CHAPER III

COMPUTATION METHOD

OF FACTORIZATION OF RATIONAL INTEGERSIN $Q(\sqrt{d})$

This chapter concern with factorization of elements of $\mathbb{Z}$ in to irreducible factors in all possible ways.

We shall consider the following theorem.

Theorem 3.1. Let a,b belong to I_d. Then

$$aI_d = bI_d \text{ if and only if } a \sim b.$$

Proof. Let a,b be any elements of I_d. If a or b is a zero element in I_d, then the theorem is true. So we assume that a and b are nonzero elements in I_d.

First, we suppose that $aI_d = bI_d$. Since $1 \in I_d$, it follows that $a \in bI_d$ and $b \in aI_d$. Then $a = bc_1$ and $b = ac_2$ for some $c_1, c_2 \in I_d$. Thus, $a = ac_1c_2$. Therefore $c_1c_2 = 1$. So c_1 is a unit of I_d. Hence, $a \sim b$.

To prove the converse, we suppose that $a \sim b$. Then $a = bu$ for some a unit u of I_d. Let $x \in aI_d$. So $x = ac_1$ for some $c_1 \in I_d$. Then $x = buc_1$. Since $uc_1 \in I_d$, it follows that $x \in bI_d$ Therefore, $aI_d \subseteq bI_d$. By the same argrument we have $bI_d \subseteq aI_d$. Hence, $aI_d = bI_d$. #

Using the fact that a is a unit of I_d if and only if $a \sim 1$. We have a corollary.

Corollary 3.2. Let a be any element of I_d. Then

$$aI_d = I_d \text{ if and only if } a \text{ is a unit of } I_d.$$

We base our method on the following remark, which follows immediatly from theorem.

<u>Remark 3.3.</u> Let $a, a_1, a_2, \ldots, a_n$ belong to I_d. If

$$aI_d = (a_1I_d)(a_2I_d)\ldots.(a_nI_d), \ldots\ldots.(I)$$

then $a = ua_1a_2\ldots.a_n$, where u is a unit of I_d.

We make use of this result as follows.

Let a be a nonzero nonunit of I_d. To find all the factorizations of a into irreducible factors, it suffices to find all factorizations of aI_d into the form (I) in which a_i is irreducible in I_d.

We can obtain all factorizations(I) with each a_i being irreducible by using the fact that each integral module, which is not I_d, can be factored into prime modules in a unique way. So we can write

$$aI_d = P_1\ldots.P_r, \qquad \ldots\ldots\ldots\ldots\ldots\ldots(II)$$

where each P_i is prime.

Note that where each factor a_iI_d on the right hand side of (I) is factored into prime modules, we must get the factorization (II). Hence each a_iI_d is a product of a combination of $P_j^{\prime}s$ on the right hand side of (II). Therefore any factorization of aI_d of the form (I) can be obtained by grouping the $P_j^{\prime s}$ in the factorization (II) in a suitable way. So we can find all factorizationsof the form (I) by inspecting all possible groupings of the $P_j^{\prime}s$ in (II).

The following results will be useful in deciding whether a module is of the form a_iI_d where a_i isirreducible in I_d.

Theorem 3.4. Let $M_1, M_2, \ldots, M_n, P_1, P_2, \ldots, P_n$ be integral modules such that

(i) each $M_i \neq I_d$,

(ii) each P_i is prime

If $P_1 \ldots P_n = M_1 \ldots M_n$, then there exists a permutation i_1, $i_2, \ldots, i_n$ of $1, 2, \ldots, n$ such that $P_j = M_{i_j}$ for $j = 1, \ldots, n$.

Proof. Suppose that $P_1 \ldots P_n = M_1 \ldots M_n$. for each $1 \leqslant i \leqslant n$, $M_i \neq I_d$. By Theorem 2.4.11.

$$M_i = M_1^i \ldots M_{r_i}^i,$$

where $M_1^i, \ldots, M_{r_i}^i$ are prime modules. So

$$P_1 \ldots P_n = M_1^1 \ldots M_{r_1}^1 M_1^2 \ldots \ldots M_{r_n}^n.$$

By Theorem 2.4.11. we have $n = r_1 + \cdots + r_n$, which implies that each $r_i = 1$. Therefore, each M_i is a prime module. Then $M_1 \ldots M_n$ is a prime factorization of $P_1 \ldots P_n$. Hence, there exists a permutation $i_1, \ldots, i_n$ of $1, \ldots, n$ such that $P_j = M_{i_j}$ for $j = 1, 2, \ldots, n$.

#

Theorem 3.5. Let $a \in \mathbb{Q}(\sqrt{d})$. If aI_d can be written in the form

$$aI_d = M_1 \ldots M_n,$$

where $M_1, \ldots, M_n$ are prime modules such that $\prod_{i \in I} M_i$ is not principal for any nonempty proper subset I of $\{1, 2, \ldots, n\}$. Then a is irreducible in I_d

Proof. Assume that $aI_d = M_1 \ldots M_n$, where $M_1, \ldots, M_n$ are prime modules such that $\prod_{i \in I} M_i$ is not principal for any nonempty proper subset I of $\{1,2,\ldots,n\}$. Hence aI_d is a principal module, so that $a \neq 0$. Since $M_1,\ldots,M_n$ are integral modules, then aI_d is an integral module. i.e. $aI_d \subseteq I_d$. So $a \in I_d$. Since $N(aI_d) = N(M_1)\ldots.N(M_n) \neq 1$, hence by Theorem 2.5.6. $aI_d \neq I_d$. Therefore, by Corollary 3.2. a is a nonunit of I_d.

Suppose that $a = bc$, where b,c are nonunits of I_d. So $bI_d \neq I_d$ and $cI_d \neq I_d$. Then by Theorem 2.4.11, we get that

$$bI_d = P_1\ldots.P_r$$

and

$$cI_d = Q_1\ldots.Q_s,$$

where $P_1,\ldots,P_r,Q_1,\ldots,Q_s$ are prime modules. Since $aI_d = (bI_d)(cI_d)$, so

$$M_1\ldots.M_n = P_1\ldots P_rQ_1\ldots Q_s.$$

By Theorem 2.4.11. we see that the product

$$P_1\ldots.P_r = \prod_{i\in I} M_i$$

for some nonempty proper subset I of $\{1,2,\ldots,n\}$. This is a contradiction. Therefore, a is irreducible in I_d.

