신 용 수 교수지도

석 사 학 위 논 문

AN INTEGRALLY CLOSED DOMAIN $\mathbb{Z}[\sqrt{2p}]$

2008

성신여자대학교 교육대학원

교육학과 수학교육전공

공 현 남

AN INTEGRALLY CLOSED DOMAIN $\mathbb{Z}[\sqrt{2p}]$

신 용 수 교수지도

이 논문을 석사학위논문으로 제출함.

2008월 5월

성신여자대학교 교육대학원

교육학과 수학교육전공

공 현 남

인 준 서

공현남의 석사학위 논문으로 인준함.

심사위원 _____ 인

심사위원 _____ 인

심사위원 _____ 인

성신여자대학교 교육대학원

논 문 개 요

Z가 정수환이고 $\mathbb{Q}$를 유리수체라 하였을 때 홀수인 소수 p에 대해서 Z[$\sqrt{2p}$]의 성질을 연구하였다.

p와 q가 서로 다른 소수이고 α와 β가 유리수일 때 s를 $\alpha+\beta\sqrt{pq}$라 하였다. s가 Z[$\sqrt{pq}$]위에서 대수적이고 s가 유리수가 아닐 때 s는 정수계수다항식 x^2+ax+b의 해가된다. 또한 s가 x^2+ax+b의 해이고 $\beta \neq 0$일 때 $a=-2\alpha$, $b=\alpha^2+pq\beta^2$이 된다. 이러한 결과를 통하여 Z[$\sqrt{2p}$]가 대수적으로 닫혀있다는 것을 증명하였다.

목 차

AN INTEGRALLY CLOSED DOMAIN $\mathbb{Z}[\sqrt{2p}]$

HYUN-NAM KONG

1. Introduction

Let $\mathbb{Z}$ be a ring of integers and $\mathbb{Q}$ be the field of rational numbers.

In this thesis, we study some properties of a ring $\mathbb{Z}[\sqrt{2p}] = \{a + b\sqrt{2p} \mid a, b \in \mathbb{Z}\}$ when p is an odd prime number.
In Section 2, we introduce some properties of integral elements, and we show that if S is an extension ring of R and $s \in S$ and s is integral over R, then $R[s]$ is a finitely generated R-module (see Remark 3). And we prove that $\overline{R}_s = \{s \in S \mid s \text{ is integral over } R\}$ is a ring which is integral over R (see Lemma 6).

In Section 3, we introduce integrally closed domains. We show that if D is a unique factorization domain, then D is integrally closed (see Lemma 8). For example, $\mathbb{Z}$ is integrally closed.

Let $s = \alpha + \beta\sqrt{pq} \in \mathbb{Q}[\sqrt{pq}]$ where α, $\beta \in \mathbb{Q}$, p and q are distinct prime numbers. We prove that if s is integral over $\mathbb{Z}[\sqrt{pq}]$, and $s \in \mathbb{Q}[\sqrt{pq}] - \mathbb{Q}$, then s is a zero of $x^2 + ax + b \in \mathbb{Z}[x]$ with $a, b \in \mathbb{Z}$ and $\beta \neq 0$, then $a = -2\alpha$ and $b = \alpha^2 - pq\beta^2$ (see Lemma 18).

Using the above result, we obtain that $\mathbb{Z}[\sqrt{2p}]$ is integrally closed when p is an odd prime (see Theorem 19).

2. Preliminaries

First we introduce following lemmas to see some properties of integral elements.

Definition 1 (Definition 5.2, [2])**.** Let S be an extension ring of R and $s \in S$. If there exists a monic polynomial $f(x) \in R[x]$ such that s is a root of f (that is, $f(s) = 0$), then s is said to be ***integral*** over R. If every element of S is ***integral*** over R, S is said to be an ***integral extension*** of R.

Lemma 2. *Let R be a commutative ring with unity 1. Suppose $(b_1, \ldots, b_n)$ is a solution of the linear system of a homogeneous linear equation*

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n &= 0 \end{aligned}$$

where $a_{ij} \in R$ for every $i, j = 1, \ldots, n$. If $A = (a_{ij})$ is the $n \times n$ matrix of coefficients, then $\det(A)b_i = 0$ for every i.

