Honam Mathematical J. **26**(2004), No. 3, pp. 247–256

ON THE STRUCTURES OF CLASS SEMIGROUPS OF QUADRATIC NON-MAXIMAL ORDERS

Yong Tae Kim

Abstract. Buchmann and Williams[1] proposed a key exchange system making use of the properties of the maximal order of an imaginary quadratic field. Hühnlein et al. [6,7] also introduced a cryptosystem with trapdoor decryption in the class group of the non-maximal imaginary quadratic order with prime conductor q. Their common techniques are based on the properties of the invertible ideals of the maximal or non-maximal orders respectively. Kim and Moon [8], however, proposed a key-exchange system and a public-key encryption scheme, based on the class semigroups of imaginary quadratic non-maximal orders. In Kim and Moon[8]'s cryptosystem, a non-invertible ideal is chosen as a generator of key-exchange ststem and their secret key is some characteristic value of the ideal on the basis of Zanardo et al.[9]'s quantity for ideal equivalence. In this paper we propose the methods for finding the non-invertible ideals corresponding to non-primitive quadratic forms and clarify the structure of the class semigroup of non-maximal order as finitely disjoint union of groups with some quantities correctly. And then we correct the misconceptions of Zanardo et al.[9] and analyze Kim and Moon[8]'s cryptosystem.

Received Jun 24, 2004; Accepted July 13, 2004.

2000 Mathematics Subject Classification: 11Y40, 94A60.

Keyword and phrases: class semigroup, non-invertible ideal, power of ideals/classes, key exchange system .

This paper was partially supported by Gwangju National University of Education 2003.

1. Introduction

Public key cryptography is unquestionably a core technology which is widely applied to information technology systems and electronic commerce. As one of public key cryptosystems, a key exchange system making use of the properties of the maximal order of an imaginary quadratic field is proposed by Buchmann and Williams[1]. Hühnlein et al [6,7] also introduced a cryptosystem with trapdoor decryption based on the difficulty of computing discrete logarithms in the class group of the non-maximal imaginary quadratic order with prime conductor q. Their common techniques are based on the properties of the invertible ideals of the maximal or non-maximal orders respectively. Kim and Moon [8], however, proposed a key-exchange system and a public-key encryption scheme, based on the class semigroups of imaginary quadratic non-maximal orders, whose securities are based on the fact that there is no efficient algorithm to compute the structure of the class semigroup of a non-maximal order and the unique factorization can fail for non-invertible ideals. In Kim and Moon[8]'s cryptosystem, a non-invertible ideal is chosen as a generator of key-exchange ststem and their secret key is some characteristic value of the ideal on the basis of Zanardo et al.[9]'s quantity for ideal equivalence. Zanardo, however, was wrong in defining the condition for equivalence relation between ideals. In this paper we propose the methods for finding the non-invertible ideals corresponding to non-primitive quadratic forms and clarify the structure of the class semigroup of non-maximal order as finitely disjoint union of groups with some quantities correctly. And then we correct the misconceptions of Zanardo et al.[9] and anlayze Kim and Moon[8]'s cryptosystem.

