หอสมุดกลาง สถาบันวิทยบริการ จุฬาลงกรณ์มหาวิทยาลัย

CHAPTER II

PRELIMINARIES

In this thesis, we shall assume that the reader is familiar with common terms used in set theory and basic knowledge of abstract algebra. The materials are standard and can be found in the reference [1] .

However, we shall review some important definitions and results. We shall use the following notations:

$\mathbb{N}$ = the set of all positive integers.

$\mathbb{Z}$ = the set of all integers.

$\mathbb{Q}$ = the set of all rational numbers.

$\mathbb{C}$ = the set of all complex numbers.

An integer p in $\mathbb{Z}$ is said to be a prime if (i) $p\neq\pm 1$ and (ii) if $a|p$, then $a=\pm 1$ or $a=\pm p$. In this thesis, we shall consider only positive prime. So when we say that $p\in\mathbb{Z}$ is a prime we always assume that $p\in\mathbb{N}$.

<u>Review Concepts in Algebra.</u>

We say that $(G,\circ)$ is a <u>semigroup</u>, if G is a nonempty set and $\circ$ is a binary operation on G, which is satisfied the associative law: for any $a,b,c,\in G$, $(a\circ b)\circ c = a\circ(b\circ c)$.

A semigroup $(G,\circ)$ is called a commutative semigroup, if $(G,\circ)$ satisfied the commutative law: for any $a,b\in G$, $a\circ b=b\circ a$.

A <u>group</u> $(G,\circ)$ is a semigroup which satisfied the following axioms:

(i). There exists an element e in G such that

$e \circ a = a = a \circ e$, for all $a \in G$. This element e is an <u>identity</u> element for $\circ$ on G.

(ii). For each a in G, there exists an element a^{-1} in G such that $a \circ a^{-1} = e = a^{-1} \circ a$. The element a^{-1} is an <u>inverse</u> of a with respect to $\circ$.

If $(G,+)$ is a group, then we shall call $(+)$ the addition. We denote the identity and the inverse of a by 0 and $-a$ respectively. Similarly, $(G,\cdot)$ is a group, then we shall call $(\cdot)$ the mutiplication and the identity is denoted by 1.

Let S be any nonempty subset of a group$(G,\circ)$. We say that S is a <u>subgroup</u> of $(G,\circ)$, if $(S,\circ)$ is a group. The subgroup of $(G,\circ)$ <u>generated</u> by S, denoted by $\langle S \rangle$, is the smallest subgroup of $(G,\circ)$ which contains S. It can be shown that if S is a nonempty subset of a commutative group $(G,+)$, then $\langle S \rangle$ is the set of all finite sum $\sum_{i=1}^{n} x_i a_i$, where $x_i \in \mathbb{Z}$ and $a_i \in S$. If $S = \{a_1,..,a_n\}$, then we denote $\langle S \rangle$ by $\langle a_1,..,a_n \rangle$. i.e. $\langle a_1,..,a_n \rangle = \{x_1a_1+\cdots+x_na_n \mid x_1,..,x_n \in \mathbb{Z}\}$.

Let $(G,\circ)$ be a group. The subgroup N of G is said to be a <u>normal subgroup</u> of G, if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$. It can be shown that the set

$$G/N = \{gN \mid g \in G\}$$

with the operation $(*)$ defined by

$$(g_1N)*(g_2N) = (g_1 \circ g_2)N \quad (g_1, g_2 \in G)$$

is a commutative group and it is called the <u>factor group</u> of G relative to N.

We say that $(R,+,\cdot)$ is a ring, if R is a nonempty set and $(+),(\cdot)$ are two binary operations on R, which satisfies the following:

(i) $(R,+)$ is a commutative group.

(ii) $(R,\cdot)$ is a semigroup.

(iii) The distributive laws hold: for all $a,b,c\in R$,

$a\cdot(b+c) = a\cdot b+a\cdot c$ and $(b+c)\cdot a = b\cdot a+c\cdot a$.

A ring $(R,+,\cdot)$ is called a ring with identity, if $1\in R$.

A ring $(R,+,\cdot)$ is called a commutative ring, if $(R,\cdot)$ is a commutative semigroup.

In the sequel, the term ring in this thesis will always mean a commutative ring with identity 1.

Let R be a ring and a,b belong to R. Then we say that a divides b (denoted $a|b$) provided that there exists $c\in R$ such that $b=ac$. We call u in R a unit provided that u^{-1} belongs to R. We say that a,b in R are associates (denoted $a\sim b$), if there is a unit u of R such that $a=bu$. We call a in R irreducible if a is a nonzero, nonunit and whenever we have $a=bc$ with b,c in R one of b and c must be a unit in R.

An integral domain D is a ring which has no zero divisors. We say that the factorization of an element a in integral domain D into irreducible factors is unique if whenever

$$a = p_1\cdots p_r \text{ and } a = q_1\cdots q_s,$$

where $p_1,\ldots,p_r,q_1,\ldots,q_s$ are irreducible, then

(i) $r=s$

and (ii) there is a permutation π of $\{1,2,\ldots,r\}$ such that p_i and $q_{\pi(i)}$ are associates for all $i=1,2,\ldots,r$. An integral domain D is said to be a unique factorization domain(U.F.D.), if each nonzero nonunit element of D has a unique factorization into irreducible factors

A ring $(R,+,\cdot)$ is called a field, if $(R-\{0\},\cdot)$ is a commutative group.

Let R be a ring. By an R-module we mean an commutative group M (written additively), together with a function $f:R\times M\to M$, for which we write $f(r,m)=rm$ $(r\in R, m\in M)$, satisfying

(i) $(r+s)m = rm+sm$,

(ii) $r(m+n) = rm+rn$,

(iii) $r(sm) = (rs)m$,

(iv) $1m = m$,

for all $r,s\in R$, $m,n\in M$.

Let S be any nonempty subset of M. It can be shown that $\langle S\rangle$ is a $\mathbb{Z}$-module.