Proof. If B_i is the $n \times n$ diagonal matrix with diagonal entries $1, \ldots, 1, b_i, 1, \ldots, 1$, then $\det(AB_i) = \det(A)\det(B_i) = \det(A)b_i$. Let $A_i = [a_{1i}, a_{2i}, \cdots, a_{ni}]^t$, for every $i = 1, 2, \ldots, n$. To show that $\det(AB_i) = 0$, we add b_i times column j of AB_i to column i for every $j \neq i$, that is,

$$\begin{aligned} \det(AB_i) &= \det(A_1, \cdots, b_iA_i, \cdots, A_n) \\ &= \det(A_1, \ldots, \underbrace{b_1A_1 + b_2A_2 + \cdots + b_nA_n}, \ldots, A_n) \end{aligned}$$

$j \neq i$. Since $(b_1, \ldots, b_n)$ is a solution of a linear system, we have

$$\begin{aligned} b_1a_{11} + b_2a_{12} + \cdots + b_na_{1n} &= 0, \\ b_1a_{21} + b_2a_{22} + \cdots + b_na_{2n} &= 0, \\ &\vdots \\ b_1a_{n1} + b_2a_{n2} + \cdots + b_na_{nn} &= 0, \end{aligned}$$

that is,

$$b_1A_1 + b_2A_2 + \cdots + b_nA_n = 0.$$

Thus

$$\det(A_1, \cdots, A_{i-1}, \mathbf{0}, A_{i+1}, \cdots, A_n) = \mathbf{0}.$$

Therefore, we have that $\det(A)b_i{=}0$ for every i, as we wished. □

Remark 3. (a) Let S be an extension ring of R and $s \in S$. Assume s is integral over R. Then there exists a polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$ such that $f(s) = 0$. In other words, we have

$$\begin{aligned} & s^n + a_{n-1}s^{n-1} + \cdots + a_1s + a_0 = 0 \\ \Rightarrow \quad & s^n = -a_{n-1}s^{n-1} - \cdots - a_1s - a_0 \\ \Rightarrow \quad & s^n \in R \cdot 1 + R \cdot s + \cdots + R \cdot s^{n-1} \\ \Rightarrow \quad & R[s] = \langle 1, s, \ldots, s^{n-1} \rangle \quad \text{as an } R\text{-module,} \end{aligned}$$

which means that $R[s]$ is a finitely generated R-module.

(b) If S is a finitely generated R-module, then there exist $s_1, \ldots, s_n \in S$ such that

$$S = Rs_1 + \cdots + Rs_n.$$

Let $s \in S$. Since $ss_i \in S$ for every $i = 1, \ldots, n$, we have

$$\begin{aligned} ss_1 &= a_{11}s_1 + \cdots + a_{1n}s_n \\ ss_2 &= a_{21}s_1 + \cdots + a_{2n}s_n \\ &\vdots \\ ss_n &= a_{n1}s_1 + \cdots + a_{nn}s_n \end{aligned}$$

for some $a_{ij} \in R$ for every $i, j = 1, \ldots, n$. Consequently, we have

$$\begin{aligned} (a_{11} - s)s_1 + a_{12}s_2 + \cdots + a_{1n}s_n &= 0 \\ a_{21}s_1 + (a_{22} - s)s_2 + \cdots + a_{2n}s_n &= 0 \\ &\vdots \\ a_{n1}s_1 + a_{n2}s_2 + \cdots + (a_{nn} - s)s_n &= 0. \end{aligned}$$

Let $A = (a_{ij})$ be the $n \times n$ matrix and let $\det(A - sI_n) = u \in S$ where I_n is the $n \times n$ unit matrix. Then, by Lemma 2, we obtain that $us_i = 0$ for every $i = 1, \ldots, n$.
Now, for every $t \in S$, there exist $t_1, \ldots, t_n \in R$ such that

$$t = t_1 s_1 + \cdots + t_n s_n.$$

Hence

$$\begin{aligned} u \cdot t &= u(t_1 s_1 + \cdots + t_n s_n) \\ &= u(t_1 s_1) + \cdots + u(t_n s_n) \\ &= t_1(us_1) + \cdots + t_n(us_n) \\ &= t_1 \cdot 0 + \cdots + t_n \cdot 0 \\ &= 0. \end{aligned}$$