2.Preliminaries

In this chapter, we introduce some facts concerning class semigroup in imaginary quadratic field. Throughout this paper, most of the terminologies are due to Gauss[3] and notations and some preliminaries due to Cox[2] and Zanardo et al.[9] and the notations O,$\mathcal{Z}$ and $\mathcal{Q}$ denote the imaginary quadratic non-maximal order, the ring of integers and the field of rational numbers respectively. Let $D_1 < 0$ be a square free rational integer and set $D = \frac{4D_1}{r^2}$, where $r = 2$ if $D_1 \equiv 1 \bmod 4$ and $r = 1$ if $D_1 \equiv 2, 3 \bmod 4$. Then $K = \mathcal{Q}(\sqrt{D_1})$ is an imaginary quadratic field of discriminant D. Note that $K = \mathcal{Q}(\sqrt{D})$. If $\alpha, \beta \in K$, we denote by $[\alpha, \beta]$ the set $\alpha\mathcal{Z} + \beta\mathcal{Z}$. Then an order in K having conductor f with discriminant $D_f = f^2D$ is denoted by $O = [1, f\omega]$, where $\omega = \frac{D+\sqrt{D}}{2}$. An (integral) ideal A of O is a subset of O such that $\alpha + \beta \in A$ and $\alpha\lambda \in A$ whenever $\alpha, \beta \in A, \lambda \in O$. For $\alpha \in K, \alpha', N(\alpha)$ and $Tr(\alpha)$ denote the complex conjugate, norm and trace of α respectively. Let $\gamma = f\omega$. Then any ideal A of O (any O-ideal) is given by $A = [a, b + c\gamma]$, where $a, b, c \in \mathcal{Z}$, $a > 0, c > 0$, $c \mid a, c \mid b$ and $ac \mid N(b + c\gamma)$. If $c = 1$, then A is called primitive, which means that A has no rational integer factors other than 1(throughout this paper we may make use of primitive ideals only, because ideal multiplication always means ideal class multiplication containing the ideal). Then $A = [a, b + \gamma]$ is O -ideal if and only if a divides $N(b + \gamma)$. We say that A and B are equivalent ideals of O and denote $A \sim B$ if there exist non-zero $\alpha, \beta \in K$ such that $(\alpha)A = (\beta)B$ (this relation actually is equivalent relation). We denote the equivalence class of an ideal A by $\overline{A}$. Let $I(O)$ be the set of non-zero fractional ideals of O and $P(O)$ the set of non-zero principal ideals of O. Then $Cls(O) = I(O)/P(O)$ will be the class semigroup of the order O.

3. Structures of the class semigroup $Cls(O)$

In this chapter we construct the ideals using positive definite quadratic forms which are the generalizations of the facts, discussed by Cox[2], for quadratic forms, orders and ideals. And we will clarify the group $G_{\overline{E}_k}$ so that we can construct $Cls(O)$ explicitely. After then, we will correct some misconceptions concerning ideal equivalence appeared in Zanardo et al.[9] and explain why the cryptosystem proposed by Kim and Moon[8] can be broken easily. The reason is closely related to the misconceptions in Zanardo et al.[9]. In the sequel, we will set the quadratic form $f(x, y) = ax^2 + bxy + cy^2$ as (a, b, c) for brevity and call η the root of $f(x, y)$ if $f(\eta, 1) = 0$ and η lies in the upper half plane $\mathcal{H}$. We begin with introducing a lemma due to Cox[2].

Lemma 3.1.(Confer [2,Proposition 7.4]) Let O be an order in a imaginary quadratic field K, and let A be a fractional O-ideal. Then

$$\{\beta \in K \mid \beta A \subset A\} = O$$

if and only if A is invertible.

The generalization of Lemma 3.1 can be as following.

Lemma 3.2. Let $f(x, y) = (a, b, c)$ be a positive definite quadratic form with discriminant D_f, where $k = \gcd(a, b, c)$. Let η be the root of $f(x)$. Then $[a, a\eta]$ is invertible ideal if $k = 1$ and is non-invertible if $k > 1$ in the order $O = [1, \gamma]$ of K.

Proof. Firstly, we note that $[1, a\eta]$ is an order of K, since $a\eta$ is an algebraic integer. Now, we can show whether $[a, a\eta]$ is a invertible ideal or not in $[1, a\eta]$ according to $k = 1$ or not. For a given $\beta \in K$, $\beta[a, a\eta] \subset [a, a\eta]$ is equivalent to $\beta a \in [a, a\eta]$ and $\beta(a\eta) \in [a, a\eta]$. Since $a\beta$ belongs to $[a, a\eta]$, $a\beta = ma + n(a\eta)$, that is , $\beta = m + n\eta$ for some rational integers m and n.
Conversely, for any rational integers m and n, $a\eta(m+n\eta)$ clearly belongs

to $[a, a\eta]$. For the second, note that

$$\beta(a\eta) = ma\eta + na\eta^2 = ma\eta + n(-b\eta - c) = -nc + (ma - nb)\eta.$$