Let $(F,+,\cdot)$ be a field and $(V,+)$ be a commutative group. We say that V is a vector space over F if V is a F-module. The elements of F and V will be referred to as scalars and vectors, respectively. If V is a vector space over F and $\{x_1,..,x_n\}$ is a finite subset of V, then for $a_i\in F$ $1\leq i\leq n$, $\sum_{i=1}^{n} a_i x_i$ is called a linear combination of $\{x_1,..,x_n\}$. The vectors $x_1,..,x_n\in V$ are said to be linearly dependent over F, if there exist scalars $a_1,..,a_n\in F$, not all of them zero such that $\sum_{i=1}^{n} a_i x_i = 0$. An arbitrary set A of vectors is said to be a linearly dependent set, if some finite subset of A is linearly dependent. Otherwise, the set A is called a <u>linearly independent</u>. If $\mathcal{B}$ is a linearly independent subset of V such that for every $v \in V$, v can be written as a linear combination of vectors in $\mathcal{B}$, we say that $\mathcal{B}$ is a <u>basis</u> of V. It can be shown that every vector in V has a unique representation as a linear combination of elements of $\mathcal{B}$ and that every basis of V has the same cardinal number. Let V be a vector space having a basis consisting of n elements. We say that n is the <u>dimension</u> of V. If V consists of 0 alone, then the basis of V is empty so that V has dimension 0.

2.1 The integersof a quadratic field.

The materials in this section are taken from [1]. Theorems will be stated without proofs. Their proofs can be found in [1].

<u>Defintion 2.1.1</u> Let d be any integer. We say that d is a <u>square-free integer</u>, if d is nonzero and is not divisible by a perfect square other then 1.

<u>Remark</u>: if d is a square-free integer, then it can be shown that, the set

$$\left\{ b+c\sqrt{d} \;\middle|\; b,c \in \mathbb{Q} \right\}$$

formsa subfield of $\mathbb{C}$.

<u>Definition 2.1.2.</u> By a <u>quadratic field</u> we mean any subfield of $\mathbb{C}$ of the form $\left\{ b+c\sqrt{d} \;\middle|\; b,c \in \mathbb{Q} \right\}$, where d is a square-free integer. We shall denote this field by $\mathbb{Q}(\sqrt{d})$.

In the sequel, d will always denote a square-free integer. And $d \neq 1$.

<u>Definition 2.1.3.</u> Let $a = b+c\sqrt{d}$ be any element of $\mathbb{Q}(\sqrt{d})$, where $b,c \in \mathbb{Q}$. The element $a' = b-c\sqrt{d}$ is called the <u>conjugate</u> of a.

<u>Theorem 2.1.4. ([1], Proposition 8.2.3.)</u>* Let a, a_1, a_2 be any elements of $\mathbb{Q}(\sqrt{d})$. Then

(i). $(a_1 \pm a_2)' = a_1' \pm a_2'$.

(ii). $(a_1 a_2)' = a_1' a_2'$.

(iii). If $a_2 \neq 0$, then $\left(\frac{a_1}{a_2}\right)' = \frac{a_1'}{a_2'}$.

(iv). $a = a'$ if and only if $a \in \mathbb{Q}$.

<u>Definition 2.1.5.</u> Let $a = b+c\sqrt{d}$ be any element of $\mathbb{Q}(\sqrt{d})$, where $b,c \in \mathbb{Q}$. The <u>trace</u> of a, denoted $T(a)$, is defined as $T(a) = a+a' = 2b$. The <u>norm</u> of a, denoted $N(a)$, is defined as $N(a) = aa' = b^2-c^2d$.

<u>Theorem 2.1.6 ([1], Proposition 8.2.5)</u> Let a, a_1, a_2 be any elements of $\mathbb{Q}(\sqrt{d})$. Then

(i). $T(a_1+a_2) = T(a_1)+T(a_2)$; $N(a_1 a_2) = N(a_1)N(a_2)$.

(ii). $T(a), N(a)$ are rational numbers.

(iii). $N(a) = 0$ if and only if $a = 0$.

(iv). a is a zero of the polynomial $x^2-T(a)x+N(a)$, i.e. a satisfies the equation $x^2-T(a)x+N(a)=0$.

<u>Definition 2.1.7.</u> Let a be any element of $\mathbb{Q}(\sqrt{d})$. We say that a is an <u>integer</u> of $\mathbb{Q}(\sqrt{d})$, provided that $T(a), N(a)$

---

* Here, [1], Proposition 8.2.3. means that this theorem is taken from Proposition 3 of Section 8.2 in [1]. Similar notations will also be used in the sequel.

หอสมุดกลาง สถาบันวิทยบริการ จุฬาลงกรณ์มหาวิทยาลัย

belong to $\mathbb{Z}$. We denote the set of integers of $\mathbb{Q}(\sqrt{d})$ by I_d.

Theorem 2.1.8. ([1], Theorem 8.3.2.) The set of I_d consists of the numbers of the form $x+y\omega_d$, where x and y belong to $\mathbb{Z}$ and

$$\omega_d = \begin{cases} \sqrt{d} & \text{if } d \equiv 2,3 \pmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Remark 2.1.9. From the above theorem, we can see that $I_d = \langle 1, \omega_d \rangle$ and it can be shown that I_d is an integral domain.

Theorem 2.1.10. ([1], Theorem 8.3.4.) The set I_d has the following properties:

(i) All elements $x+y\sqrt{d}$, where $x,y \in \mathbb{Z}$, are in I_d.

(ii) If a is in I_d, then a' is also.

(iii) If a is in I_d and is a rational number, then $a \in \mathbb{Z}$

Remark. In the sequel, we shall simply call any element of I_d an integer. (iii) of Theorem 2.1.10. tells us that an integer is rational if and only if it is in $\mathbb{Z}$. Hence any element of $\mathbb{Z}$ is an integer which is a rational. So any element of $\mathbb{Z}$ will be called a rational integer.

Theorem 2.1.11. ([1], Proposition 8.3.5.) Let $a \in \mathbb{Q}(\sqrt{d})$. Then there is a nonzero rational integer n such that na is in I_d.

