ACTA ARITHMETICA
107.3 (2003)

Subrings in imaginary quadratic fields which are not universal for GE_2

by

Sheng Chen and Hong You (Harbin)

1. Introduction. Let R be a commutative ring with identity 1, R^* the group of units in R. Denote by $SL_n(R)$ and $E_n(R)$ the special linear groups and the subgroups of $SL_n(R)$ generated by elementary matrices respectively.

Let F be a number field and let S be a finite set of places containing S_∞, the set of infinite places in F. Denote by O_S the ring of S-integers of F, i.e., $O_S = \{x \in F \mid v(x) \geq 0 \text{ for } v \notin S\}$. If $S = S_\infty$, then O_S is the ring of integers of F. The study of $K_2(n, O_S)$ is related to the presentation of $E_n(O_S)$. We know that if $n \geq 3$, then $K_2(n, O_S) = K_2(O_S)$ and $E_n(O_S) = SL_n(O_S)$, and if O_S^* is infinite (i.e., $|S| > 1$), then the natural homomorphism from $K_2(2, O_S)$ to $K_2(n, O_S)$ $(n \geq 3)$ is surjective and $SL_2(O_S) = E_2(O_S)$ (cf. A. J. Hahn and O. T. O'Meara [7], W. van der Kallen [11], B. Liehl [14] and L. N. Vasershteĭn [17]).

It is known that K_2F consists of symbols (see [13]). However, this is not generally true for O_S. Denote by O_F the ring of integers of a quadratic field $F = \mathbb{Q}(\sqrt{d})$ and by d_F the discriminant of F. For $d > 0$, J. Browkin and J. Hurrelbrink [2] proved that K_2O_F is generated by symbols if and only if $d_F = 5, 8, 13$. T. Mulders [16] showed that if O_F contains nontorsion units, then it is often the case that K_2O_F is generated by Dennis–Stein symbols. On the other hand, K. Hutchinson [8] showed that K_2O_F, where $F = \mathbb{Q}(\sqrt{-34}, \sqrt{-206})$, cannot be generated by Dennis–Stein symbols, although O_F^* is infinite.

For $K_2(2, O_S)$, the explicit computations are quite rare. However, P. M. Cohn [3, 4] determined $K_2(2, O_F)$ completely, where O_F is the ring of integers of an imaginary quadratic field. In particular, it is proved that except for $d_F = -7$, -8, -11, $K_2(2, O_F)$ is generated by symbols as a normal subgroup of $St(2, O_F)$. F. Kirchheimer and J. Wolfart [12] computed $K_2(2, O_F)$, where O_F is the real quadratic field with $d_F = 5$, 8, 12, 13. By the stability

2000 *Mathematics Subject Classification*: Primary 19F15; Secondary 11R11.

result of W. van der Kallen [11] and results in [2, 12], it can be seen that if O_F is the ring of integers of a real quadratic field, then O_F is universal for GE_2 if and only if $d_F = 5$, 8, 13, although O_F^* is infinite.

Let v be a finite place outside S, $S' = S \cup \{v\}$, $R = O_S$ and $R' = O_{S'}$. Suppose that the prime ideal P in R corresponding to v is principal and the natural homomorphism $R^* \to (R/P)^*$ is surjective. E. Abe and J. Morita [1] showed that if R is universal for GE_2, then so is R'. This raises the question of whether the result is still true if P is nonprincipal.

The purpose of this note is to answer this question in the negative. In fact, we prove the following result.

Theorem 1. *Let* $F = \mathbb{Q}(\sqrt{d})$ *and let* p *be a prime number, and* $n \geq 2$. *Suppose that* d *is one of the following forms*:

(a) $d = -p(p^n + 1)$, *here* $n \neq 3$ *if* $p = 2$;
(b) $d = -p(p^n - 1)$;
(c) $d = -(p^n + 1)$, *here* $p = 2$ *and* $n \neq 3$;
(d) $d = -(p^n - 7)$, *here* $p = 2$ *and* $n \geq 6$, $n \neq 7, 15$.

Then $K_2(2, O_F[1/p])$ *cannot be generated by symbols, i.e.,* $O_F[1/p]$ *is not universal for* GE_2, *where* O_F *denotes the ring of integers in* $F = \mathbb{Q}(\sqrt{d})$.