In other words, u annihilates S, that is, $u \cdot S = \{0\}$. In particular, since $1 \in S$, we have $u = u \cdot 1 = 0$. If $f(x) = \det(A - xI_n)$ in $R[x]$, then either f or $-f$ is a monic polynomial and $\pm f(s) = \pm \det(A - sI_n) = \pm u = 0$, and thus S is integral over R as we wished.

In particular, s is integral over R if and only if $R[s]$ is a finitely generated R-module.

(c) Assume S is an extension ring of R and T is an extension ring of S. If S is a finitely generated R-module and T is a finitely generated S-module, then T is a finitely generated R-module.
In fact, suppose $S = Rs_1 + \cdots + Rs_p$ where $s_i \in S$ for $i = 1, 2, \ldots, p$, and $T = St_1 + \cdots + St_q$ where $t_j \in T$ for $j = 1, 2, \ldots, q$. Then, for every $t \in T$, there exist $b_1, \ldots, b_q \in S$ such that $t = b_1 t_1 + \cdots + b_q t_q$. Moreover, since $b_j \in S$, for every $j = 1, \ldots, q$, there exist $a_{j1}, \ldots, a_{jp} \in R$ such that $b_j = a_{j1} s_1 + a_{j2} s_2 + \cdots + a_{jp} s_p$.

In other words,

$$\begin{aligned} t &= b_1t_1 + \cdots + b_qt_q \\ &= (a_{11}s_1 + a_{12}s_2 + \cdots + a_{1p}s_p) \cdot t_1 + \\ &\quad (a_{21}s_1 + a_{22}s_2 + \cdots + a_{2p}s_p) \cdot t_2 \\ &\quad + \cdots + \\ &\quad (a_{q1}s_1 + a_{q2}s_2 + \cdots + a_{qp}s_p) \cdot t_q \\ &= \sum_{1\le i\le p, 1\le j\le q} a_{ij}(s_jt_i), \end{aligned}$$

which means that T is a finitely generated R-module.
In general, if S_{i+1} is an extension ring of S_i and S_{i+1} is a finitely generated S_i-module for $i = 1, 2, \ldots, n-1$, then S_n is a finitely generated S_1-module.

Definition 4 (Definition 31.3, [1])**.** An integral domain D is a unique factorization domain (abbreviated UFD) if the following conditions are satisfied:

(a) Every element of D that is neither 0 nor a unit can be factored into a product of a finite number of irreducibles of D.
(b) If $p_1 \cdots p_r$ and $q_1 \cdots q_s$ are two factorizations of the same element of D into irreducibles of D, then $r = s$ and the q_j can be renumbered so that p_i and q_i are associates.

We recall some well-known results in the following remark for the rest of this section.

Remark 5. (a) Let S be a ring extension of R. If S is finitely generated as an R-module, then S is integral over R by Remark 3 (b).
(b) Let S and R be as in (a). Assume $s_1, \ldots, s_t \in S$ are integral over R. Note that $R[s_1, \ldots, s_i] = R[s_1, \ldots, s_{i-1}][s_i]$ is a finitely generated $R[s_1, \ldots, s_{i-1}]$-module. Hence, by Remark 3 (c), $R[s_1, \ldots, s_t]$ is also a finitely generated R-module, and so by Remark 3 (b), $R[s_1, \ldots, s_t]$ is integral over R.