Remark 2.1.12. It can be shown that

(i) $\mathbb{Q}(\sqrt{d})$ is a vector space over $\mathbb{Q}$ which has a basis $\{1, \sqrt{d}\}$.

(ii) If $\{a,b\}$ is a basis of $\mathbb{Q}(\sqrt{d})$ and c is a nonzero element of $\mathbb{Q}(\sqrt{d})$, then $\{ac, bc\}$ is a basis of $\mathbb{Q}(\sqrt{d})$.

Definition 2.1.13. Let a,b belong to $\mathbb{Q}(\sqrt{d})$. The determinant

$$\Delta(a,b) = \begin{vmatrix} a & a' \\ b & b' \end{vmatrix}^2 = (ab'-ba')^2$$

is called the discriminant of a,b.

Lemma 2.1.14. ([1], Lemma 8.5.3.) Let a,b belong to $\mathbb{Q}(\sqrt{d})$.

Then

(i) $\Delta(a,b)$ is a rational number.

(ii) If $a,b \in I_d$, then $\Delta(a,b)$ is a rational integer.

(iii) $\{a,b\}$ is a basis of $\mathbb{Q}(\sqrt{d})$ if and only if $\Delta(a,b) \neq 0$.

Remark 2.1.15. It can be shown that if $\{a_1,a_2\}$ and $\{a_3,a_4\}$ are bases of $\mathbb{Q}(\sqrt{d})$ and $\langle a_1,a_2\rangle = \langle a_3,a_4\rangle$, then

(i) there exist $n_1,n_2,n_3,n_4 \in \mathbb{Z}$ such that

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} n_1 & n_2 \\ n_3 & n_4 \end{pmatrix}\begin{pmatrix} a_3 \\ a_4 \end{pmatrix} \text{ and } \det\begin{pmatrix} n_1 & n_2 \\ n_3 & n_4 \end{pmatrix} = \pm 1,$$

(ii) $\Delta(a_1,a_2) = \Delta(a_3,a_4)$.

Theorem 2.1.16 ([1], Lemma 8.7.2.) An element a of I_d is a unit of I_d if and only if $N(a) = \pm 1$.

Theorem 2.1.17 ([1], Lemma 9.1.1.) Let a,b belong to I_d and assume that $a \mid b$, then $N(a) \mid N(b)$.

Theorem 2.1.18. ([1], Lemma 9.1.2.) Let $a \in I_d$ and $|N(a)|=p$, where p is a rational prime. Then a is an irreducible element of I_d.

Theorem 2.1.19. ([1], Theorem 9.1.3.) Let a be a nonzero nonunit element of I_d. Then a can be written in the form $a = b_1 \ldots b_t$, where $b_1,\ldots,b_t$ are irreducible elements of I_d.

2.2. The sp-modules.

Definition 2.2.1. Let A and B be any two nonempty subsets of $\mathbb{Q}(\sqrt{d})$. The product AB of A and B is the set of all sums of the form

$$a_1b_1+a_2b_2+\cdots+a_nb_n,$$

where $a_1,\ldots,a_n$ belong to A and $b_1,\ldots,b_n$ belong to B. In case $A=\{a\}$, we shall also denote AB simply by aB.

Remark 2.2.2. For any subsets A,B,C of $\mathbb{Q}(\sqrt{d})$, it can be shown that

(i). $AB = BA$,

(ii). $(AB)C = A(BC)$,

and (iii). $aB = \{ab \mid b\in B\}$, if $a\in\mathbb{Q}(\sqrt{d})$ and B is closed under addition.

Let a_1,a_2 be any elements of $\mathbb{Q}(\sqrt{d})$. Then the additive subgroup $\langle a_1,a_2\rangle$ is a $\mathbb{Z}$-module. We shall give a special name to such a $\mathbb{Z}$-module in which $\{a_1,a_2\}$ forms a basis of $\mathbb{Q}(\sqrt{d})$.

Definition 2.2.3. Let M be any subset of $\mathbb{Q}(\sqrt{d})$. M is called an sp-module, if there exists a basis $\{a_1,a_2\}$ of $\mathbb{Q}(\sqrt{d})$ such that $M = \langle a_1,a_2\rangle$.

Theorem 2.2.4. ([1] ,Theorem 8.5.6.) Let M be a subset of $\mathbb{Q}(\sqrt{d})$. Then M is an sp-module if and only if the following three conditions hold:

(i). M is a $\mathbb{Z}$-module.

(ii). M contains a basis of $\mathbb{Q}(\sqrt{d})$.

(iii). there is a nonzero rational integer k such that $kM\subseteq I_d$.

Remark 2.2.5. I_d is an sp—module. This follows from the fact that $I_d = \{x+y\omega_d \mid x,y\in\mathbb{Z}\}$, where ω_d is as defined in Theorem 2.1.8. and $\{1,\omega_d\}$ is a basis of $\mathbb{Q}(\sqrt{d})$.

Definition 2.2.6. For any nonzero element γ in $\mathbb{Q}(\sqrt{d})$, γI_d is called a principal module and $\gamma I_d = \langle\gamma, \gamma\omega_d\rangle$. γ is called a generator.

Remark 2.2.7. It can be shown that the following hold:

(i). Every principal module is an sp-module.

(ii). If aI_d and bI_d are principal modules, then

$$(aI_d)(bI_d) = (ab)I_d.$$

Definition 2.2.8. The discriminant Δ_M of the sp-module $M = \langle a,b\rangle$ is defined to be the nonzero rational number $\Delta(a,b)$. The discriminant Δ_M is well defined by Remark 2.1.15(ii). We shall denote Δ_{I_d} by Δ_d. We can verify that

$$\Delta_d = \begin{cases} d & \text{if } d \equiv 1 (\mathrm{mod} 4), \\ 4d & \text{if } d \equiv 2,3 \ (\mathrm{mod} 4). \end{cases}$$ So $\Delta_d \equiv 0$ or 1 (mod4).