2. Preliminaries. For any associative ring R with 1, denote by $St(n, R)$ ($n \geq 2$) the *Steinberg group* over R, i.e., the group with generators $x_{ij}(r)$ with $r \in R$, and i, j distinct integers between 1 and n, and subject to the relations

$$x_{ij}(r)x_{ij}(s) = x_{ij}(r + s), \tag{1}$$

$$[x_{ij}(r), x_{kl}(s)] = \begin{cases} x_{il}(rs) & \text{if } j = k,\ i \neq l, \\ 1 & \text{if } j \neq k,\ i \neq l, \end{cases} \tag{2}$$

$$w_\alpha(t)x_{-\alpha}(r)w_\alpha(t)^{-1} = x_\alpha(-trt) \tag{3}$$

where $w_\alpha(t) = x_\alpha(t)x_{-\alpha}(-t^{-1})x_\alpha(t)$, $\alpha = ij$, $-\alpha = ji$, $r, s \in R$ and $t \in R^*$. For $n \geq 3$ only the relations (1) and (2) are needed. When $n = 2$, the relation (2) is vacuous.

There is a natural surjective map $\phi_n : St(n, R) \to E_n(R)$ sending $x_{ij}(r)$ to $e_{ij}(r)$. Denote by $K_2(n, R)$ the kernel of ϕ_n and by $K_2(R)$ the direct limit of $K_2(n, R)$ ($n \geq 2$).

Now suppose that R is a commutative ring. Given a pair of units u and v, one can construct the universal symbol $\{u, v\}_\alpha$, called the *symbol* in the sequel, as follows:

$$\{u, v\}_\alpha = h_\alpha(uv)h_\alpha(u)^{-1}h_\alpha(v)^{-1},$$

where $h_\alpha(u) = w_\alpha(u)w_\alpha(-1)$.

Now we recall the definition of a ring to be universal for GE_2 (see [3]). For any $a \in R$, $u, v \in R^*$, write

$$E(a) = \begin{pmatrix} a & 1 \\ -1 & 0 \end{pmatrix}, \quad [u, v] = \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix}, \quad D(u) = [u, u^{-1}].$$

We shall write $E(2, R)$ for the group generated by all $E(a)$, $D_2(R)$ for the group generated by all $[u, v]$, and $GE_2(R)$ for the group generated by $E(2, R)$ and $D_2(R)$. It is easy to see that $E_2(R) = E(2, R)$.

We have the relations

$$E(a)E(0)E(b) = -E(a+b), \quad \text{where } a, b \in R, \tag{4}$$

$$E(u)E(u^{-1})E(u) = -D(u), \tag{5}$$

$$E(a)[u, v] = [v, u]E(v^{-1}au), \quad \text{where } a \in R \text{ and } u, v \in R^*. \tag{6}$$

In addition we have certain obvious relations in $D_2(R)$, expressing it effectively as the direct product of two copies of R^*. The relations (4)–(6) together with the relations in $D_2(R)$ are called the *universal relations* for $GE_2(R)$. When they constitute a complete set of defining relations, R is said to be *universal* for GE_2. That R is universal for GE_2 is equivalent to the condition that $K_2(2, R)$ is generated by symbols as a normal subgroup of $St(2, R)$ (cf., R. K. Dennis and M. R. Stein [5]). Some examples of rings which are not universal for GE_2 are given in [6].

3. Proof of Theorem. Let R and S be any commutative rings with 1. An additive group homomorphism $f : R \to S$ is said to be a *U-homomorphism* if $f(1) = 1$ and $f(ux) = f(u)f(x)$ for all $x \in R$, $u \in R^*$ (see [3, p. 39]).

LEMMA 2 [3, Th. 11.2]. *Suppose that R and S are commutative rings with 1 and R is universal for GE_2. If $f : R \to S$ is a U-homomorphism, then f induces a group homomorphism $f^* : GE_2(R) \to GE_2(S)$ by the rule*

$$E(r) \mapsto E(f(r)), \quad [u, v] \mapsto [f(u), f(v)].$$

LEMMA 3. *Suppose that R and S are commutative rings with 1 and there exist a U-homomorphism f from R to S and $a, b \in R$ such that $u = 1 + ab \in R^*$ and $1 + f(a)f(b) \neq f(u)$. Then R is not universal for GE_2.*

Proof. Suppose that R is universal for GE_2. Let f^* be the induced homomorphism in Lemma 2. Note that in $GE_2(R)$,

$$E\left(\frac{b}{u}\right)E(a)E(-b)E\left(-\frac{a}{u}\right) = [u^{-1}, u]. \tag{7}$$

In $GE_2(S)$, we have

$$E\left(\frac{f(b)}{f(u)}\right)E(f(a))E(-f(b))E\left(-\frac{f(a)}{f(u)}\right) = [f(u)^{-1}, f(u)]. \tag{8}$$

Direct computation will show that the $(2,2)$-entries on the two sides of (8) are $1 + f(a)f(b)$ and $f(u)$ respectively. By the assumption, this is a contradiction. ∎

LEMMA 4 [15]. *Let p be a prime number and $n \geq 2$. If $p \neq 2$ or $n \neq 3$, then the Diophantine equation*

$$x^2 = p^n \pm 1$$

has no solution x in $\mathbb{Z}$.