(c) Assume T is an integral extension ring of S and S is an integral extension of R. Then T is an integral extension of R.
In fact for every $t \in T$, there exist $s_0, \ldots, s_{n-1} \in S$ such that $s_0 + s_1 t + \cdots + s_{n-1}t^{n-1} + t^n = 0$. In other words, t is integral over $R[s_0, s_1, \ldots, s_{n-1}]$ and hence $R[s_0, \ldots, s_{n-1}][t] = R[s_0, s_1, \ldots, s_{n-1}, t]$ is a finitely generated $R[s_0, s_1, \ldots, s_{n-1}]$-module by Remark 3 (a). Thus, by Remark 3 (b), $R[s_0, \ldots, s_{n-1}, t]$ is a finitely generated R-module, that is, t is also integral over R.

(d) Let D be a unique factorization domain and F be a field of quotients of D. It is well-known that a nonconstant $f(x) \in D[x]$ factors into a product of two polynomials of lower degrees r and s in $F[x]$ if and only if it has a factorization into polynomials of the same degrees r and s in $D[x]$.

(e) Let D and F be as in (d) and $f(x)$ be a primitive polynomial of positive degree in $D[x]$. Then $f(x)$ is irreducible in $D[x]$ if and only if $f(x)$ is irreducible in $F[x]$.

Lemma 6. *Let S be a ring extension of R and let $\overline{R}_s := \{s \in S \mid s \text{ is integral over } R\}$. Then $\overline{R}_s$ is a ring such that*

(a) $R \leq \overline{R}_s \leq S$;
(b) $\overline{R}_s$ *is integral over* R.

Proof. If suffices to show that $\overline{R}_s$ is a ring. For every $\alpha, \beta \in \overline{R}_s$, note that $R[\alpha, \beta]$ is integral over R by Remark 3 (b) (or Remark 5 (a)). In other words, $\alpha \pm \beta$, $\alpha\beta \in R[\alpha, \beta]$, that is, $\alpha \pm \beta$, $\alpha\beta \in \overline{R}_s$, as we wished. □

3. Integrally Closed Domains

Definition 7 ([2])**.** (a) Let S be a ring extension of R. The ring $\overline{R}_s$ of Lemma 6 is the integral closure of R in S. In particular, if $R{=}\overline{R}_s$, then R is ***integrally closed*** in S.

(b) An integral domain R is ***integral closed*** if R is integral closed in its quotient field.

Lemma 8. *Let D and F be as in Remark 5 (d) again. If $s \in F$ is integral over D, then $s \in D$. In other words, D is integrally closed.*

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a monic polynomial in $D[x]$ such that $f(s) = 0$ and let $s = \frac{q}{p}$ where $p, q \in D$ and $\gcd(p, q) = 1$.
(Note that $\gcd(p, q)$ always exists since D is a UFD.)
Hence

$$\begin{aligned} & (\tfrac{q}{p})^n + a_{n-1}(\tfrac{q}{p})^{n-1} + \cdots + a_1(\tfrac{q}{p}) + a_0 = 0 \\ \Rightarrow \quad & q^n + a_{n-1}q^{n-1}p + \cdots + a_1qp^{n-1} + a_0p^n = 0 \\ \Rightarrow \quad & p \mid q^n \\ \Rightarrow \quad & p \mid q. \end{aligned}$$

Since $\gcd(p, q) = 1$, we have p is a unit of D. In other words, $s = \frac{q}{p} = p^{-1}q$ is in D. Hence D is integrally closed, as we wanted. □

Before we prove the main result in this section, we need the following lemma, which we will also use in the next section.

Definition 9 (Definition 45.21, [1])**.** Let D be a UFD. A nonconstant polynomial

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

in $D[x]$ is ***primitive*** if 1 is a gcd of the a_i for $i = 0, 1, \ldots, n$.

Lemma 10 (Lemma 45.13, [1]). *If D is a UFD, then for every nonconstant $f(x) \in D[x]$ we have $f(x) = (c)g(x)$, where $c \in D$, $g(x) \in D[x]$, and $g(x)$ is primitive. The element c is unique up to a unit factor in D and is the* ***content of*** *$f(x)$. Also $g(x)$ is unique up to a unit factor in D.*

Lemma 11 (Lemma 45.25, [1]). *If D is a UFD, then a product of two primitive polynomials in $D[x]$ is again primitive.*

Definition 12 (Definitions 29.6, 31.1, [1]).
(a) An element α of an extension field E of a field F is ***algebraic over*** F if $f(\alpha) = 0$ for some nonzero $f(x) \in F[x]$.
(b) An extension field E of a field F is an ***algebraic extension of*** F if every element in E is algebraic over F.