Theorem 2.2.9. ([1], Proposition 9.3.3.) Let $M_1 = \langle a_1, b_1\rangle$ and $M_2 = \langle a_2, b_2\rangle$ be sp-modules in $\mathbb{Q}(\sqrt{d})$. Then M_1M_2 is the set of all numbers of $\mathbb{Q}(\sqrt{d})$ of the form

$$xa_1a_2+ya_1b_2+za_2b_1+wb_1b_2,$$

where x,y,z,w are rational integers.

Theorem 2.2.10. The set of all sp—modules is a commutative semigroup under the multiplication.

Proof. Since every sp-module is a subset of $\mathbb{Q}(\sqrt{d})$, it follows from Remark 2.2.2. that commutative and associative laws hold. So we need to show that the multiplication is closed. Let $M_1 = \langle a_1, b_1\rangle$ and $M_2 = \langle a_2, b_2\rangle$ be any sp-modules.

By Theorem 2.2.9 we get

$$M_1M_2 = \left\{ xa_1a_2+ya_1b_2+za_2b_1+wb_1b_2 \,\middle|\, x,y,z,w \in \mathbb{Z} \right\}. \quad \ldots(1)$$

Since $\{a_1, b_1\}$ is a basis of $\mathbb{Q}(\sqrt{d})$ and $a_2 \neq 0$, it follows from Remark 2.1.12(ii) that $\{a_1a_2, b_1a_2\}$ is a basis of $\mathbb{Q}(\sqrt{d})$. From (1) we see that M_1M_2 contains a basis of $\mathbb{Q}(\sqrt{d})$. It is clear that, the sum and difference of two elements of M_1M_2 belong to M_1M_2. So we can conclude that M_1M_2 is a $\mathbb{Z}$-module. By Theorem 2.1.11. there is a nonzero rational integer n such that na_1, na_2, nb_1, nb_2 belong to I_d. From (1) we see that $n^2M_1M_2 \subseteq I_d$. Therefore, M_1M_2 is an sp-module. Hence, the set of all sp-modules is a commutative semigroup.

#

<u>Definition 2.2.11</u>. Let M_1 and M_2 be any sp-modules. We say that M_1 and M_2 are <u>similar</u>, if there is an element α in $\mathbb{Q}(\sqrt{d})$ such that $M_1 = \alpha M_2$. When M_1 and M_2 are similar, we write $M_1 \sim M_2$.

<u>Theorem 2.2.12. ([1] , Proposition 9.6.2.)</u> Similarity of sp-modules is an equivalence relation.

We shall denote the equivalence class containing M by $[M]$.

<u>2.3 The spg-modules.</u>

<u>Definition 2.3.1</u>. Let M be any sp-module. The set of elements a in $\mathbb{Q}(\sqrt{d})$ having the property $aM \subseteq M$ is called <u>the ring of coefficients (or coefficient ring)</u> of M and will be denoted by $\mathcal{O}_M$

Observe that any coefficient ring is always a ring.

Theorem 2.3.2. ([1], Lemma 8.6.9.) Let M be an sp-module. Then $\mathcal{O}_M \subseteq I_d$.

Theorem 2.3.3. ([1], Theorem 8.6.10) Let M be any sp-module. There is a positive rational integer f such that $\mathcal{O}_M = \langle 1, f\omega_d\rangle$. The rational integer f is characterized as the least positive rational integer such that $f\omega_d$ is in $\mathcal{O}_M$.

Remark 2.3.4. The element f in Theorem 2.3.3. will be called the conductor of $\mathcal{O}_M$. It is clear from Definition 2.2.3. that $\mathcal{O}_M$ is an sp-module.

Definition 2.3.5. Let M be any sp-module. The number

$$N(M) = \sqrt{\frac{\Delta_M}{\Delta_{\mathcal{O}_M}}}$$

is called the norm of M.

Definition 2.3.6. Let $\mathcal{O}$ be a ring of coefficients, and M an sp-module. If M has $\mathcal{O}$ as its ring of coefficient, then we say that M belongs to $\mathcal{O}$. If $M \subseteq \mathcal{O}$ and M belongs to $\mathcal{O}$, then we say that M is an integral module (for $\mathcal{O}$). That is, M is an integral module if and only if $M \subseteq \mathcal{O}_M$.

Definition 2.3.7. Let M be an integral module belonging to $\mathcal{O}$. We say that M is a prime module if and only if, whenever $M = M_1M_2$, with M_1 and M_2 integral modules belonging to $\mathcal{O}$, we have either $M_1 = \mathcal{O}$ or $M_2 = \mathcal{O}$.

Definition 2.3.8. Let M be an sp-module. M is called an spg-module*, if $\mathcal{O}_M = I_d$.

In our work we need to consider only the spg-modules. So that definitions and theorems stated in this study are special cases of those in [1]. To obtain our result from the general results in [1] we use the fact that when $\mathcal{O}_M = I_d$, 1 is the conductor of I_d.

Using the fact " $M \subseteq MI_d$ " and the definition of spg-module. We have the following theorem.

Theorem 2.3.9. Let M be any sp-module. Then

M is an spg-module if and only if $MI_d = M$.

Remark 2.3.10. It can be shown that the following hold:

(i). Every principal module is an spg-module

(ii). Let M_1 and M_2 be any sp-modules such that $M_1 \sim M_2$. If M_1 is an spg-module, then M_2 is also.

(iii). If M_1 and M_2 are spg-modules, then M_1M_2 is also.

In the sequel, we shall need to compute the rings of coefficients of sp-modules of the form $M = \langle 1, \gamma \rangle$. The following theorem tells us how to compute them.

Theorem 2.3.11. ([1] , Lemma 8.6.13.) Let $M = \langle 1, \gamma \rangle$ be any sp-module. Then $\mathcal{O}_M = \langle 1, a\gamma \rangle$, where γ satisfies the equation $a\gamma^2 - b\gamma + c = 0$ with a,b,c being rational integers; $a > 0$ and a,b,c have no common factor>1.

---

* It can be shown that the concept of spg-module is the same as that of fractional ideals. See Theorem B in Appendix I.