#

When we take $n = 1$ in Theorem 3.5. we get the following corollary.

<u>Corollary 3.6.</u> If aI_d is a prime module, then a is irreducible in I_d.

Theorem 3.7. Let M be any integral module and $a \in I_d$. If $M(aI_d) = bI_d$ for some nonzero element b in I_d, then M is principal. Furthermore, if $M \neq I_d$ and a is nonunit, then b is reducible in I_d.

Proof. Let M be any integral module and $a \in I_d$ such that $M(aI_d) = bI_d$, for some nonzero element b in I_d. Here a cannot be zero, otherwise we would have $b = 0$. So $M(aI_d)(a^{-1}I_d) = (bI_d)(a^{-1}I_d)$. Therefore, $M = (ba^{-1})I_d$, i.e. M is principal.

If we further assume that $M \neq I_d$ and a is nonunit, then $N(M) \neq 1$ and $N(aI_d) \neq 1$. So $N(bI_d) = N(M(aI_d)) \neq 1$. Therefore, $bI_d \neq I_d$. By Corollary 3.2. b is nonunit. Since $M = (ba^{-1})I_d$, it follows from Corollary 3.2. that ba^{-1} is nonunit in I_d. Since a is nonunit, then $b = (ba^{-1})a$ is reducible. ※

Theorem 3.8. Let $M = \langle a, b+c\omega_d \rangle$ be an integral module. If $M = \alpha I_d$, then $|N(\alpha)| = |ac|$ and $ac \mid N(b+c\omega_d)$.

Proof. Let $M = \langle a, b+c\omega_d \rangle$ be an integral module such that $M = \alpha I_d$. Then by Remark 2.3.14, $N(M) = N(\alpha I_d) = |N(\alpha)|$. By Theorem 2.5.4, $N(M) = |ac|$. Therefore, $|N(\alpha)| = |ac|$. Since $b+c\omega_d \in M$, so $b+c\omega_d = \alpha\gamma$ for some $\gamma \in I_d$. So $N(b+c\omega_d) = N(\alpha\gamma) = N(\alpha)N(\gamma)$. Since $b+c\omega_d$, α and $\gamma \in I_d$, then $N(b+c\omega_d)$, $N(\alpha)$ and $N(\gamma)$ are rational integers. So $N(\alpha) \mid N(b+c\omega_d)$. Therefore, $ac \mid N(b+c\omega_d)$. #

Theorem 3.9. Let M be any integral module in $\mathbb{Q}(\sqrt{d})$ of norm n. Then M is not principal in the following cases:

(i) $d\equiv 1 \pmod 4$ and $|x^2-dy^2| = 4n$ is not solvable in rational integers.

(ii) $d\equiv 2,3 \pmod 4$ and $|x^2-dy^2| = n$ is not solvable in rational integers.

Proof. Let M be any integral module in $\mathbb{Q}(\sqrt{d})$ of norm n. We shall show by contrapositive. Suppose that M is principal. Then $M = \alpha I_d$ for some $\alpha \in I_d$. Therefore, $\alpha = a+b\omega_d$, for some $a,b\in\mathbb{Z}$. Since $N(M) = n$ and

$$\begin{aligned} N(M) &= N((a+b\omega_d)I_d) \\ &= |N(a+b\omega_d)| \\ &= |a^2+ab\omega_d+ab\omega_d'+b^2\omega_d\omega_d'|, \end{aligned}$$

so

$$|a^2+ab\omega_d+ab\omega_d'+b^2\omega_d\omega_d'| = n. \qquad \text{.......(I)}$$

For the case $d\equiv 1 \pmod 4$, we have $\omega_d = (\frac{1+\sqrt{d}}{2})$.

Therefore, the left hand side of (I) is

$$|a^2+ab\omega_d+ab\omega_d'+b^2\omega_d\omega_d'| = |a^2+ab+(\tfrac{1-d}{4})b^2|.$$

So that (I) becomes $|a^2+ab+(\frac{1-d}{4})b^2| = n$. Therefore, there exist $a,b\in\mathbb{Z}$ such that $|a^2+ab+(\frac{1-d}{4})b^2| = n$. Let $x = 2a+b$ and $y = b$. Then clearly $x,y\in\mathbb{Z}$ and

$$\begin{aligned} |x^2-dy^2| &= |4a^2+4ab+b^2-db^2| \\ &= 4|a^2+ab+(\tfrac{1-d}{4})b^2| \\ &= 4n \end{aligned}$$

Hence, there exist $x,y\in\mathbb{Z}$ such that $|x^2-dy^2| = 4n$.

For the case $d \equiv 2,3 \pmod 4$, we have $\omega_d = \sqrt{d}$. So that $\left|a^2+ab\omega_d+ab\omega_d'+b^2\omega_d\omega_d'\right| = \left|a^2-db^2\right|$. Let $x = a$ and $y = b$. Clearly, $x,y \in \mathbb{Z}$ and $\left|x^2-dy^2\right| = n$.

#

<u>Lemma 3.10.</u> Let $a \in I_d$ and M be any principal integral module such that $M \neq I_d$. If a is irreducible and $M \mid aI_d$, then $M=aI_d$.

<u>Proof.</u> Assume that a is irreducible and $M \mid aI_d$. Since M isaprincipal integral module such that $M \neq I_d$, then $M=bI_d$ for some nonzero nonunit b in I_d. So $bI_d \mid aI_d$. Then $aI_d=(bI_d)M_1$ for some integral module M_1. By Theorem 3.7, M_1 is principal. Then $M_1=cI_d$, for some nonzero element c in I_d. Therefore, $aI_d=(bI_d)(cI_d)$. By Remark 3.3, $a=ubc$, where u is a unit of I_d. Since a is irreducible and b is nonunit, we can conclude that c is a unit. By Corollary 3.2, $cI_d=I_d$. Therefore, $aI_d=M$.