Definition 13 (Definition 31.2, [1]). If an extension field E of a field F is of finite dimension n as a vector space over F, then E is a ***finite extension of degree n over*** F. We shall let $[E : F]$ be the ***degree*** n of E over F.

Theorem 14 (Theorem 31.3, [1]). *A finite extension field E of a field F is an algebraic extension of F.*

Theorem 15 (Theorem 29.18, [1]). *Let E be a simple extension $F(\alpha)$ of a field F, and let α be algebraic over F. Let the degree of $irr(\alpha, F)$ be $n \geq 1$. Then every element β of $E = F(\alpha)$ can be uniquely expressed in the from*

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

where b_i is in F.

Theorem 16 (Theorem 31.4, [1]). *If E is a finite extension field of a field F, and K is a finite extension field of E, then K is a finite extension of F, and*

$$[K : F] = [K : E][E : F].$$

Theorem 17 (Theorem 29.13, [1]). *Let E be an extension field of F, and let $\alpha \in E$, where α is algebraic over F. Then there is an irreducible polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$. This irreducible polynomial $p(x)$ is uniquely determined up to a constant factor in F and is a polynomial of minimal degree ≥ 1 in $F[x]$ having α as a zero. If $f(\alpha) = 0$ for $f(x) \in F[x]$, with $f(x) \neq 0$, then $p(x)$ divides $f(x)$.*

Lemma 18. *Let p and q be distinct prime numbers.*

(a) *The integral domain $\mathbb{Z}[\sqrt{pq}]$ is an integral extension of $\mathbb{Z}$ with quotient field $\mathbb{Q}[\sqrt{pq}]$.*

(b) *Let $s \in \mathbb{Q}[\sqrt{pq}]$ be integral over $\mathbb{Z}[\sqrt{pq}]$. Then s is integral over $\mathbb{Z}$. In particular, if $s \in \mathbb{Q}$ is integral over $\mathbb{Z}$, then $s \in \mathbb{Z}$. If $s \in \mathbb{Q}[\sqrt{pq}] - \mathbb{Q}$, then s is a zero of $x^2 + ax + b$ in $\mathbb{Z}[x]$.*

(c) *Let $s = \alpha + \beta\sqrt{pq} \in \mathbb{Q}[\sqrt{pq}]$ where $\alpha, \beta \in \mathbb{Q}$. If s is a zero of $x^2 + ax + b \in \mathbb{Z}[x]$ and $\beta \neq 0$, then $a = -2\alpha$ and $b = \alpha^2 - pq\beta^2$.*

Proof. (a) For every $a + b\sqrt{pq} \in \mathbb{Z}[\sqrt{pq}]$ with $a, b \in \mathbb{Z}$, $a + b\sqrt{pq}$ is a zero of a monic polynomial $x^2 - 2ax + (a^2 - b^2pq) \in \mathbb{Z}[x]$. Hence $a + b\sqrt{pq}$ is integral over $\mathbb{Z}$, $\mathbb{Z}[\sqrt{pq}]$ is an integral extension of $\mathbb{Z}$.

Now let $a+b\sqrt{pq}$ and $c+d\sqrt{pq}$ be in $\mathbb{Z}[\sqrt{pq}]$ where a, b, c, and $d \in \mathbb{Z}$, and $c+d\sqrt{pq} \neq 0$. Then

$$\frac{a + b\sqrt{pq}}{c + d\sqrt{pq}} = \frac{(a + b\sqrt{pq})(c - d\sqrt{pq})}{c^2 - d^2pq}$$

$$= \frac{ac - bdpq}{c^2 - d^2pq} + \frac{cd - ad}{c^2 - d^2pq}\sqrt{pq} \in \mathbb{Q}[\sqrt{pq}],$$

and so any quotient of two elements in $\mathbb{Z}[\sqrt{pq}]$ is in $Q[\sqrt{pq}]$. Conversely, for every