Example 2.3.12. We shall show that $M = \langle 5, 2+\omega_{-6}\rangle$ is an spg-module in $\mathbb{Q}(\sqrt{-6})$. Clearly, M isan sp-module in $\mathbb{Q}(\sqrt{-6})$. Let $M_1 = \langle 1, \gamma\rangle$, where $\gamma = \frac{2}{5}+\frac{\omega_{-6}}{5}$. So $M = 5M_1$. We can check that γ satisfies the equation $5\gamma^2-4\gamma+2 = 0$. By Theorem 2.3.11.

$$\mathcal{O}_{M_1} = \langle 1, 5\gamma\rangle = \langle 1, 2+\omega_{-6}\rangle = I_{-6}.$$

Therefore, M_1 is an spg-module. By Remark 2.3.10(ii) M is an spg-module

Similary, we can show that $\langle 11, 4+\omega_{-6}\rangle$ is an spg-module in $\mathbb{Q}(\sqrt{-6})$ and $\langle 2, \omega_{-31}\rangle$, $\langle 5, 3+\omega_{-31}\rangle$ are spg-modules in $\mathbb{Q}(\sqrt{-31})$.

#

A concept which is important in the study of sp-modules is that of the norm of a sp-module. However, we need to consider only the case of spg-module. For this special case we have the following:

Remark 2.3.13. Let M be any spg-module. Then the norm of M is

$$N(M) = \sqrt{\frac{\Delta_M}{\Delta_d}}.$$

Remark 2.3.14. Let a be any nonzero element of $\mathbb{Q}(\sqrt{d})$. Then aI_d is an spg-module and

$$\Delta_{aI_d} = \begin{vmatrix} a & a' \\ a\omega_d & a'\omega_d' \end{vmatrix}^2 = (aa'\omega_d' - a'a\omega_d)^2 = (aa')^2(\omega_d'-\omega_d)^2.$$

Since $\Delta_d = \begin{vmatrix} 1 & 1 \\ \omega_d & \omega_d' \end{vmatrix}^2 = (\omega_d'-\omega_d)^2$, it follows that

$$N(aI_d) = \sqrt{\frac{(aa')^2(\omega_d'-\omega_d)^2}{(\omega_d'-\omega_d)^2}} = |N(a)|.$$

011327

i 17663416

Definition 2.3.15. Let M be any nonempty subset of $\mathbb{Q}(\sqrt{d})$. Define

$$M' = \{c' \mid c \in M\}.$$

M' will be called the conjugate of M.

Remark 2.3.16. It can be shown that conjugation has the following properties.

(i). If S is a nonempty subset of $\mathbb{Q}(\sqrt{d})$. Then

$$\langle S\rangle' = \langle S'\rangle.$$

(ii). If A,B are nonempty subsets of $\mathbb{Q}(\sqrt{d})$. Then

$$(AB)' = A'B'.$$

(iii). If M is an spg-module, then

M' is an spg-module and $N(M) = N(M')$.

(iv). If M_1 and M_2 are sp-modules, then

$M_1 \sim M_2$ if and only if $M_1' \sim M_2'$.

Theorem 2.3.17. ([1] , Theorem 9.3.8.) Let M be an spg-module. Then $MM' = N(M)I_d$.

Theorem 2.3.18. ([1] , Corollary 9.3.12.) Let M_1 and M_2 be spg-modules. Then $N(M_1M_2) = N(M_1)N(M_2)$.

Theorem 2.3.19. The set of all spg-modules is a commutative group under the multiplication.

Proof. Let $\mathcal{M}$ be the set of all spg-modules. Since $\mathcal{M}$ is a subset of the set of all sp-modules, it follows from Theorem 2.2.10. and Remark 2.3.10(iii). that $\mathcal{M}$ is a commutative semigroup. From Theorem 2.3.9. we see that I_d is an identity. Let $M \in \mathcal{M}$. Then $M' \in \mathcal{M}$. Since $M' \sim \frac{M'}{N(M)}$, it follows from Remark 2.3.10(ii) that $\frac{M'}{N(M)} \in \mathcal{M}$. By Theorem 2.3.17, $MM' = N(M)I_d$. So $M(\frac{M'}{N(M)}) = I_d$. Therefore, $\frac{M'}{N(M)}$ is

an inverse of M. Hence, $\mathcal{M}$ is a commutative group.
#

Theorem 2.3.20. The set of all principal modules is a normal subgroup of the group of all spg-modules.

Proof. Let $\mathcal{P}$ be the set of all principal modules and $\mathcal{M}$ be the group of all spg-modules. By Remark 2.3.10(i) and Remark 2.2.7(ii) that, $\mathcal{P} \subseteq \mathcal{M}$ and $\mathcal{P}$ is closed. Let $M \in \mathcal{P}$. Then $M = aI_d$ for some nonzero element $a \in \mathbb{Q}(\sqrt{d})$. So $(aI_d)(a^{-1}I_d) = (aa^{-1})I_d = I_d$. Therefore, $a^{-1}I_d$ is an inverse of aI_d. Hence, $\mathcal{P}$ is a subgroup of $\mathcal{M}$. Since $\mathcal{M}$ is commutative, it follows that $\mathcal{P}$ is a normal subgroup.
#

Definition 2.3.21. Let $\mathcal{M}$ be the set of all spg-modules and $\mathcal{P}$ be the set of all principal modules. Then $(\mathcal{M}/\mathcal{P}, *)$ is a factor group of $\mathcal{M}$ relative to $\mathcal{P}$. $\mathcal{M}/\mathcal{P}$ is denoted by $\mathcal{J}_d$ and is called the class group of I_d. The number of elements of $\mathcal{J}_d$ is called the class number of I_d which denoted by h_d.

Remark 2.3.22. Let $M \in \mathcal{M}$. It can be verified that $M\mathcal{P} = [M]$, $\mathcal{P} = [I_d]$ and $[M'] = [M]^{-1}$.

