b)$, suy ra $a = b$ dẫn đến đồng cấu trên là một đơn cấu. Vì $|\phi_D(\pi_q^n)| = |\phi_{\mathbb{Z}}(q^n)| = q^n - q^{n-1}$ nên ánh xạ trên là đẳng cấu, do đó

$\phi_D(\pi_q^n) \cong \phi_{\mathbb{Z}}(q^n) \cong \mathbb{Z}_{q^n - q^{n-1}}$. ■

### 3.3. Cấu trúc của nhóm $\phi_D(\langle p^n \rangle)$

***Định lí 3.6.*** Với $n \in \mathbb{N}, n \ge 1$, ta có:

$\phi_D(\langle p^n \rangle) \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^2-1}$.

*Chứng minh.* Trước hết, áp dụng Bổ đề 3.3, ta suy ra cấp của $\left[1 + p\sqrt{-6}\right]$ trong nhóm $\phi_D(\langle p^n \rangle)$ là $p^{n-1}$, do đó $X = \langle \left[1 + p\sqrt{-6}\right] \rangle$ cũng có cấp là $p^{n-1}$.

Tiếp theo, ta xét ánh xạ

$\phi_{\mathbb{Z}}(p^n) \to \phi_D(\langle p^n \rangle), [a] \mapsto [a]$,

rõ ràng, ánh xạ này là một đơn cấu. Chú ý rằng $\phi_{\mathbb{Z}}(p^n)$ là nhóm cyclic có cấp là $\varphi_{\mathbb{Z}}(p^n) = p^{n-1}(p-1)$, từ đó tồn tại một lớp $[a]$ trong nhóm $\phi_{\mathbb{Z}}(p^n)$ có cấp đúng bằng $p^{n-1}$. Đặt $Y = \langle [a] \rangle$ trong $\phi_D(\langle p^n \rangle)$, khi đó cấp của $Y$ là $p^{n-1}$. Ngoài ra, từ Bổ đề 3.2 thì $\left(1 + p\sqrt{-6}\right)^{p^{n-2}} \equiv 1 + p^{n-1}\sqrt{-6} \pmod{p^n}$ nên

$\left[\left(1 + p\sqrt{-6}\right)^{p^{n-2}}\right] = \left[1 + p^{n-1}\sqrt{-6}\right] \notin Y$.

Bởi vậy theo Bổ đề 3.4, $X \cap Y = \{[1]\}$ và $XY$ có cấp $p^{2n-2}$. Ta có $\langle p \rangle$ là iđêan nguyên tố trong $D$ nên $D/_{\langle p \rangle}$ là trường có hữu hạn phần tử, dẫn đến $\phi_D(\langle p \rangle)$ là một nhóm cyclic có cấp $p^2 - 1$ (theo Hệ quả 2.4). Gọi $[\zeta]$ là phần tử sinh $\phi_D(\langle p \rangle)$ và $\sigma = \zeta^{p^{2n-2}}$. Đặt $k$ là cấp của $[\sigma]$ trong $\phi_D(\langle p^n \rangle)$. Vì $\phi_D(\langle p^n \rangle)$ có cấp là $\varphi_D(\langle p^n \rangle) = p^{2n-2}(p^2-1)$ nên $[\sigma]^{p^2-1} = [\zeta]^{p^{2n-2}(p^2-1)} = \left[\overline{1}\right]$ trong $\phi_D(\langle p^n \rangle)$, do đó $k \mid p^2 - 1$. Mặt khác $[\sigma]^k = \left[\overline{1}\right]$ trong $\phi_D(\langle p^n \rangle)$ nên $[\sigma]^k = \left[\overline{1}\right]$ trong $\phi_D(\langle p \rangle)$, suy ra $[\zeta]^{kp^{2n-2}} = \left[\overline{1}\right]$ trong $\phi_D(\langle p \rangle)$, do đó $p^2 - 1 \mid kp^{2n-2}$ hay $p^2 - 1 \mid k$. Vậy $k = p^2 - 1$ hay $[\sigma]$ có cấp là $p^2 - 1$ trong $\phi_D(\langle p^n \rangle)$. Lấy $Z = \langle [\sigma] \rangle$ trong $\phi_D(\langle p^n \rangle)$. Vì mọi phần tử trong $XY$ đều có cấp là luỹ thừa của $p$ nên $(XY) \cap Z = \left\{\left[\overline{1}\right]\right\}$ và cấp của nhóm $XYZ$ là $p^{2n-2}(p^2-1)$ và cũng chính là $\varphi_D(\langle p^n \rangle)$. Ta kết luận