Thus, $\beta(a\eta) \in [a, a\eta]$ if and only if $a \mid nc$ and $a \mid nb$ and m is arbitrary. If $k = 1$, then $a \mid n$. However if $k > 1$, then $\gcd(a, b)$ and $\gcd(a, c) \geq k$. Therefore there exist an non-trivial divisor s of a and arbitrary rational integer m such that $a(m + s\eta) \in [a, a\eta]$. These facts tell us,

$$\{\beta \in K \mid \beta[a, a\eta] \subset [a, a\eta]\} = [1, a\eta]$$

if and only if $k = 1$. Therefore $[a, a\eta]$ is invertible in $[1, a\eta]$ if $k = 1$ and non-invertible if $k > 1$ by Lemma 3.1. Moreover, since f is the conductor of O with discriminant D_f, $a\eta = -\frac{b+fD}{2} + \gamma$. Since fD and b have the same parity, we have $\frac{b+fD}{2} \in \mathcal{Z}$. It follows that $[1, a\eta] = [1, \gamma]$ and thus $[a, a\eta] = [a, -\frac{b+fD}{2} + \gamma]$ is an O-ideal. □

Especially if $a = k$, then we denote the module $[k, k\eta]$ by E_k. For a quadratic form $f(x, y)$, let $f(x, y) = (ka_1, kb_1, kc_1) = kf_1(x, y)$ whenever $k = \gcd(a, b, c)$ from now on.

Corollary 3.3. For any divisor $k \mid f, E_k = [k, \gamma]$. Moreover, $E_k^2 = kE_k$, in other words $\overline{E}_k^2 = \overline{E}_k$.

Proof. Let $f(x, y) = (k, kb_1, kc_1)$ with discriminant D_f , where $f = kd, k = \gcd(k, kb_1, kc_1)$. Then $k\eta - \gamma \in k\mathcal{Z}$ since b_1 and dD are same parity. Therefore $[k, k\eta] = [k, \gamma]$. Clearly k divides $N(\gamma)$ so that E_k is an O-ideal. To prove the last claim, note that $E_k = E_k'$, since k devides $Tr(\gamma)$. From this fact and $k^2 | N(\gamma)$, we have

$$E_k^2 = E_k E_k' = [k, \gamma][k, \gamma'] = [k^2, k\gamma, k\gamma', N(\gamma)] = k[k, \gamma] = kE_k$$

and thus $\overline{E}_k^2 = \overline{E}_k$. □

We, now, introduce some facts due to Zanardo et al.[9] and Howie[5] below. In [9], Zanardo et al. described the structure of the class semigroup $Cls(O)$ explicitly. They, however, were wrong in defining the ideal equivalence. Therefore the structure of $Cls(O)$ was somewhat ambiguous. After dicussing some facts concerning the set of groups G's consisting of $Cls(O)$, we will clarify the structure of $Cls(O)$ by giving a theorem. We remind that the commutative semigroup $\mathcal{S}$ is called a Clifford commutative semigroup if one of the following equivalent statements holds(Confer [9] and [5,pp94-95 Theorem 2.1]).

C1) every element x of $\mathcal{S}$ is contained in a subgroup G of $\mathcal{S}$,

C2) every element x of $\mathcal{S}$ is regular, i.e. there exists $y \in \mathcal{S}$ such that $x = x^2 y$ (such an x is called von Neumann regular) ,

C3) $\mathcal{S}$ is a semilattice of groups.

And recall that a commutative semigroup $\mathcal{S}$ is the disjoint union of the subgroups of the form G_e generated by an idempotent e, where $G_e = \{x \in \mathcal{S} \mid xe = x \text{ and } xy = e \text{ for some } y \in \mathcal{S}\}$. Let us denote by $\mathcal{C}$ the set of idempotent elements of $Cls(O)$. Recall that a non-zero ideal E of O is called idempotent if $\overline{E}$ is idempotent as an element of $Cls(O)$, that is $E^2 = \lambda E$ for some $\lambda \in K$. Therefore E_k is idempotent and especially O is an idempotent element of itself and the subgroup $G_{\overline{O}}$ of $Cls(O)$ consists of the equivalence classes of invertible ideals of $E_1 = O$ since $k = 1$. Thus we shall write each element of $\mathcal{C}$ in the form $\overline{E}_k$, where $E_k = [k, \gamma]$ for a suitable divisor k of f and E_k is said to be a canonical representative for the class containing it. For an non-zero O-ideal $I = [a, b+\gamma]$, We now define an important quantity $\gcd(I) = \gcd(a, Tr(b+\gamma), \frac{N(b+\gamma)}{a})$. To complete the discussion for the structure of $Cls(O)$, let's characterize some properties of $\gcd(I)$.

Lemma 3.4. If $I = [a, b+\gamma]$ is a non-zero -ideal, then $\gcd(I)$ divides f.