2.4 Integral modules and Prime modules.

In this section we review the concepts of integral modules and prime modules for the case of spg-modules. We provide known results on factorization of integral modules into prime modules.

Remark 2.4.1. Let M be any spg-module. Then M is an integral module* if and only if $M \subseteq I_d$.

Remark 2.4.2. The following observations will be useful in the sequel.

(i). An integral module M contains a unit of I_d if and only if $M = I_d$.

(ii). $M_1 M_2$ is an integral module, if M_1 and M_2 are integral modules.

(iii). aI_d is an integral module if and only if a belongs to I_d.

Proof. (ii) and (iii) are clear. We shall show (i). Let M be any integral module. So $M \subseteq I_d$. Suppose that M contains a unit of I_d. Then M contains 1. Since $MI_d \subseteq M$, then $I_d \subseteq M$. therefore, $M = I_d$.
The converse is obvious. #

Remark 2.4.3. Let M be any integral module, $M \neq I_d$. Then M is prime if and only if, whenever $M = M_1 M_2$, with M_1 and M being integral modules, we have either $M_1 = I_d$ or $M_2 = I_d$.

Remark 2.4.4. If M is a prime module, then M' is also.

Theorem 2.4.5.([1] , Theorem 9.4.2.) If the norm of any integral module is a rational prime, then it must be a prime module.

---

* It can be shown that the concept of integral module is the same as that of ideal. See Theorem A in Appendix I.

Note that the converse of this theorem is not true. A counter example can be found in Example 2.4.19. Later on we shall give a necessary condition for an integral module to be prime (see Theorem 2.4.13.).

Definition 2.4.6. Let A,B be integral modules. Then we say that A divides B, written $A|B$, if there is an integral module C such that AC =B.

Remark 2.4.7. Let A and B be any integral module such that $A|B$. Then we can show that $N(A)|N(B)$.

Theorem 2.4.8. ([1], Theorem 9.4.6.) Let A and B be integral modules. Then $A|B$ if and only if $B \subseteq A$.

Theorem 2.4.9 ([1], Corollary 9.4.10.) Let P,A,B be any integral modules. If P is prime and $P|AB$, then $P|A$ or $P|B$.

Corollary 2.4.10. Let $A_1,\ldots,A_n$ be any integral modules and P be a prime module such that $P|A_1\ldots.A_n$. Then $P|A_i$, for some i, $1\leq i\leq n$.

Theorem 2.4.11. ([1], Theorem 9.4.4.) Let $M(\neq I_d)$ be an integral module. Then M can be written in the form

$$M = P_1 \ldots . P_t,$$

where $P_1,\ldots,P_t$ are prime modules. Moreover, this repersentation is unique up to the order of $P_1,\ldots,P_t$.

Theorem 2.4.12. ([1], Proposition 9.5.1.) Let P be any prime module and a,b belong to I_d. If $ab \in P$, then $a \in P$ or $b \in P$.

Remark 2.4.13. Let P be a prime module. It can be shown that $N(P) = p$ or p^2, for some rational prime p.

Theorem 2.4.14. ([1], Theorem 9.5.2.) Let P be a prime module. Then there is a rational prime p such that $P \mid pI_d$. Conversely, if p is a rational prime, then there are three possibilities:

(i). $pI_d = P$ is a prime module and $N(P) = p^2$.

(ii). $pI_d = P^2$, where P is a prime module such that $P = P'$ and $N(P) = p$.

(iii). $pI_d = PP'$, where P and P' are distinct prime modules and $N(P) = N(P') = p$.

Definition 2.4.15. Let p be any rational prime. Then

(i). p is inert, if $pI_d = P$, where P is a prime module and $N(P) = p^2$.

(ii). p is decomposed, if $pI_d = PP'$, where P and P' are distinct prime modules and $N(P) = N(P') = p$.

(iii). p is ramified, if $pI_d = P^2$, where P is a prime module such that $P = P'$ and $N(P) = p$.

According to the above theorem(Theorem 2.4.14.), we see that any rational prime p must be either inert, decomposed or ramified. The following theorem will be useful in deciding whether a rational prime p is inert, decomposed or ramified. This theorem also gives us the prime factorization of pI_d.

Theorem 2.4.16. ([1] , Theorem 9.5.3.) Let p be a rational prime.

(i). Assume that $p \nmid \Delta_d$. Then p is decomposed if and only if the congruence $x^2 \equiv \Delta_d \pmod{4p}$ is solvable.

Otherwise, p is inert. In the case p is decomposed, say $pI_d = PP'$, then

$$P = \left\langle p,\ a - \frac{\Delta_d + \sqrt{\Delta_d}}{2} \right\rangle,$$

where a is a rational integer such that $x = 2a - \Delta_d$ is a solution of $x^2 \equiv \Delta_d \pmod{4p}$.

(ii). Assume that $p \mid \Delta_d$. Then p is ramified, $pI_d = P^2$ and

$$P = \begin{cases} \left\langle p,\ \dfrac{\Delta_d + \sqrt{\Delta_d}}{2} \right\rangle & \text{if } p \text{ is odd} \\ \left\langle 2, \sqrt{\dfrac{\Delta_d}{4}} \right\rangle & \text{if } p=2, d \equiv 2 \pmod 4 \\ \left\langle 2,\ 1+\sqrt{\dfrac{\Delta_d}{4}} \right\rangle & \text{if } p=2, d \equiv 3 \pmod 4). \end{cases}$$

<u>Theorem 2.4.17.</u> Let p be a rational prime.