#

<u>Lemma 3.11.</u> Let $a_1,\dots,a_t$ be any irreducible elements in I_d and $P_1,\dots,P_r$ be any prime modules such that

$$(a_1I_d)\dots(a_tI_d) = P_1\dots P_r.$$

If P_1 is principal, then there exists i_1 such that $a_{i_1}I_d=P_1$.

<u>Proof.</u> Let $a_1,\dots,a_t$ be any irreducible elements of I_d. Let $P_1,\dots,P_r$ be prime modules such that

$$(a_1I_d)\dots(a_tI_d) = P_1\dots P_r. \quad \dots(I)$$

Suppose that, P_1 is principal. From (I), using Corollary 2.4.10, we get $P_1 \mid a_{i_1}I_d$, for some $1 \leqslant i_1 \leqslant t$. By Lemma 3.10, $a_{i_1}I_d = P_1$.

#

<u>Theorem 3.12.</u> Let $a_1,\dots,a_t$ be any irreducible elements of I_d. Let $P_1,\dots,P_r$ be prime modules such that

$$(a_1I_d)\cdot\ldots\cdot(a_tI_d) = P_1\cdot\ldots\cdot P_r.$$

If $P_1,\dots,P_s, s\leq r, s\leq t$, are principal, then there exist $i_1,\dots,i_s$ such that $a_{i_j}I_d = P_j$ $(j=1,2,\dots,s)$.

<u>Proof.</u> Since P_1 is principal, hence by Lemma 3.11, there is i_1 such that

$$a_{i_1}I_d = P_1.$$

Assume that we have found $i_1,\dots,i_k, k<s$ such that

$$a_{i_j}I_d = P_j\ , \quad (j=1,2,\dots,k)$$

Then we have

$$\prod_{i=1}^{t} a_iI_d = P_1\ldots P_kP_{k+1}\ldots P_r.$$

$$\Big(\prod_{j=1}^{k} a_{i_j}I_d\Big)\Big(\prod_{\substack{i=1\\ i\neq i_1,\dots,i_k}}^{t} a_iI_d\Big) = \Big(\prod_{i=1}^{k} P_i\Big)P_{k+1}\ldots P_r.$$

Since $$\prod_{j=1}^{k} a_{i_j}I_d = \prod_{j=1}^{k} P_j,$$

hence, we have

$$\prod_{\substack{i=1\\ i\neq i_1,\dots,i_k}}^{t} a_iI_d = P_{k+1}\ldots P_r.$$

Since P_{k+1} is principal, hence by Lemma 3.11. there exists $i_{k+1}\neq i_1,\dots,i_k$ such that

$$a_{i_{k+1}}I_d = P_{k+1}.$$

Hence we can choose $i_1,\dots,i_s$ such that $a_{i_j}I_d = P_j, j=1,\dots,s$

#

<u>Theorem 3.13.</u> Let $a \in I_d$. If aI_d can be factored into

$$aI_d = (a_1I_d)(a_2I_d)\ldots.(a_nI_d),$$

where $a_1I_d,\ldots.,a_nI_d$ are prime modules, then

$$a = ua_1\ldots.a_n,$$

where u is a unit and a_i is irreducible. When this is the case, the factorization of a into irreducible elements is unique.

<u>Proof.</u> Let $a \in I_d$ such that $aI_d=(a_1I_d)\ldots.(a_nI_d)$, where $a_1I_d,\ldots,a_nI_d$ are prime modules. By Corollary 3.6, $a_1,\ldots,a_n$ are irreducible in I_d. By Remark 3.3, $a=ua_1\ldots a_n$, where u is a unit of I_d.

Let $b_1,\ldots,b_m$ be any irreducible elements of I_d such that $a=b_1\ldots.b_m$. So $aI_d = (b_1I_d)\ldots.(b_mI_d)$. Therefore,

$$(b_1I_d)\ldots.(b_mI_d) = (a_1I_d)\ldots.(a_nI_d) \quad \ldots.(I)$$

For each $1\leqslant k\leqslant n$, $1\leqslant l\leqslant m$, a_k and b_l are irreducible. Then a_k and b_l are not associate to 1. By Corollary 3.2, $a_kI_d \neq I_d$ and $b_lI_d \neq I_d$. By Corollary 2.5.6, we have

$$N(a_kI_d) \neq 1 \text{ and } N(b_lI_d) \neq 1 \quad \ldots\ldots(II)$$

Suppose that, $m<n$. Then by Theorem 3.12, there exist $i_1,\ldots,i_m$ such that $b_{i_j}I_d = a_jI_d,(j=1,2,..,m)$. So we cancel $b_{i_j}I_d = a_jI_d$, for $j=1,2,..,m$ in (I). We get

$$I_d = (a_{m+1}I_d)\ldots.(a_nI_d).$$

So

$$1 = N(I_d) = N(a_{m+1}I_d)\ldots\ldots N(a_nI_d).$$

It contradicts to (II).

Suppose that, m>n. Then by Theorem 3.12, there exist $i_1,\ldots,i_n$ such that $b_{i_j}I_d = a_jI_d$, $j = 1,2,\ldots,n$. So we cancel $b_{i_j}I_d = a_jI_d$ for $j = 1,2,..,n$. in (I). We get

$$(b_{n+1}I_d)\ldots.(b_mI_d) = I_d.$$

So

$$N(b_{n+1}I_d)\ldots.N(b_mI_d) = N(I_d) = 1.$$

It contradictsto (II).

Thus, we can conclude that m = n. By Theorem 3.12, there exist $i_1,\ldots,i_n$ such that $b_{i_j}I_d = a_jI_d$ for $j = 1,.,n$.

By Theorem 3.1, $b_{i_j} \sim a_j$ for $j = 1,2,..,n$. #

Theorem 3.14. In any quadratic fields $\mathbb{Q}(\sqrt{d})$. If p is a rational prime, then the factorization of p into irreducible elements of I_d is unique.