REMARK 1. From the lemma above we know that $p^n + 1$ $(n \geq 2)$ is a square if and only if $p = 2$ and $n = 3$.

LEMMA 5 [10]. *If $n \geq 6$, $n \neq 7, 15$, then the Diophantine equation*

$$x^2 = 2^n - 7$$

has no solution x in $\mathbb{Z}$.

Now let us recall some basic facts on imaginary quadratic fields (see [9]). Suppose that $-d$ is a nonsquare positive integer and $d = d_1 d_2^2$, where d_1 is square-free, and d_2 is a positive integer. Then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d_1})$.

If $d_1 \equiv 2, 3 \pmod 4$, then $d_F = 4d_1$ and $O_F = \mathbb{Z} + \mathbb{Z}\omega$, where $\omega = \sqrt{d_1}$.

If $d_1 \equiv 1 \pmod 4$, then $d_F = d_1$ and $O_F = \mathbb{Z} + \mathbb{Z}\omega$, where $\omega = (1 + \sqrt{d_1})/2$.

Let p be a prime number and P a prime ideal in O_F containing p. If p is odd and $p \mid d_F$, then $P = (p, \sqrt{d_1})$ and $P^2 = (p)$. If $p = 2$ and $2 \mid d_F$, then $d_1 \equiv 2, 3 \pmod 4$ and $P^2 = (p)$, where $P = (2, \sqrt{d_1})$ if $d_1 \equiv 2 \pmod 4$, and $P = (2, 1 + \sqrt{d_1})$ if $d_1 \equiv 3 \pmod 4$.

LEMMA 6. *Let $F = \mathbb{Q}(\sqrt{d_1})$, where d_1 is a square-free negative integer. Assume that a prime number p ramifies in F, $(p) = P^2$. If* (i) *d_1 is composite, or* (ii) *$d_1 \leq -3$ and $p = 2$, then the ideal P is not principal.*

Proof. Suppose that the ideal P is principal, $P = (\alpha)$, where $\alpha \in O_F$. Then taking norms we get $p = N(P) = N(\alpha)$.

If $d_1 \equiv 2, 3 \pmod 4$, then $\alpha = a + b\sqrt{d_1}$, where $a, b \in \mathbb{Z}$, $b \neq 0$.

If $d_1 \equiv 1 \pmod 4$, then $\alpha = \frac{1}{2}(a + b\sqrt{d_1})$, where $a, b \in \mathbb{Z}$, $b \neq 0$, $a \equiv b \pmod 2$.

Hence $N(\alpha) = p$ gives

$$a^2 - d_1 b^2 = p \quad \text{if } d_1 \equiv 2, 3 \pmod 4, \tag{9}$$

$$a^2 - d_1 b^2 = 4p \quad \text{if } d_1 \equiv 1 \pmod 4. \tag{10}$$

If $p = 2$ is ramified in F, then $d_1 \equiv 2, 3 \pmod 4$ and (9) implies that $-d_1 \leq -d_1 b^2 \leq p = 2$. This contradicts assumptions (i) and (ii).

Thus p is odd, and $p \mid d_1$ since p ramifies in F. From (9) and (10) it follows that $p \mid a$, consequently (9) and (10) take the form

$$p\left(\frac{a}{p}\right)^2 - \frac{d_1}{p}\, b^2 = 1 \text{ or } 4. \tag{11}$$

Since d_1 is composite and $b \neq 0$, we have $-(d_1/p)b^2 \geq -d_1/p \geq 2$. The first case of (11) is impossible. In the second case we have $d_1 \equiv 1 \pmod 4$, hence $4 \geq -(d_1/p)b^2 \geq -d_1/p \geq 3$, thus $b^2 = 1$. Then $a \equiv b \pmod 2$ implies that a is odd. Consequently $p(a/p)^2 \geq p \geq 3$, and $4 = p(a/p)^2 - (d_1/p)b^2 \geq 3+3$, contradiction. ∎

LEMMA 7. *Let F, p, and P be as in Lemma 6. Then the mapping $f : O_F[1/p] \to \mathbb{Z}[1/p]$ defined by $a + b\omega \mapsto a + b$, where $a, b \in \mathbb{Z}[1/p]$, is a U-homomorphism.*

Proof. Since the ideal P is not principal in O_F, it follows that $O_F[1/p]^*$ is a multiplicative group generated by -1 and p. Thus $O_F[1/p]^* = \mathbb{Z}[1/p]^*$. Since the mapping f is $\mathbb{Z}[1/p]$-linear, it is a U-homomorphism. ∎

Now let us complete the proof of Theorem 1.