(i). If $p \mid \Delta_d$, then p is ramified, i.e. we have

$$pI_d = P^2,$$

where P is the prime module given by

$$P = \begin{cases} \left\langle p,\ \dfrac{\Delta_d + \sqrt{\Delta_d}}{2} \right\rangle & \text{if } p \text{ is odd} \\ \left\langle 2, \sqrt{\dfrac{\Delta_d}{4}} \right\rangle & \text{if } p=2, d \equiv 2 \pmod 4 \\ \left\langle 2,\ 1+\sqrt{\dfrac{\Delta_d}{4}} \right\rangle & \text{if } p=2, d \equiv 3 \pmod 4 \end{cases}$$

(ii). If $p \nmid \Delta_d$, then p is either decomposed or inert. p is decomposed if and only if the congruence

$$x^2 \equiv \Delta_d \pmod{4p}$$

is solvable, and in this case P in the factorization

$$pI_d = PP',$$

is given by

$$P = \left\langle p, \frac{x - \sqrt{\Delta_d}}{2} \right\rangle,$$

หอสมุดกลาง สถาบันวิทยบริการ จุฬาลงกรณ์มหาวิทยาลัย

where x is a solution of $x^2 \equiv \Delta_d \pmod{4p}$.

Theorem 2.4.17 is just a restatement of Theorem 2.4.16. The following examples will illustrate how the above theorem can be applied. In fact the results of these examples will be needed later on.

Example 2.4.18. We shall factor $5I_{-6}$ in to a product of prime modules in $\mathbb{Q}(\sqrt{-6})$. Since $-6 \equiv 2 \pmod 4$, it follows from Remark 2.2.8, that $\Delta_{-6}=-24$. Since $5 \nmid -24$, hence, by Theorem 2.4.17(ii), 5 is decomposed or inert. Observe 4 is a solution of $x^2 \equiv -24 \pmod{20}$ (see Example 11 in Appendix II) Hence, 5 is decomposed and $5I_{-6}=PP'$, where

$P = \left\langle 5, \frac{4+\sqrt{-24}}{2}\right\rangle$. Thus, $P = \langle 5,2+\sqrt{-6}\rangle$ and $P' = \langle 5,3+\sqrt{-6}\rangle$.

Therefore $$5I_{-6} = \langle 5,2+\sqrt{-6}\rangle \langle 5,3+\sqrt{-6}\rangle .$$ #

Example 2.4.19. We shall factor $3I_{-31}$ in to a product of prime modules in $\mathbb{Q}(\sqrt{-31})$. Since $-31 \equiv 1 \pmod 4$, it follows from Remark 2.2.8, that $\Delta_{-31}=-31$. Since $3 \nmid -31$, hence by Theorem 2.4.17(ii). 3 is decomposed or inert. It can be shown that $x^2 \equiv -31 \pmod{12}$ has no solution (see Example 10 in Appendix II). Hence, 3 is inert. Therefore,

$$3I_{-31} \text{ is a prime module.}$$ #

Note that, $N(3I_{-31}) = 9$. This example is a counter-example of prime module which has the norm is not rational prime.

Example 2.4.20. We shall factor $2I_{-5}$ in to a product of prime modules in $\mathbb{Q}(\sqrt{-5})$. Since $-5 \equiv 3 \pmod 4$, it follows from Remark 2.8.8. that $\Delta_{-5} = -20$. Since $2 \mid -20$, hence by Theorem 2.4.17(i) 2 is ramified. Therefore, $2I_{-5} = P^2$, where P is a prime module given by $P = \langle 2, 1+\sqrt{-5} \rangle$. Hence,

$$2I_{-5} = \langle 2, 1+\sqrt{-5} \rangle^2. \qquad \#$$

2.5 The computation method of the product of integral modules.

In this section we provide a computation method to determine a product of integral modules. They will be followed by examples. This computation method willbe based on Theorem 2.5.7. and Theorem 2.5.8.

Lemma 2.5.1. ([1] , Lemma 9.2.3.) Let M be an sp-module and c be any element of $\mathbb{Q}(\sqrt{d})$. Then there exists a positive rational integer k such that $kc \in M$.

Remark 2.5.2. It follows from this lemma that every sp-module contain a positive rational integer. This can be seen by taking $c = 1$.

Theorem 2.5.3. ([1] , Corollary 9.2.5.) Let M be an integral module. Let $a > 0$ be the least rational integer in M and let $b+c\omega_d$ be an element of M for which $c > 0$ is as small as possible. Then $M = \langle a, b+c\omega_d \rangle$. Furthermore, we may assume that $0 \leqslant b < a$.

Theorem 2.5.4. Let $M = \langle a, b+c\omega_d \rangle$ be an integral module, where $a,b,c \in \mathbb{Z}$. Then $N(M) = |ac|$.

Proof. Let $M = \langle a, b+c\omega_d \rangle$ be an integral module, where $a,b,c \in \mathbb{Z}$. Then

$$\Delta_M = \begin{vmatrix} a & a \\ b+c\omega_d & b+c\omega_d' \end{vmatrix}^2 = (ac)^2(\omega_d' - \omega_d)^2.$$

Since $\Delta_d = (\omega_d' - \omega_d)^2$, it follows that $N(M) = \sqrt{\frac{\Delta_M}{\Delta_d}} = |ac|$. #

Remark 2.5.5. From Theorem 2.5.3. and Theorem 2.5.4. we see that the norm of any integral module is a positive rational integer.

Corollary 2.5.6. Let M be any integral module. Then

$$N(M) = 1 \text{ if and only if } M = I_d.$$

Proof. Let M be any integral module.
First, we assume that $N(M) = 1$. By Theorem 2.5.3. $M = \langle a, b+c\omega_d \rangle$, where a is the smallest positive rational integer in M, c is the smallest positive rational integer such that $b+c\omega_d$ is in M and $0 \leqslant b < a$. By Theorem 2.5.4. $N(M) = |ac|$. So $|ac| = 1$. Since a and c are positive rational integer, we can conclude that $a=c=1$ and $b=0$. Thus, $M=I_d$.
Conversely, if $M = I_d$, then $\Delta_M = \Delta_d$. So $N(M) = \sqrt{\frac{\Delta_M}{\Delta_d}} = 1$. #

The following theorems will be useful in finding product of any two integral modules.