Proof. Let $\mathbb{Q}(\sqrt{d})$ be any quadratic field and p be rational prime.

Case I. Assume that p is inert. Then pI_d is a prime module. By Corollary 3.6, p is an irreducible element of I_d.

Case II. Assume that p is not inert. Then p is ramified or decomposed. So $pI_d=PP'$, where P and P' are prime modules. If P is principal, then by Theorem 3.7, P' is principal. Hence, by Theorem 3.13, the factorization of p into irreducible elements of I_d is unique. If P is not principal, then by Theorem 3.7, P' is not principal. By Theorem 3.5, p is irreducible.

Hence, the factorization of p into irreducible elements of I_d is unique.

#

Example 3.15. We shall find all factorizations of 55 in $\mathbb{Q}(\sqrt{-6})$. Since $-6 \equiv 2 \pmod 4$, it follows from Remark 2.1.9 and Remark 2.2.8 that $I_{-6} = \langle 1, \sqrt{-6} \rangle$ and $\Delta_{-6} = -24$.

Observe that $$55I_{-6} = (5I_{-6})(11I_{-6}).$$

Using Theorem 2.4.17(ii) and Definition 2.4.15, it can be verified that 5 is decomposed and we have

(1) $$5I_{-6} = P_1P_1',$$

where $P_1 = \langle 5, 2+\sqrt{-6} \rangle$ and $P_1' = \langle 5, 3+\sqrt{-6} \rangle$ are distinct prime modules such that $N(P_1) = N(P_1') = 5$ (See Example 2.4.18.) By the same argument we have

(2) $$11I_{-6} = P_2P_2',$$

where $P_2 = \langle 11, 4+\sqrt{-6} \rangle$ and $P_2' = \langle 11, 7+\sqrt{-6} \rangle$ are distinct prime modules such that $N(P_2) = N(P_2') = 11$. Therefore,

(3) $$55I_{-6} = P_1P_1'P_2P_2'.$$

Now our problem is to group the productsof P_1, P_1', P_2, P_2' to form principal modules generated by irreducible elements. We claim that P_1, P_1', P_2, P_2' are not principal. Observe that each of the equations

$$|x^2+6y^2| = 5$$

and

$$|x^2+6y^2| = 11$$

does not have any solution in $\mathbb{Z}$. Hence, by Theorem 3.9, any integral modules of norm 5 or 11 is not principal. Hence P_1, P_1', P_2, P_2' are not principal.

Therefore, there are 3 cases to be considered:

(I) $$55I_{-6} = (P_1P_1')(P_2P_2')$$

(II) $$55I_{-6} = (P_1P_2)(P_1'P_2')$$

(III) $$55I_{-6} = (P_1P_2')(P_1'P_2).$$

Clearly, case (I) gives

$$(I') \qquad 55I_{-6} = (5I_{-6})(11I_{-6}),$$

For case (II), we first determine the product P_1P_2. From Example 2.5.10, we have

$$P_1P_2 = \langle 5, 2+\sqrt{-6}\rangle\langle 11, 4+\sqrt{-6}\rangle.$$
$$= \langle 55, 37+\sqrt{-6}\rangle.$$

Therefore

$$P_1P_2 = (1+3\sqrt{-6})\langle 1-3\sqrt{-6}, 1-2\sqrt{-6}\rangle$$
$$= (1+3\sqrt{-6})\langle -\sqrt{-6}, 1-2\sqrt{-6}\rangle$$
$$= (1+3\sqrt{-6})\langle -\sqrt{-6}, 1\rangle$$
$$= (1+3\sqrt{-6})I_{-6}.$$

Since $P_1'P_2' = (P_1P_2)'$, it follows that $P_1'P_2' = ((1+3\sqrt{-6})I_{-6})'$ $= (1-3\sqrt{-6})I_{-6}$. Then from (II) we get

$$(II') \qquad 55I_{-6} = (1+3\sqrt{-6})I_{-6}(1-3\sqrt{-6})I_{-6}.$$

Finally, we consider case (III). By the same argument as in this case (II), we have $P_1P_2' = (7+\sqrt{-6})I_{-6}$ and $P_1'P_2 = (7-\sqrt{-6})I_{-6}$. So in this case we get

$$(III') \qquad 55I_{-6} = (7+\sqrt{-6})I_{-6}(7-\sqrt{-6})I_{-6}.$$

By Theorem 3.5, we can verify that $5, 11, 1+3\sqrt{-6}, 7+\sqrt{-6}$, $7-\sqrt{-6}$ are irreducible elements of I_{-6}. So using Remark 3.3 to (I'),(II'),(III'), we see that the only factorizationsof 55 into a product of irreducible are

$$(I'') \qquad 55 = u_1.5.11$$

$$(II'') \qquad 55 = u_2(1+3\sqrt{-6})(1-3\sqrt{-6})$$

$$(III'') \qquad 55 = u_3(7+\sqrt{-6})(7-\sqrt{-6}),$$

where u_1, u_2, u_3 are units. In this cases we have $u_1 = u_2 = u_3 = 1$.

#

Example 3.16. We shall find all factorizations of 42 in $\mathbb{Q}(\sqrt{-5})$. Since $-5\equiv 3 \pmod 4$, it follows from Remark2.1.9. and Remark 2.2.8 that $I_{-5} = \langle 1,\sqrt{-5}\rangle$ and $\Delta_{-5} = -20$.

Observe that, $42I_{-5} = (2I_{-5})(3I_{-5})(7I_{-5})$.