$\phi_D(\langle p^n \rangle) = XYZ \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^2-1}$. ■

### 3.4. Cấu trúc của nhóm $\phi_D(\alpha^n)$

***Định lí 3.7.*** Ta có:

1) $\phi_D(\alpha) = \{\overline{1}\}$; $\phi_D(\alpha^2) = \left\langle \left[1 + \sqrt{-6}\right] \right\rangle \cong \mathbb{Z}_2$; $\phi_D(\alpha^3) = \left\langle \left[1 + \sqrt{-6}\right] \right\rangle \cong \mathbb{Z}_4$.
2) $\phi_D(\alpha^{2m}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_{2^m}$, với $m > 1$.
3) $\phi_D(\alpha^{2m+1}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^m}$, với $m > 1$.

*Chứng minh.*

1) Dễ dàng suy ra từ kiểm tra trực tiếp.

2) Với $m > 1$, trước hết theo Bổ đề 3.3, ta có $H = \langle[1 + \sqrt{-6}]\rangle$ là nhóm con có cấp $2^m$ của $\phi_D(\alpha^{2m})$. Tiếp theo, ta có ánh xạ:

$$\phi_{\mathbb{Z}}(2^m) \to \phi_D(\alpha^{2m}), [a] \mapsto [a]$$

là đơn cấu nhóm và $\phi_{\mathbb{Z}}(2^m) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}$ nên trong $\phi_D(\alpha^{2m})$ có nhóm con $K \cong \phi_{\mathbb{Z}}(2^m) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}$.

Theo Bổ đề 3.2, $\left[\left(1 + \sqrt{-6}\right)^{2^{m-1}}\right] = \left[1 + 2^{m-1}\sqrt{-6}\right] \notin K$ nên theo Bổ đề 3.4, $H \cap K = \{[1]\}$ và tích $HK$ là tích trực tiếp có cấp là $2^m.2^{m-1} = 2^{2m-1} = \varphi_D(\alpha^{2m})$. Như vậy:

$$\phi_D(\alpha^{2m}) = HK \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_{2^m}.$$

3) Chứng minh tương tự như (2), với lưu ý rằng đơn cấu nhóm ta xét sẽ là $\phi_{\mathbb{Z}}(2^{m+1}) \to \phi_D(\alpha^{2m+1}), [a] \mapsto [a]$. ■

### *3.5. Cấu trúc của nhóm $\phi_D(\beta^n)$*

***Định lí 3.8.*** Ta có:

1) $\phi_D(\beta) = \langle[2]\rangle \cong \mathbb{Z}_2$.

2) $\phi_D(\beta^{2m}) \cong \mathbb{Z}_{2.3^{m-1}} \times \mathbb{Z}_{3^m}$, với $m \geq 1$.

3) $\phi_D(\beta^{2m+1}) \cong \mathbb{Z}_{2.3^m} \times \mathbb{Z}_{3^m}$, với $m \geq 1$.

*Chứng minh.*

1) Do $\phi_D(\beta)$ chỉ có 2 phần tử là $[1], [2]$ nên đẳng cấu với $\mathbb{Z}_2$.

2) Với $m > 1$, trước hết theo Bổ đề 3.3, ta có $H = \langle[1 + \sqrt{-6}]\rangle$ là nhóm con có cấp $3^m$ của $\phi_D(\beta^{2m})$. Tiếp theo, ta có ánh xạ:

$$\phi_{\mathbb{Z}}(3^m) \to \phi_D(\beta^{2m}), [a] \mapsto [a]$$

là đơn cấu nhóm. Do đó nếu $[a]$ là phần tử sinh của $\phi_{\mathbb{Z}}(3^m)$ với $a \in \mathbb{Z}$ thì cấp của $[a]$ trong $\phi_D(\beta^{2m})$ là $2.3^{m-1}$. Suy ra $K = \langle[a]\rangle$ có cấp $2.3^{m-1}$ trong $\phi_D(\beta^{2m})$.