Theorem 2.5.7. Assume that $d \equiv 1 \pmod 4$ Let $M_1 = \langle a_1, b_1+c_1\omega_d \rangle$ and $M_2 = \langle a_2, b_2+c_2\omega_d \rangle$ be any integral modules. Let

$$c = g.c.d.(a_1c_2,\ a_2c_1,\ b_1c_2+b_2c_1+c_1c_2),$$

$$a = \frac{N(M_1)N(M_2)}{c}$$

Let x,y,z be any rational integers such that

$$xa_1c_2+ya_2c_1+z(b_1c_2+b_2c_1+c_1c_2) = c$$

Then

$$M_1M_2 = \langle a, b+c\omega_d \rangle,$$

where $b = xa_1b_2+ya_2b_1+z(b_1b_2+c_1c_2(\frac{d-1}{4}))$.

Proof. From Theorem2.2.9, any element α in M_1M_2 can be written in the form

$$\alpha = ra_1a_2+sa_1(b_2+c_2\omega_d)+ta_2(b_1+c_1\omega_d)+u(b_1+c_1\omega_d)(b_2+c_2\omega_d)$$

$$= ra_1a_2+ sa_1b_2+ ta_2b_1+ u(b_1b_2+ c_1c_2\omega_d^2)$$

$$+ (sa_1c_2+ ta_2c_1+ u(b_1c_2+ c_1b_2))\omega_d,$$

where $r,s,t,u\in\mathbb{Z}$. From Theorem 2.1.8. we have $\omega_d = \frac{1+\sqrt{d}}{2}$, so that $\omega_d^2 = \frac{d-1}{4}+\omega_d$. Therefore,

$$\alpha = ra_1a_2+ sa_1b_2 + ta_2b_1 + u(b_1b_2+ c_1c_2(\frac{d-1}{4}))$$

$$+ (sa_1c_2 + ta_2c_1 + u(b_1c_2 + c_1b_2+ c_1c_2))\omega_d, \ldots (I)$$

where $r, s,t,u\in\mathbb{Z}$. Since $c = g.c.d.(a_1c_2,a_2c_1,b_1c_2+c_1b_2+c_1c_2)$, then c is the smallest positive rational integer of the form $la_1c_2+ma_2c_1+n(b_1c_2+c_1b_2+c_1c_2)$, where $l,m,n\in\mathbb{Z}$. Let $b = xa_1b_2+ya_2b_1+z(b_1b_2+c_1c_2(\frac{d-1}{4}))$. From (I) we can see that $b+c\omega_d$ is in M_1M_2. By Remark 2.5.2. we can choose the smallest positive rational integer k such that $k\in M_1M_2$. By Theorem 2.5.3. we have $M_1M_2 = \langle k,b+c\omega_d\rangle$ and by Theorem 2.5.4. we have $N(M_1M_2) = |kc| = kc$. Thus,

$$k = \frac{N(M_1M_2)}{c} = \frac{N(M_1)N(M_2)}{c} = a.$$

Therefore, $M = \langle a,b+c\omega_d\rangle$.

#

Theorem 2.5.8. Assume that $d\equiv 2,3 \pmod 4$.
Let $M_1 = \langle a_1,b_1+c_1\omega_d\rangle$ and $M_2= \langle a_2,b_2+c_2\omega_d\rangle$ be any integral modules. Let

$$c = g.c.d.(a_1c_2,a_2c_1,b_1c_2+b_2c_1),$$

$$a = \frac{N(M_1)N(M_2)}{c}.$$

Let x,y,z be any rational integers such that

$$xa_1c_2+ya_2c_1+z(b_1c_2+b_2c_1) = c$$

Then

$$M_1M_2 = \langle a, b+c\omega_d\rangle ,$$

where

$$b = xa_1b_2+ya_2b_1+z(b_1b_2+c_1c_2d).$$

The proof of Theorem 2.5.8. is similar to that of Theorem 2.5.7. So it will be omitted.

The following will illustrate the method above. Note that from Example 2.3.12. we have seen that $\langle 2,\omega_{-31}\rangle$ $\langle 5,3+\omega_{-31}\rangle$ and $\langle 5,2+\omega_{-6}\rangle$, $\langle 11,4+\omega_{-6}\rangle$ are spg-modules in $Q(\sqrt{-31})$ and $Q(\sqrt{-6})$ respectively. It is clear that they are integral modules. Weshall demonstrate how to obtain the product of these pairs of them.

<u>Example 2.5.9.</u> Let $M_1 = \langle 2,\omega_{-31}\rangle$ and $M_2 = \langle 5,3+\omega_{-31}\rangle$ be integral modules. We shall find the product $M = M_1M_2$ and represent it in form

$$M = \langle a, b+c\omega_{-31}\rangle .$$

Since $-31\equiv 1 \pmod 4$, hence by Theorem 2.5.7. we see that

$$c = \text{g.c.d.}(2,5,4) = 1.$$

By Theorem 2.5.4. we can see that $N(M_1) = 2$ and $N(M_2) = 5$.

Therefore

$$a = \frac{N(M_1)N(M_2)}{1} = 10$$

A solution of $2x+5y+4z = 1$ is $x=-2$, $y = 1$, $z = 0$. So $b=-12$.

Therefore, $M = \langle 10,-12+\omega_{-31}\rangle = \langle 10,-2+\omega_{-31}\rangle$

#

Example 2.5.10. Let $M_1 = \langle 5, 2+\omega_{-6} \rangle$ and $M_2 = \langle 11, 4+\omega_{-6} \rangle$ be integral modules. We shall find the product $M = M_1 M_2$ and represent it in the form

$$M = \langle a, b+c\,\omega_{-6} \rangle .$$

Since $-6 \equiv 2 \pmod 4$, hence by Theorem 2.5.8. we see that

$$c = \text{g.c.d.}(5,11,6) = 1.$$

By Theorem 2.5.4. we can see that $N(M_1) = 5$ and $N(M_2) = 11$.

Therefore,

$$a = \frac{N(M_1)N(M_2)}{1} = 55.$$

A solution of $5x+11y+6z = 1$ is $x = -2$, $y = 1$, $z = 0$. So $b = -22$. Therefore, $M = \langle 55, -22+\omega_{-6} \rangle = \langle 55, 37+\omega_{-6} \rangle$

#