Using Theorem 2.4.17(i) and Definition 2.4.15, we can verify that 2 is ramified. i.e. we have

(1) $$2I_{-5} = P_1^2,$$

where $P_1 = P_1' = \langle 2,1+\sqrt{-5}\rangle$ is a prime module and $N(P_1) = 2$. (See Example 2.4.19) By Theorem 2.4.17(ii) and Definition 2.4.15, we can verify that 3,7 are decomposed, and we have

(2) $$3I_{-5} = P_2P_2',$$

where $P_2 = \langle 3,1+\sqrt{-5}\rangle$ and $P_2' = \langle 3,2+\sqrt{-5}\rangle$ are distinct prime modules such that $N(P_2) = N(P_2') = 3$. And

(3) $$7I_{-5} = P_3P_3',$$

where $P_3 = \langle 7,3+\sqrt{-5}\rangle$ and $P_3' = \langle 7,4+\sqrt{-5}\rangle$ are distinct prime modules such that $N(P_3) = N(P_3') = 7$. Therefore,

(4) $$42I_{-5} = P_1^2P_2P_2'P_3P_3'.$$

Now we consider all possible groupings of the productsof $P_1,P_1,P_2,P_2',P_3,P_3'$ to form principal modules generated by irreducible elements.

Using Theorem 3.9, we can verify that P_1,P_2,P_2',P_3 P_3' are not principal

First, we consider the groupingsof the P_i,P_i' in the factorization (4) in which each group contains two modules.

There are 15 cases:

$$\text{(I)} \quad 42I_{-5} = (P_1^2)(P_2P_2')(P_3P_3')$$

$$\text{(II)} \quad 42I_{-5} = (P_1^2)(P_2P_3)(P_2'P_3')$$

$$\text{(III)} \quad 42I_{-5} = (P_1^2)(P_2P_3')(P_2'P_3)$$

$$\text{(IV)} \quad 42I_{-5} = (P_1P_2)(P_1P_2')(P_3P_3')$$

$$\text{(V)} \quad 42I_{-5} = (P_1P_2)(P_1P_3)(P_2'P_3')$$

$$\text{(VI)} \quad 42I_{-5} = (P_1P_2)(P_1P_3')(P_2'P_3)$$

$$\text{(VII)} \quad 42I_{-5} = (P_1P_2')(P_1P_2)(P_3P_3')$$

$$\text{(VIII)} \quad 42I_{-5} = (P_1P_2')(P_1P_3)(P_2P_3')$$

$$\text{(IX)} \quad 42I_{-5} = (P_1P_2')(P_1P_3')(P_2P_3)$$

$$\text{(X)} \quad 42I_{-5} = (P_1P_3)(P_1P_2)(P_2'P_3')$$

$$\text{(XI)} \quad 42I_{-5} = (P_1P_3)(P_1P_2')(P_2P_3')$$

$$\text{(XII)} \quad 42I_{-5} = (P_1P_3)(P_1P_3')(P_2P_2')$$

$$\text{(XIII)} \quad 42I_{-5} = (P_1P_3')(P_1P_2)(P_2'P_3)$$

$$\text{(XIV)} \quad 42I_{-5} = (P_1P_3')(P_1P_2')(P_2P_3)$$

$$\text{(XV)} \quad 42I_{-5} = (P_1P_3')(P_1P_3)(P_2P_2').$$

Note that we have

$$\text{(i)} \qquad P_1^2 = 2I_{-5}, \quad P_2P_2' = 3I_{-5}, \quad P_3P_3' = 7I_{-5}.$$

By using Theorem 2.5.8, we have

$$\text{(ii)} \quad P_1P_2 = \langle 2,1+\sqrt{-5}\rangle\langle 3,1+\sqrt{-5}\rangle = \langle 6,1+\sqrt{-5}\rangle = (1+\sqrt{-5})I_{-5}$$

$$\text{(iii)} \quad P_1P_3 = \langle 2,1+\sqrt{-5}\rangle\langle 7,3+\sqrt{-5}\rangle = \langle 14,3+\sqrt{-5}\rangle = (3+\sqrt{-5})I_{-5}$$

$$\text{(iv)} \quad P_2P_3 = \langle 3,1+\sqrt{-5}\rangle\langle 7,3+\sqrt{-5}\rangle = \langle 21,10+\sqrt{-5}\rangle = (1-2\sqrt{-5})I_{-5}$$

$$\text{(v)} \quad P_2'P_3 = \langle 3,2+\sqrt{-5}\rangle\langle 7,3+\sqrt{-5}\rangle = \langle 21,-4+\sqrt{-5}\rangle = (4-\sqrt{-5})I_{-5}$$

It follows that

$$\text{(vi)} \quad P_1'P_2' = (P_1P_2)' = (1-\sqrt{-5})I_{-5}$$

$$\text{(vii)} \quad P_1'P_3' = (P_1P_3)' = (3-\sqrt{-5})I_{-5}$$

$$\text{(viii)} \quad P_2'P_3' = (P_2P_3)' = (1+2\sqrt{-5})I_{-5}$$

(ix) $P_2P_3' = (P_2'P_3)' = (4+\sqrt{-5})I_{-5}$.

So we can see that any product of two modules from P_i, P_i', $i = 1,2,3$, is principal with irreducible generator. The fact that the generator is irreducible follows from Theorem 3.5.

From the above results, we see that every product of any four modules from $P_i, P_i', i = 1,2,3$, is also principal. However, its generator will not be an irreducible element. We now consider the productsof three or five modules from P_i, P_i', $i = 1,2,3$. Suppose that there exists a product of three of these modules which is principal. For example, suppose that $P_1P_2'P_3$ is principal. Since $P_2'P_3 = (4-\sqrt{-5})I_{-5}$, it follows that $P_1(4-\sqrt{-5})I_{-5} = P_1P_2'P_3$ is principal. So by Theorem 3.7, it follows that P_1 must be principal. This is a contradiction. So that the product $P_1P_2'P_3$ is not principal. By the same argument we see that any productsof three or five of $P_1, P_1, P_2, P_2', P_3, P_3'$ cannot be principal.