$p + q\sqrt{pq} \in \mathbb{Q}[\sqrt{pq}]$ with $p, q \in \mathbb{Q}$, let $p = \frac{a}{b}$ and $q = \frac{c}{d}$ where $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{Z} - \{0\}$.
Then

$$\begin{aligned} p + q\sqrt{pq} &= \frac{a}{b} + \frac{c}{d}\sqrt{pq} \\ &= \frac{ad + bc\sqrt{pq}}{bd}. \end{aligned}$$

Note that $ad + bc\sqrt{pq}$ and bd are in $\mathbb{Z}[\sqrt{pq}]$. In other words, $p + q\sqrt{pq}$ is a quotient of two elements in $\mathbb{Z}[\sqrt{pq}]$. Therefore, $\mathbb{Q}[\sqrt{pq}]$ is contained in a quotient field of $\mathbb{Z}[\sqrt{pq}]$, that is, $\mathbb{Q}[\sqrt{pq}]$ is a quotient field of $\mathbb{Z}[\sqrt{pq}]$.

(b) Since $\sqrt{pq}$ is a zero of $x^2 - pq \in \mathbb{Z}[x]$, we have $\sqrt{pq}$ is integral over $\mathbb{Z}$, and so $\mathbb{Z}[\sqrt{pq}]$ is integral over $\mathbb{Z}$ by Remark 5 (b).
Since $\mathbb{Z}[\sqrt{pq}]$ is integral over $\mathbb{Z}$, that is, $\mathbb{Z}[\sqrt{pq}]$ is a finitely generated $\mathbb{Z}$-module, and so by Remark 3 (b), $\mathbb{Z}[\sqrt{pq}, s]$ is also a finitely generated $\mathbb{Z}$-module, that is, s is also integral over $\mathbb{Z}$.

Now let $s \in \mathbb{Q}$ be integral over $\mathbb{Z}$. Since $\mathbb{Z}$ is a UFD and $\mathbb{Q}$ is a field of quotient of $\mathbb{Z}$, by Lemma 8, $s \in \mathbb{Z}$.

Assume $s \in \mathbb{Q}[\sqrt{pq}] - \mathbb{Q}$. Note that $\sqrt{pq}$ is a zero of $x^2 - pq \in \mathbb{Q}[x]$ and $\sqrt{pq} \notin \mathbb{Q}$, that is, $[\mathbb{Q}[\sqrt{pq}] : \mathbb{Q}] = 2$. In other words, $\mathbb{Q}[\sqrt{pq}]$ is a finite extension of $\mathbb{Q}$, that is, by Theorem 14, $s \in \mathbb{Q}[\sqrt{pq}] - \mathbb{Q}$ is algebraic over $\mathbb{Q}$. Hence there exists a nonzero polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(s) = 0$. Moreover, since s is integral over $\mathbb{Z}$, we may assume that $f(x) \in \mathbb{Z}[x]$ and $f(x)$ is a monic polynomial. Since $\mathbb{Q} \lneq \mathbb{Q}[s] \leq \mathbb{Q}[\sqrt{pq}]$ and $[\mathbb{Q}[\sqrt{pq}] : \mathbb{Q}] = 2$, by Theorem 16, $[\mathbb{Q}[s] : \mathbb{Q}] = 2$. In other words, s is a zero of a quadratic irreducible polynomial $g(x) \in \mathbb{Q}[x]$.
Note that $f(x) = g(x) \cdot h(x)$ where $h(x) \in \mathbb{Q}[x]$, by Theorem 17. Note that $cg(x), dh(x) \in \mathbb{Z}[x]$ for some nonzero integers $c, d \in \mathbb{Z}$. Hence $cg(x) = (c_1) \cdot g_1(x)$, $dh(x) = (d_1)h_1(x)$ where $c_1, d_1 \in \mathbb{Z}$ are contents of $cg(x)$ and $dh(x)$, respectively. Since $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$.