Theo Bổ đề 3.2, $\left[\left(1 + \sqrt{-6}\right)^{3^{m-1}}\right] = \left[1 + 2.3^{m-1}\sqrt{-6}\right] \notin K$ nên theo Bổ đề 3.4, $H \cap K = \{[1]\}$ và tích $HK$ là tích trực tiếp có cấp là $2.3^{2m-1} = \varphi_D(\beta^{2m})$. Như vậy:

$$\phi_D(\beta^{2m}) = HK \cong \mathbb{Z}_{2.3^{m-1}} \times \mathbb{Z}_{3^m}$$

3) Chứng minh tương tự như (2), với lưu ý rằng đơn cấu nhóm ta xét sẽ là $\phi_{\mathbb{Z}}(3^{m+1}) \to \phi_D(\beta^{2m+1}), [a] \mapsto [a]$. ■

### *3.6. Cấu trúc nhóm nhân $\phi_D(I)$ của vành thương $D/I$*

Do $D$ là miền Dedekind nên mỗi iđêan $I$ khác $0, D$ của $D$ đều có phân tích duy nhất dưới dạng $I = P_1^{n_1}P_2^{n_2} \dots P_k^{n_k}$, trong đó với mỗi $i \in \{1,2, \dots, k\}$, $P_i$ là các iđêan nguyên tố khác 0 được mô tả trong Định lí 2.1, $n_i$ là số nguyên dương. Dạng phân tích trên gọi là dạng phân tích tiêu chuẩn của iđêan $I$.

***Định lí 3.9.*** Cho iđêan $I$ khác $0, D$ của $D$ có phân tích tiêu chuẩn $I = P_1^{n_1}P_2^{n_2} \dots P_k^{n_k}$. Khi đó:

$$\phi_D(I) \cong \phi_D\left(P_1^{n_1}\right) \times \phi_D\left(P_2^{n_2}\right) \times \dots \times \phi_D\left(P_k^{n_k}\right);$$

do đó ta cũng có

$$\varphi_D(I) = \varphi_D\left(P_1^{n_1}\right)\varphi_D\left(P_2^{n_2}\right) \dots \varphi_D\left(P_k^{n_k}\right).$$

*Chứng minh.* Trước hết, ta chứng minh nhận xét sau: Cho $M, N$ là các iđêan của $D$, nguyên tố cùng nhau (tức $M + N = D$). Khi đó ánh xạ

$$\overline{\theta}: D/MN \to D/M \times D/N, \overline{\theta}(\overline{a}) = (\overline{a}, \overline{a})$$

là đẳng cấu vành.

Thật vậy, dễ thấy ánh xạ

$$\theta: D \to D/M \times D/N, \theta(\mathrm{a}) = (\overline{a}, \overline{a})$$

là đồng cấu vành có $Ker(\theta) = \{\mathrm{a} \in \mathrm{D}, \overline{a} = \overline{0}\ trong\ D/M\ và\ \overline{a} = \overline{0}\ trong\ D/N\}$

$$= \{\mathrm{a} \in \mathrm{D}, \mathrm{a} \in M \text{ và } \mathrm{a} \in N\} = M \cap N.$$

Ta luôn có $MN \subset M \cap N$. Vì $M, N$ nguyên tố cùng nhau nên tồn tại $x \in M, y \in N$ sao cho $x + y = 1$. Khi đó với $a \in M \cap N$ bất kì thì $a = ax + ay \in MN$. Vậy $MN = M \cap N$ nên $Ker(\theta) = MN$.