Proof. Let $k = \gcd(I)$ for brevity. Since I is an primitive -ideal, a divides $N(b+\gamma)$, and thus $k = \gcd(a, Tr(b+\gamma), \frac{N(b+\gamma)}{a})$ divides a and $k^2 \mid N(b+\gamma)$ and $k|Tr(b+\gamma)$. If we choose an element $\theta = \frac{1}{k}(b+\gamma) \in K$, then $Tr(\theta) = \frac{1}{k}Tr(b+\gamma)$ and $N(\theta) = \frac{1}{k^2}N(b+\gamma)$, which are both rational integers, since $k^2 \mid N(b+\gamma)$ and $k \mid Tr(b+\gamma)$. Therefore θ is an algebraic integer and thus is contained in the maximal order $[1,\omega]$. Consequently k divides both b and f. □

Lemma 3.5.(Confer [9, Theorem 10, Proposition 13)
(a) Let $I = [a, b+\gamma]$ be a non-zero O-ideal and let $k = \gcd(I)$ and $E_k = [k,\gamma]$. Then we have $II' = aE_k, IE_k = kI$.
(b)The idempotents of $Cls(O)$ are the equivalence classes of ideals of the forms $E_k = [k,\gamma]$, where $k \in \mathcal{Z}$ divides f.

Lemma 3.6. (Confer Gauss[3, art.236])
Let A and B be O-ideals. Then $\gcd(AB) = lcm(\gcd(A), \gcd(B))$.

It is well-known that the cardinality of $Cls(O)$ is finite. Then we have the following.

Theorem 3.7. The class semigroup $Cls(O) = \cup_{k|f} G_{\overline{E_k}}$, where $G_{\overline{E_k}}$ is the set of all O-ideals A's such that $\gcd(A) = k$.

Proof. For any O-ideal $A = [a, b+\gamma]$ with $\gcd(A) = k$, $A^2A' = A(aE_k) = akA$ by Lemma 3.5 (a), that is $\overline{A} = \overline{A}^2\overline{A'}$. In other words $\overline{A}$ is von Neumann regular. Therefore $Cls(O)$ is a Clifford semigroup by the equivalence relation (C2). Equivalently $Cls(O)$ is a finitely disjoint union of groups of the form G_e's, where e is an idempotent element of $Cls(O)$. Moerover $Cls(O)$ has a semilattice structure (C3) with a homomorphism between groups. From Lemma 3.5(b), $\mathcal{C}= \{\overline{E_k} \mid k \mid f\}$. Then $G_{\overline{E_k}} = \{\overline{A} \mid \overline{AE_k} = \overline{A}$ and $\overline{AB} = \overline{E_k}$ for some $\overline{B} \in Cls(O)\}$. Let G be the set of all O-ideal A's such that $\gcd(A) = k$. We claim that $G_{\overline{E_k}} = G$. In fact; For any O-ideal A, $\gcd(A)$ divides f by Lemma 3.4. Suppose that $\gcd(A) = k$, then $\overline{AE_k} = \overline{A}$ and $\overline{AA'} = \overline{E_k}$ by

Lemma 3.5 (a). Therefore $\overline{A} \in G_{\overline{E_k}}$. Conversely suppose that $\overline{B} \in G_{\overline{E_k}}$ and $\gcd(B) = h$. Then $\overline{BB'} = \overline{E_k}$ by Lemma 3.5 (a). Note that $\gcd(A) = \gcd(A')$. Therefore $\gcd(AA') = \gcd(A)$ by Lemma 3.6. Therefore $h = \gcd(B) = \gcd(BB') = \gcd(E_k) = k$. This completes the proof □

Combining Lemma 3.6 and Theorem 3.7, we can see the following.

Corollary 3.8. If two ideal classes $\overline{A}$ and $\overline{B}$ belong to $G_{\overline{E}_k}$ and $G_{\overline{E}_h}$ respectively, then $\overline{AB}$ belongs to $G_{\overline{E}_l}$, where $l = lcm(k, h)$.

Now we discuss some facts concerning the ideal equivalence which was claimed by Zanardo et al.[9] and the secret key which was chosen by Kim and Moon[8]. By the facts discussed above we can see the following.