Thus

$$\begin{aligned}(cd)f(x) &= (cg(x))(dh(x)) \\ &= (c_1g_1(x))(d_1h_1(x)) \\ &= (c_1d_1)(g_1(x)h_1(x)).\end{aligned}$$

Note that $f(x)$ and $g_1(x)h_1(x)$ are all primitive polynomials by Lemma 11. Moreover, by Theorem 17, $f(x) = \pm g_1(x) \cdot h_1(x)$. Without loss of generality, we may assume that $g_1(x)$ and $h_1(x)$ are monic polynomials in $\mathbb{Z}[x]$.
Furthermore, s is a zero of $g_1(x) \in \mathbb{Z}[x]$ and $\deg g_1(x) = 2$. That is, s is a zero of $g_1(x) = x^2 + ax + b \in \mathbb{Z}[x]$.

(c) Let s be a zero of $x^2 + ax + b \in \mathbb{Z}[x]$, such that,

$$\begin{aligned}& (\alpha + \beta\sqrt{pq})^2 + a(\alpha + \beta\sqrt{pq}) + b = 0 \\ \Rightarrow\ & (\alpha^2 + \beta^2 pq + a\alpha + b) + (2\alpha\beta + a\beta)\sqrt{pq} = 0 \\ \Rightarrow\ & \alpha^2 + \beta^2 pq + a\alpha + b = 0 \text{ and } 2\alpha\beta + a\beta = 0.\end{aligned}$$

Since $2\alpha\beta + a\beta = 0$ and $\beta \neq 0$, we set $a = -2\alpha$. Moreover,

$$\begin{aligned}& \alpha^2 + \beta^2 pq + (-2\alpha^2) + b = 0 \\ \Rightarrow\ & -\alpha^2 + \beta^2 pq + b = 0 \\ \Rightarrow\ & b = \alpha^2 - \beta^2 pq.\end{aligned}$$

Therefore $a = -2\alpha$ and $b = \alpha^2 - pq\beta^2$. □

Theorem 19. *Let p be an odd prime number. Then $\mathbb{Z}[\sqrt{2p}]$ is integrally closed.*

Proof. First, by Lemma 18 (a), the quotient field of $\mathbb{Z}[\sqrt{2p}]$ is $\mathbb{Q}[\sqrt{2p}]$.
Let $s = \alpha + \beta\sqrt{2p} \in \mathbb{Q}[\sqrt{2p}]$ with $\alpha, \beta \in \mathbb{Q}$ and s be integral over $\mathbb{Z}[\sqrt{2p}]$. Then, by Lemma 18 (b), s is integral over $\mathbb{Z}$. In particular, by Lemma 18 (b) again, if $s \in \mathbb{Q}$, then $s \in \mathbb{Z}$, and hence $s \in \mathbb{Z}[\sqrt{2p}]$.

So, we assume $s \in \mathbb{Q}[\sqrt{2p}]-\mathbb{Q}$. Then, by Lemma 18 (c), s is a zero of $x^2+ax+b \in \mathbb{Z}[x]$ with $a, b \in \mathbb{Z}$, and

$$a = -2\alpha, \qquad b = \alpha^2 - 2q\beta^2.$$

Assume a is odd. Let $\beta = \frac{k}{\ell}$ $(k, \ell \in \mathbb{Z},\ (k, \ell) = 1)$.

$$\begin{aligned} & b = \alpha^2 - 2q\beta^2 = \frac{a^2}{4} - \frac{2qk^2}{\ell^2} \\ \Leftrightarrow \quad & 4b\ell^2 = a^2\ell^2 - 8qk^2 \\ \Rightarrow \quad & 2 \mid a^2\ell^2 \\ \Rightarrow \quad & 2 \mid \ell^2 \qquad (\because (a, 2) = 1) \\ \Rightarrow \quad & \ell \text{ is even.} \end{aligned}$$

Let $\ell = 2m$ and $m \in \mathbb{Z}$. Then

$$\begin{aligned} & 4b\ell^2 = a^2 4m^2 - 8qk^2 \\ \Leftrightarrow \quad & 4bm^2 = a^2m^2 - 2qk^2 \\ \Rightarrow \quad & 2 \mid a^2m^2 \\ \Rightarrow \quad & 2 \mid m^2 \qquad (\because (a, m) = 1) \\ \Rightarrow \quad & 2 \mid m. \end{aligned}$$