Therefore, all possible groupingsof the productsof $P_1, P_1, P_2, P_2', P_3, P_3'$ to form principal modules generated by irreducible elements are as listed in cases(I) through (XV). By substituting (i),(ii),(iii),(iv),(v),(vi),(vii),(viii) in the case(I) through (XV), we get that

(I$'$) $42I_{-5} = (2I_{-5})(3I_{-5})(7I_{-5})$

(II$'$) $42I_{-5} = (2I_{-5})(1-2\sqrt{-5})I_{-5}(1+2\sqrt{-5})I_{-5}$

(III$'$) $42I_{-5} = (2I_{-5})(4+\sqrt{-5})I_{-5}(4-\sqrt{-5})I_{-5}$

(IV$'$) $42I_{-5} = (1+\sqrt{-5})I_{-5}(1-\sqrt{-5})I_{-5}(7I_{-5})$

$$(V') \quad 42I_{-5} = (1+\sqrt{-5})I_{-5}(3+\sqrt{-5})I_{-5}(1+2\sqrt{-5})I_{-5}$$

$$(VI') \quad 42I_{-5} = (1+\sqrt{-5})I_{-5}(3-\sqrt{-5})I_{-5}(4-\sqrt{-5})I_{-5}$$

$$(VII') \quad 42I_{-5} = (1-\sqrt{-5})I_{-5}(1+\sqrt{-5})I_{-5}(7I_{-5})$$

$$(VIII') \quad 42I_{-5} = (1-\sqrt{-5})I_{-5}(3+\sqrt{-5})I_{-5}(4+\sqrt{-5})I_{-5}$$

$$(IX') \quad 42I_{-5} = (1-\sqrt{-5})I_{-5}(3-\sqrt{-5})I_{-5}(1-2\sqrt{-5})I_{-5}$$

$$(X') \quad 42I_{-5} = (3+\sqrt{-5})I_{-5}(1+\sqrt{-5})I_{-5}(1+2\sqrt{-5})I_{-5}$$

$$(XI') \quad 42I_{-5} = (3+\sqrt{-5})I_{-5}(1-\sqrt{-5})I_{-5}(4+\sqrt{-5})I_{-5}$$

$$(XII') \quad 42I_{-5} = (3+\sqrt{-5})I_{-5}(3-\sqrt{-5})I_{-5}(3I_{-5})$$

$$(XIII') \quad 42I_{-5} = (3-\sqrt{-5})I_{-5}(1+\sqrt{-5})I_{-5}(4-\sqrt{-5})I_{-5}$$

$$(XIV') \quad 42I_{-5} = (3-\sqrt{-5})I_{-5}(1-\sqrt{-5})I_{-5}(1-2\sqrt{-5})I_{-5}$$

$$(XV') \quad 42I_{-5} = (3-\sqrt{-5})I_{-5}(3+\sqrt{-5})I_{-5}(3I_{-5}).$$

Observe that some of these factorizationsare the same, for example (IV$'$) and (VII$'$). The only distinct factorizationsare (I$'$),(II$'$),(III$'$),(IV$'$),(V$'$),(VI$'$),(VIII$'$),(IX$'$),(XII$'$). From these distinct factorizations, using Remark 3.3, we obtain all the distinct factorizations of 42 into irreducible factors as follows:

$$(I'') \quad 42 = u_1 \cdot 2.3.7$$

$$(II'') \quad 42 = u_2 . 2(1-2\sqrt{-5})(1+2\sqrt{-5})$$

$$(III'') \quad 42 = u_3 . 2(4+\sqrt{-5})(4-\sqrt{-5})$$

$$(IV'') \quad 42 = u_4(1+\sqrt{-5})(1-\sqrt{-5}).7$$

$$(V'') \quad 42 = u_5(1+\sqrt{-5})(3+\sqrt{-5})(1+2\sqrt{-5})$$

$$(VI'') \quad 42 = u_6(1+\sqrt{-5})(3-\sqrt{-5})(4-\sqrt{-5})$$

$$(VIII'') \quad 42 = u_8(1-\sqrt{-5})(3+\sqrt{-5})(4+\sqrt{-5})$$

$$(IX'') \quad 42 = u_9(1-\sqrt{-5})(3-\sqrt{-5})(1-2\sqrt{-5})$$

$$(XII'') \quad 42 = u_{12}(3+\sqrt{-5})(3-\sqrt{-5}) \cdot 3,$$

where $u_1, u_2, u_3, u_4, u_5, u_6, u_8, u_9, u_{12}$ are units. In these case we have $u_1=u_2=u_3=u_4=u_6=u_8=u_{12}=1$ and $u_5=u_9=-1$.

#

Theorem 3.17. Let M_1 and M_2 be any spg-modules. Then $M_1 \sim M_2$ if and only if M_1M_2' is a principal module.

Proof. Using Remark 2.3.22, we have

$$\begin{aligned} M_1 \sim M_2 &\Longleftrightarrow [M_1] = [M_2] \\ &\Longleftrightarrow [M_1M_2'] = [M_1][M_2'] = [M_2][M_2'] = [M_2M_2'] = [I_d] \\ &\Longleftrightarrow M_1M_2' \text{ is principal} \end{aligned}$$

Therefore, $M_1 \sim M_2$ if and only if M_1M_2' is a principal module.

Theorem 3.18. Let $\mathbb{Q}(\sqrt{d})$ be any quadratic field with $h_d = 2$. Then the product of any two spg-modules, which are not principal, is principal.

Proof. Let M_1 and M_2 be any spg-modules which are not principal. So that $[M_1] \neq [I_d]$, $[M_2] \neq [I_d]$. Since $h_d = 2$, hence $[M_1] = [M_2]$. Therefore, $M_1M_2 \in [M_1][M_2] = [M_1]^2 = [I_d]$. i.e. M_1M_2 is principal.

#

Example 3.19. We shall find all factorizations of 6510 in $\mathbb{Q}(\sqrt{-31})$. Since $-31 \equiv 1 \pmod 4$, it follows from Remark 2.1.9. and Remark 2.2.8, that $I_{-31} = \left\langle 1, \frac{1+\sqrt{-31}}{2} \right\rangle$ and $\Delta_{-31} = -31$. In the Table 3 of [1], we see that $h_{-31} = 3$.