Tiếp theo, ta chứng minh θ là toàn cấu vành. Với mọi $a, b \in D$, xét $u = ay + bx$. Khi đó $u = a(1 - x) + bx = a + (b - a)x$ nên $\overline{u} = \overline{a}$ trong $D/M$ (vì $(b - a)x \in M$), ta cũng có $u = ay + b(1 - y) = b + (a - b)y$ nên $\overline{u} = \overline{b}$ trong $D/N$. Vậy $\theta(\mathrm{u}) = \left(\overline{a}, \overline{b}\right) \in D/M \times D/N$ hay θ là toàn cấu. Theo Định lí Noether thì θ cảm sinh đẳng cấu vành trên. Ta thấy rằng kết quả trên có thể mở rộng cho hữu hạn các iđêan của $D$, đôi một nguyên tố cùng nhau bằng quy nạp.

Từ đó, theo nhận xét trên, do các iđêan $P_1^{n_1}, P_2^{n_2}, \dots, P_k^{n_k}$ đôi một nguyên tố cùng nhau nên ta có đẳng cấu vành

$$\overline{\theta}: D/I \cong D/P_1^{\mathrm{n}_1} \times D/P_2^{\mathrm{n}_2} \times \dots \times D/P_k^{\mathrm{n}_\mathrm{k}}.$$

Đẳng cấu vành $\overline{\theta}$ cảm sinh đẳng cấu nhóm nhân

$$(D/I)^* \cong \left(D/P_1^{\mathrm{n}_1}\right)^* \times \left(D/P_2^{\mathrm{n}_2}\right)^* \times \dots \times \left(D/P_k^{\mathrm{n}_\mathrm{k}}\right)^*$$

hay

$$\phi_D(I) \cong \phi_D\left(P_1^{n_1}\right) \times \phi_D\left(P_2^{n_2}\right) \times \dots \times \phi_D\left(P_k^{n_k}\right).$$

Do đó ta có

$$\varphi_D(I) = \varphi_D\left(P_1^{n_1}\right)\varphi_D\left(P_2^{n_2}\right) \dots \varphi_D\left(P_k^{n_k}\right).$$ ■

Sau đây, chúng tôi đưa ra một ví dụ minh họa

***Ví dụ 3.10.*** Mô tả nhóm $\Phi_D(I)$ với

$$I = \langle 573300, 4118400 - 3900\sqrt{-6} \rangle.$$

Đầu tiên, ta phân tích $I$ thành các iđêan nguyên tố.

Ta có: $I = 3900\langle 147,1056 - \sqrt{-6} \rangle = 3900J$.

Theo Định lí 2.1 thì

$3900 = 2^2.3.5^2.13 = \alpha^4\beta^2\pi_5^2.\overline{\pi_5}^2.13.$

Ta phân tích $J = \langle 147, 1056 - \sqrt{-6}\rangle$ thành tích các iđêan nguyên tố.

Ta có:

$J.\bar{J} = \langle 147, 1056 - \sqrt{-6}\rangle.\langle 147, 1056 + \sqrt{-6}\rangle$

$= \langle 147^2, 147(1056 + \sqrt{-6}), 147(1056 - \sqrt{-6}), 1115142\rangle$

$= 147\langle 147, 1056 + \sqrt{-6}, 1056 - \sqrt{-6}, 7586\rangle = 147K.$

Vì $147,7586 \in K$ và $(147,7586) = 1$ nên $1 \in K$. Vậy $K = D$ và $J.\bar{J} = 147 = 3.7^2$.

Ta có:

i) $3 = \beta^2 \mid J.\bar{J}$ nên $\beta \mid J$ và $\beta \mid \bar{J}$.

ii) $7 = \langle 7, 1 + \sqrt{-6}\rangle.\langle 7, 1 - \sqrt{-6}\rangle = \pi_7.\overline{\pi_7}$. Khi đó $\pi_7.\overline{\pi_7} \mid J.\bar{J}$, dẫn đến $\pi_7 \mid J$ hoặc $\overline{\pi_7} \mid J$. Mà $1056 - \sqrt{-6} = 1057 - (1 + \sqrt{-6}) \in \pi_7$ và $147 \in \pi_7$ nên $\pi_7 \mid J$, từ đó $\overline{\pi_7} \mid \bar{J}$. Nếu như $\pi_7 \mid \bar{J}$ thì $\overline{\pi_7} \mid J$, thì $7 \mid J, J'$ và $J = J' = 7\beta$. Điều này mâu thuẫn vì $J \neq J'$. Vậy $\pi_7 \nmid \bar{J}$. Cuối cùng, ta có được $\pi_7^2 \mid J$ và $\overline{\pi_7}^2 \mid \bar{J}$.