Remark 3.9. (a) Two ideals A and B are in the same group $G_{\overline{E}_k}$ if and only if $k = \gcd(A) = \gcd(B)$ by Theorem 3.7. In general the fact that two O-ideal A and B is equivalent if and only if $\gcd(A)$=$\gcd(B)$ (confer [9, p.387]) is not true. For example, suppose that O is an order with $D_1 = -6$ and $f = 5$. Then $D_f = -600$, $K = \mathcal{Q}(\sqrt{-6})$ and $O = [1, 5\sqrt{-6}]$. Then there are only two idempotents $\overline{O}$ and $\overline{E_5} = \overline{[5, 5\sqrt{-6}]}$ in $Cls(O)$. Therefore $Cls(O) = G_{\overline{O}} \cup G_{\overline{E_5}}$ and two ideal classes $\overline{E_5} = \overline{[5, 5\sqrt{-6}]}$ and $\overline{N} = \overline{[10, 5\sqrt{-6}]}$ belong to $G_{\overline{E_5}}$. Note that $\gcd(E_5) = \gcd(N) = 5$ and they are not equivalent.
(b) Analysis of Kim-Moon's key-exchange system
Kim and Moon proposed the following cryptosystem[8, Chapter 3.1, p492].
Two users Alice and Bob select a value D_f and a non-invertible ideal I in O. The value of D_f and ideal I made public.
1.Alice selects at random an integer x and computes a reduced ideal J

such that

$$J \sim I^x.$$

Alice sends J to Bob.

2. Bob selects at random an integer y and computes a reduced ideal M such that

$$M \sim I^y.$$

Bob sends M to Alice.

3. Alice computes a reduced ideal $U_1 \sim M^x$; Bob computes a reduced ideal $U_2 \sim J^y$.

Note that $U_1 \sim M^x \sim (I^y)^x = (I^x)^y \sim J^y \sim U_2$. Thus if $U_1 = [L(U_1), \alpha_1]$ and $U_2 = [L(U_2), \alpha_2]$, then Alice and Bob can use

$$\gcd(L(U_1), \frac{N(\alpha_1)}{L(U_1)}, Tr(\alpha_1)) = \gcd(L(U_2), \frac{N(\alpha_2)}{L(U_2)}, Tr(\alpha_2))$$

as their secret key.

The class $\overline{I}$ of the generator I in this system belongs to $G_{\overline{E_k}}$ for some divisor k of f. Then $\gcd(I) = k$. However, any power of I is equivalent to a unique reduced ideal T with the same $\gcd(T) = k$ since $\overline{T}$ belongs to $G_{\overline{E_k}}$ by Theorem 3.7. Therefore this cryptosystem becomes to be trivial.

References

[1] J. Buchmann, H. C. Willams, *A key exchange system based on imaginary quadratic fields*, J. Cryptology 1, pp.107-118,(1988).

[2] D. Cox,*Primes of the form $x^2 + ny^2$*, Wiley,New York, (1989).

[3] C. F. Gauss, *Disquisitiones Arithmeticae,* translated by Clarke A. A., Springer-Verlag, New York, (1986).

[4] R. Gilmer, *Multiplicative ideal theory,* Marcel Dekker, Inc. New York, (1972).

[5] J. M. Howie, *An introduction to semigroup theory,* Academic Press, New York,(1976).

[6] D. Hühnlein, J. J. Jr. Michael, S. Paulus and T. Tagaki, *A cryptosystem based on the non-maximal imaginary quadratic orders with fast decryption*, in Advanced Cryptology Eurocrypt '98, LNCS 1403, Springer-Verlag, Berlin, pp. 294-307,(1989).

[7] D. Hühnlein, T. Tagaki, *Reducing logarithms in the totally non-maximal imaginary quadratic orders*, in Advances in Cryptology - ASIACRYPTO '99, LNCS 1716, Springer-Verlag, Berlin, pp.219-231,(1999).

[8] H. Kim, S. Moon,*Public-Key Cryptosystems based on Class Semigroups of Imaginary Quadratic Non-maximal Orders*, ASISP 2003, LNCS 2727, pp.488-497,(2003).

[9] P. Zanardo, U. Zannier, *The class semigroup of orders in number fields*, Math. Proc. Camb.Phil. Soc. 115, pp. 379-391,(1994).

Yong Tae Kim
Department of Mathematics Education,
Gwangju National University of Education,
Gwangju, 500-703, Korea
E-mail: ytkim@gnue.ac.kr