Let $m = 2r$ and $r \in \mathbb{Z}$. Then

$$\begin{aligned} & 8br^2 = 2a^2r^2 - qk^2 \\ \Rightarrow \quad & 2 \mid qk^2 \\ \Rightarrow \quad & 2 \mid k^2 \qquad (\because (q, 2) = 1) \\ \Rightarrow \quad & 2 \mid k \\ \Rightarrow \quad & k \text{ is even.} \end{aligned}$$

Thus $(k, \ell) \geq 2$, a contradiction. Hence a can not be odd, that is, a has to be even.

Then $\alpha = -\frac{a}{2} \in \mathbb{Z}$. Since $b \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}$,

$$b - \alpha^2 = -2q\beta^2 := n \in \mathbb{Z}.$$

Let $\beta = \frac{d}{c}$ where $c, d \in \mathbb{Z}$ and $(c, d) = 1$. Hence

$$\begin{aligned} & (-2q)(\frac{d^2}{c^2}) = n \\ \Rightarrow \quad & c \mid -2qd^2 = c^2 \cdot n \\ \Rightarrow \quad & c \mid 2q \qquad (\because (c, d) = (c, d^2) = 1) \end{aligned}$$

First, if $c = 2 \cdot e$ for some $e \in \mathbb{Z}$, then

$$\begin{aligned} & -2qd^2 = 4e^2n \\ \Rightarrow \quad & -qd^2 = 2e^2n \\ \Rightarrow \quad & 2 \mid (-qd^2) \\ \Rightarrow \quad & 2 \mid d^2 \qquad (\because (2, q) = 1) \\ \Rightarrow \quad & d \text{ is even.} \end{aligned}$$

Hence, $(c, d) \geq 2$, a contradiction.

If $c = q \cdot f$, for some $f \in \mathbb{Z}$, then

$$\begin{aligned} & -2qd^2 = q^2f^2n \\ \Rightarrow \quad & -2d^2 = qf^2n \\ \Rightarrow \quad & q \mid (-2d^2) \\ \Rightarrow \quad & q \mid d \qquad (\because (2, q) = 1) \end{aligned}$$

Hence, $(c, d) \geq q > 1$, a contradiction. In other words, $c = \pm 1$, that is $\beta = \pm d \in \mathbb{Z}$. Therefor $s = \alpha + \beta\sqrt{2p} \in \mathbb{Z}[\sqrt{2p}]$ and so $\mathbb{Z}[\sqrt{2p}]$ is integrally closed, as we desired. $\square$

References

[1] John B. Fraleigh, *A first course in abstract algebra*, Addison-Wesley, Seventh edition(2003).
[2] T.W. Hungerford, *Algebra*, Springer-Verlag, (1973).

ABSTRACT

AN INTEGRALLY CLOSED DOMAIN $\mathbb{Z}[\sqrt{2p}]$

Kong Hyun Nam
Major in Mathematics Education
Graduate school of Education
Sungshin Women's University
Supervised by Professor Shin Yong su Ph.D.

Let Z be a ring of integers and $\mathbb{Q}$ be a field of rational numbers. In this thesis, we study some properties of a ring Z[$\sqrt{2p}$] when p is an odd prime number.

Let s = $\alpha + \beta\sqrt{pq} \in \mathbb{Q}\sqrt{pq}$ where α, $\beta \in \mathbb{Q}$, p and q are distinct prime numbers. We prove that if s is integral over Z[$\sqrt{pq}$], and s $\in \mathbb{Q}\sqrt{pq} - \mathbb{Q}$, then s is a zero of $x^2 + ax + b \in$ Z[x] with a, b $\in$ Z and $\beta \neq 0$,

then $a = -2\alpha$ **and** $b = \alpha^2 - pq\beta^2$.

Using the above result, we obtain that $Z[\sqrt{2p}]$ **is integrally closed.**