Vậy $J = \beta\pi_7^2$. Do đó, phân tích tiêu chuẩn của $I$ là

$I = \alpha^4\beta^3\pi_5^2.\overline{\pi_5}^2.\pi_7^2.13.$

Áp dụng các Định lí 3.5 – 3.9, ta có:

$\Phi_D(I) \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_3 \times \mathbb{Z}_{20} \times \mathbb{Z}_{20} \times \mathbb{Z}_{42} \times \mathbb{Z}_{168}.$

$\varphi_D(I) = 2.4.6.3.20.20.42.168 = 406425600.$

❖ ***Tuyên bố về quyền lợi:*** *Các tác giả xác nhận hoàn toàn không có xung đột về quyền lợi.*

❖ ***Lời cảm ơn:*** *Nghiên cứu này được tài trợ bởi Nguồn ngân sách khoa học và công nghệ Trường Đại học Sư phạm Thành phố Hồ Chí Minh trong đề tài sinh viên nghiên cứu khoa học năm học 2025-2026.*

## TÀI LIỆU THAM KHẢO

Alaca, S., & Williams, K. S. (2004). *Introductory algebraic number theory*. Cambridge University Press.

Andreescu, T., Dospinescu, G., & Mushkarov, O. (2017). *Number theory: Concepts and problems*. XYZ Press.

Buçaj, V. (2014). Finding factors of factor rings over the Eisenstein integers. *International Mathematical Forum*, *9*(31), 1521–1537. https//doi.org/10.12988/imf.2014.111121

Cross, J. T. (1983). The Euler φ-function in the Gauss integers. *The American Mathematical Monthly, 90*(8), 518–528. https//doi.org/10.2307/2322785

Dresden, G., & Dymáček, W. M. (2005). Finding factors of factor rings over the Gaussian integers. *The American Mathematical Monthly*, *112*(7), 602–611. https//doi.org/10.1080/00029890.2005.11920231

Greene, J., & Jing, W. (2024). The factor ring structure of quadratic principal ideal domains. *The American Mathematical Monthly*, *131*(1), 20–29. https//doi.org/10.1080/00029890.2023.2261827

My, V. Q., & Cao, P. A. D. (2025). The structure of multiplicative groups of residue class rings of the eisenstein integers. *Ho Chi Minh City University of Education Journal of Science*, *22*(5), 814-823. https://doi.org/10.54607/hcmue.js.22.5.4730(2025)

Niven, I., & Zuckerman, H. S. (1980). *An introduction to the theory of numbers* (4th ed.). Wiley.

---

## THE STRUCTURE OF THE MULTIPLICATIVE GROUP OF THE QUOTIENT RING OF THE RING OF ALGEBRAIC INTEGERS $\mathbb{Z}[\sqrt{-6}]$

***My Vinh Quang, Nguyen Cao Minh****

*Ho Chi Minh City University of Education, Vietnam*

**Corresponding author: Nguyen Cao Minh – Email: 4901101055@student.hcmue.edu.vn*

*Received: November 14, 2025; Revised: November 20, 2025; Accepted: December 25, 2025*

## ABSTRACT

*This paper provides a detailed description of the multiplicative group structure of the quotient rings of the ring of algebraic integers $\mathbb{Z}[\sqrt{-6}]$ with respect to powers of prime ideals. As a consequence, a complete characterization of the unit group of the quotient rings of $\mathbb{Z}[\sqrt{-6}]$ is established for every nonzero ideal. Finally, the paper presents an illustrative example to demonstrate the application of the obtained results in a specific case.*

***Keywords:*** multiplicative group of a quotient ring; quotient ring; ring of algebraic integers