Observe that $6510 I_{-31} = (3I_{-31})(31I_{-31})(2I_{-31})(5I_{-31})(7I_{-31})$

Using Theorem 2.4.17(ii) and Definition 2.4.15, we can verify that 3 is inert, (See Example 2.4.19), i.e. we have

$$3I_{-31}$$

is a prime module. By Theorem 2.4.17(i) and Definition 2.4.15, we can see that 31 is ramified. i.e. we have

$$31I_{-31} = P^2,$$

where $P = \left\langle 31, \frac{-31+\sqrt{-31}}{2} \right\rangle$ is a prime module. By Theorem 2.4.17(ii) and Definition 2.4.15, we can verify that 2,5,7 are decomposed. i.e. we have

(i) $$2I_{-31} = P_1 P_1',$$

where $P_1 = \langle 2, 1+\omega_{-31} \rangle$, $P_1' = \langle 2, \omega_{-31} \rangle$ are distinct prime modules such that $N(P_1) = N(P_1') = 2$.

(ii) $$5I_{-31} = P_2 P_2',$$

where $P_2 = \langle 5, 3+\omega_{-31} \rangle$, $P_2' = \langle 5, 1+\omega_{-31} \rangle$ are distinct prime modules such that $N(P_2) = N(P_2') = 5$.

(iii) $$7I_{-31} = P_3 P_3',$$

where $P_3 = \langle 7, 2+\omega_{-31} \rangle$, $P_3' = \langle 7, 4+\omega_{-31} \rangle$ are distinct prime modules such that $N(P_3) = N(P_3') = 7$. Therefore,

(iv) $$6510I_{-31} = (3I_{-31})P^2 P_1 P_1' P_2 P_2' P_3 P_3'.$$

Now we consider all possible groupingsof the productsof $(3I_{-31}), P, P, P_1, P_1', P_2, P_2', P_3, P_3'$ to form principal modules with irreducible generator. Clearly, $3I_{-31}$ is principal and its generator 3 is irreducible. So we consider

(v) $$P = \left\langle 31, \frac{-31+\sqrt{-31}}{2} \right\rangle$$
$$= (\sqrt{-31}) \left\langle -\sqrt{-31}, \frac{\sqrt{-31}+1}{2} \right\rangle$$
$$= (\sqrt{-31}) \left\langle 1, \frac{\sqrt{-31}+1}{2} \right\rangle$$
$$= (\sqrt{-31}) I_{-31}$$

Therefore, P is a principal module with irreducible generator. Using Theorem 3.9, we can verify that $P_1, P_1', P_2, P_2', P_3, P_3'$ are not principal.

Next we consider the groupings of the prime modules on the right hand side of(iv). By Theorem 3.7, each of the prime module $3I_{-31}$, P cannot be grouped among themself or with any other modules $P_i, P_i', i=1,2,3,$ to form a principal module with irreducible generator. So, we need to consider only the groupings of $P_1, P_1', P_2, P_2', P_3, P_3'$. So we know that $h_{-31} = 3$. So we may assume that the class group of I_{-31} is $\left\{ [I_{-31}], [P_1], [P_1'] \right\}$. So that each of P_2, P_2', P_3, P_3' must belong to $[P_1]$ or $[P_1']$. By using Theorem 2.5.7, it can be verified that

(vi) $$P_1' P_2 = \langle 2, \omega_{-31} \rangle \langle 5, 3+\omega_{-31} \rangle$$
$$= \langle 10, -2+\omega_{-31} \rangle$$
$$= (-2+\omega_{-31}) \langle -2+\omega_{-31}', 1 \rangle$$
$$= (-2+\omega_{-31}) I_{-31}$$

The detail calculation of this result is shown in Example 2.5.9. By the same method we have

(vii) $$P_1' P_3 = \langle 2, \omega_{-31} \rangle \langle 7, 2+\omega_{-31} \rangle$$
$$= \langle 14, 2+\omega_{-31} \rangle$$
$$= (2+\omega_{-31}) \langle 2+\omega_{-31}', 1 \rangle$$
$$= (2+\omega_{-31}) I_{-31}$$

By Theorem 3.17, we conclude that P_1', P_2', P_3' are similar . So $P_2', P_3' \in [P_1']$. Then $P_2, P_3 \in [P_1]$. Then we see that the product of two modules from $P_i, P_i', (i=1,2,3)$ is principal if and only if each module is in the distinct class. This can happen in the following 6 cases:

(I) $(P_1P_1')(P_2P_2')(P_3P_3')$

(II) $(P_1P_1')(P_2P_3')(P_2'P_3)$

(III) $(P_1P_2')(P_1'P_2)(P_3P_3')$

(IV) $(P_1P_2')(P_1'P_3)(P_2P_3')$

(V) $(P_1P_3')(P_1'P_2)(P_2'P_3)$

(VI) $(P_1P_3')(P_1'P_3)(P_2P_2')$

Observe that the grouping in to a group of three:

(VII) $(P_1P_2P_3)(P_1'P_2'P_3')$

also gives principal modules. It can be verified that every other grouping of three modules does not give principal factors.

Next, observe that any grouping of the product of at least four modules from P_i, P_i' $(i=1,2,3)$ must contain a product of two modules from different classes. It follows from Theorem 3.7 that if the product of such a grouping is principal, then its generator will not be irreducible. So only cases(I) through (VII) are possible. Thus all possible groupings of the products of $3I_{-31}, P, P, P_1, P_1', P_2, P_2', P_3, P_3'$ which give principal modules with irreducible generators are the following 7 possibilities:

$$(I') \quad 6510I_{-31} = (3I_{-31})(P)(P)(P_1P_1')(P_1P_2')(P_3P_3')$$
$$(II') \quad 6510I_{-31} = (3I_{-31})(P)(P)(P_1P_1')(P_2P_3')(P_2'P_3)$$
$$(III') \quad 6510I_{-31} = (3I_{-31})(P)(P)(P_1P_2')(P_1'P_2)(P_3P_3')$$
$$(IV') \quad 6510I_{-31} = (3I_{-31})(P)(P)(P_1P_2')(P_1'P_3)(P_2P_3')$$
$$(V') \quad 6510I_{-31} = (3I_{-31})(P)(P)(P_1P_3')(P_1'P_2)(P_2'P_3)$$
$$(VI') \quad 6510I_{-31} = (3I_{-31})(P)(P)(P_1P_3')(P_1'P_3)(P_2P_2')$$
$$(VII') \quad 6510I_{-31} = (3I_{-31})(P)(P)(P_1P_2P_3)(P_1'P_2'P_3')$$

By using Theorem 2.5.7, we get

$$\begin{aligned}
(viii) \quad P_2P_3' &= \langle 5, 3+\underline{\omega}_{31}\rangle\langle 7, 4+\underline{\omega}_{31}\rangle \\
&= \langle 35, 18+\underline{\omega}_{31}\rangle \\
&= (1+2\underline{\omega}_{31})\langle 1+2\underline{\omega}_{31}', 1+\underline{\omega}_{31}\rangle \\
&= (1+2\underline{\omega}_{31})I_{-31}
\end{aligned}$$

and

$$\begin{aligned}
(ix) \quad P_1P_2P_3 &= \langle 2, 1+\underline{\omega}_{31}\rangle\langle 5, 3+\underline{\omega}_{31}\rangle\langle 7, 2+\underline{\omega}_{31}\rangle \\
&= \langle 10, 3+\underline{\omega}_{31}\rangle\langle 7, 2+\underline{\omega}_{31}\rangle \\
&= \langle 70, 23+\underline{\omega}_{31}\rangle \\
&= (-1+3\underline{\omega}_{31})\langle -1+3\underline{\omega}_{31}', \underline{\omega}_{31}'\rangle \\
&= (-1+3\underline{\omega}_{31})I_{-31}
\end{aligned}$$

It follows that

$$\begin{aligned}
(x) \quad P_1P_2' &= (P_1'P_2)' = (-2+\underline{\omega}_{31}'')I_{-31} \\
(xi) \quad P_1P_3' &= (P_1'P_3)' = (2+\underline{\omega}_{31}')I_{-31} \\
(xii) \quad P_2'P_3 &= (P_2P_3') = (1+2\underline{\omega}_{31}')I_{-31} \\
(xiii) \quad P_1'P_2'P_3' &= (P_1P_2P_3)' = (-1+3\underline{\omega}_{31}')I_{-31}
\end{aligned}$$

By substituting (ii),(iii),(v),(vi),(vii),(viii),(ix),(x),(xi),(xii),(xiii) in case (I') through case (VII'), we get that

$$(\mathrm{I}'')\quad 6510I_{-31} = (3I_{-31})(\sqrt{-31}I_{-31})^2(2I_{-31})(5I_{-31})(7I_{-31})$$

$$(\mathrm{II}'')\quad 6510I_{-31} = (3I_{-31})(\sqrt{-31}I_{-31})^2(2I_{-31})(1+2\underline{\omega}_{31})I_{-31}(1+2\underline{\omega}'_{31})I$$

$$(\mathrm{III}'')\quad 6510I_{-31} = (3I_{-31})(\sqrt{-31}I_{-31})^2(-2+\underline{\omega}'_{31})I_{-31}(-2+\underline{\omega}_{31})I_{-31}(7I_{-31})$$

$$(\mathrm{IV}'')\quad 6510I_{-31} = (3I_{-31})(\sqrt{-31}I_{-31})^2(-2+\underline{\omega}'_{31})I_{-31}(2+\underline{\omega}_{31})I_{-31}(1+2\underline{\omega}_{31})I_{-31}$$

$$(\mathrm{V}'')\quad 6510I_{-31} = (3I_{-31})(\sqrt{-31}I_{-31})^2(2+\underline{\omega}'_{31})I_{-31}(-2+\underline{\omega}_{31})I_{-31}(1+2\underline{\omega}'_{31})I_{-31}$$

$$(\mathrm{VI}'')\quad 6510I_{-31} = (3I_{-31})(\sqrt{-31}I_{-31})^2(2+\underline{\omega}'_{31})I_{-31}(2+\underline{\omega}_{31})I_{-31}(5I_{-31})$$

$$(\mathrm{VII}'')\quad 6510I_{-31} = (3I_{-31})(\sqrt{-31}I_{-31})\ (-1+3\underline{\omega}_{31})I_{-31}(-1+3\underline{\omega}'_{31})I_{-31}$$

Using Theorem 3.5 and Corollary 3.6 we can check that the generator of any principal modules in the right hand side of case (I'') through case (VII'') are irreducible elements. Using Remark 3.3 to case (I'') through case (VII'') we obtain all the factoriztions of 6510. They are as follows:

$$(\mathrm{I}''')\quad 6510 = u_1.3(\sqrt{-31})^2.2.5.7$$

$$(\mathrm{II}''')\quad 6510 = u_2.3(\sqrt{-31})^2.2(1+2\underline{\omega}_{31})(1+2\underline{\omega}'_{31})$$

$$(\mathrm{III}''')\quad 6510 = u_3.3(\sqrt{-31})^2(-2+\underline{\omega}'_{31})(-2+\underline{\omega}_{32}).7$$

$$(\mathrm{IV}''')\quad 6510 = u_4.3(\sqrt{-31})^2(-2+\underline{\omega}'_{31})(2+\underline{\omega}_{31})(1+2\underline{\omega}_{31})$$

$$(\mathrm{V}''')\quad 6510 = u_5.3(\sqrt{-31})^2(2+\underline{\omega}'_{31})(-2+\underline{\omega}_{31})(1+2\underline{\omega}'_{31})$$

$$(\mathrm{VI}''')\quad 6510 = u_6.3(\sqrt{-31})^2(2+\underline{\omega}'_{31})(2+\underline{\omega}_{31}).5$$

$$(\mathrm{VII}''')\quad 6510 = u_7.3(\sqrt{-31})^2(-1+3\underline{\omega}_{31})(-1+3\underline{\omega}'_{31}),$$

where $u_1, u_2, u_3, u_4, u_5, u_6, u_7$ are units. In this cases, we have $u_1 = u_2 = u_3 = u_4 = u_5 = u_6 = u_7 = -1$.

#