Let f be the U-homomorphism of Lemma 7. By Lemma 3, it is sufficient to show that there exist $s, t \in R = O_F[1/p]$ such that $1 + st = u \in R^*$ and $1 + f(s)f(t) \neq f(u)$.

Since $\omega = \sqrt{d_1}$ or $\frac{1}{2}(1 + \sqrt{d_1})$, we get $\sqrt{d_1} = \omega$ or $2\omega - 1$. Hence $f(\sqrt{d_1}) = 1$ in both cases. Consequently, $f(\sqrt{d}) = f(d_2\sqrt{d_1}) = d_2$.

In cases (a) and (b) of Theorem 1 we have $d = -p(p^n + \varepsilon)$, where $\varepsilon = \pm 1$, and its maximal square-free divisor d_1 is composite in view of Lemma 4. Let $s = \sqrt{d}/p$ and $t = \sqrt{d}/p^n$. Then

$$u = 1 + st = 1 + \frac{d}{p^{n+1}} = -\frac{\varepsilon}{p^n} \in R^*.$$

Now, $f(s) = d_2/p$ and $f(t) = d_2/p^n$, hence $1 + f(s)f(t) = 1 + d_2^2/p^{n+1} > 1$, and $f(u) = u = -\varepsilon/p^n < 1$. Contradiction.

In case (c) of Theorem 1 we have $d = -(2^n + 1)$ and $d_1 \leq -3$ in view of Lemma 4. Let $s = \sqrt{d}$ and $t = \sqrt{d}/2^n$. Then

$$u = 1 + st = 1 + \frac{d}{2^n} = -\frac{1}{2^n} \in R^*.$$

Now, $f(s) = d_2$ and $f(t) = d_2/2^n$, hence $1 + f(s)f(t) = 1 + d_2^2/2^n > 0$ and $f(u) = u = -1/2^n < 0$. Contradiction.

In case (d) of Theorem 1 we have $d = -(2^n - 7)$ and $d_1 \leq -3$ in view of Lemma 5. Since $d \equiv 3 \pmod 4$, 2 should ramify in $F = \mathbb{Q}(\sqrt{d})$, and $(2) = P^2$.

So P is not principal by Lemma 6. Let $s = \sqrt{d} - 3$ and $t = \frac{1}{2}(\sqrt{d} + 3)$. Then

$$u = 1 + st = 1 + \frac{1}{2}(d - 9) = \frac{1}{2}(d - 7) = -2^{n-1} \in O_F\left[\frac{1}{2}\right]^*.$$

Now, $f(s) = d_2 - 3$ and $f(t) = \frac{1}{2}(d_2 + 3)$, then $f(s)f(t) = \frac{1}{2}(d_2^2 - 7) > -4 > f(u) = u$. Contradiction.

Thus in all cases $1 + f(s)f(t) \neq f(u)$. ■

4. Example. Let $F = \mathbb{Q}(\sqrt{d})$, where $d = -(2^n + 1)$, $n \neq 3$ and $R = O_F = O_{S_\infty}$. Suppose that v is the finite place in F corresponding to the prime ideal P in O_F containing $p = 2$. Let $S' = S_\infty \cup \{v\}$, and $R' = O_{S'} = O_F[1/2]$. Note that if $n = 2$, then $d = -5$ and $d_F = -20$, and if $n \geq 4$, then $d \equiv -1 \pmod 8$, d_2 is odd, $d_2^2 \equiv 1 \pmod 8$ and $d_1 \equiv -1 \pmod 8$. In either case $d_F \neq -7,-8,-11$, so R is universal for GE_2. Although the natural homomorphism $R^* \to (R/P)^* \simeq (\mathbb{Z}/2\mathbb{Z})^*$ is surjective, R' is not universal for GE_2.

Acknowledgements. The authors would like to thank the referee for many valuable suggestions to the earlier version of the paper. The work is supported by the National Natural Science Foundation of China, the Natural Science Foundation of Heilongjiang Province in China and Project HIT.2001.41 of the Scientific Research Foundation of Harbin Institute of Technology.

References

[1] E. Abe and J. Morita, *Some Tits systems with affine Weyl groups in Chevalley groups over Dedekind domains*, J. Algebra 115 (1988), 450–465.

[2] J. Browkin and J. Hurrelbrink, *On the generation of $K_2(O)$ by symbols*, in: Lecture Notes in Math. 1046, Springer, 1982, 29–31.

[3] P. M. Cohn, *On the structure of GL_2 of a ring*, Inst. Hautes Études Sci. Publ. Math. 30 (1966), 5–53.

[4] —, *A presentation of SL_2 of Euclidean imaginary quadratic number fields*, Mathematika 15 (1968), 156–163.

[5] R. K. Dennis and M. R. Stein, *The functor K_2: a survey of computations and problems*, in: Lecture Notes in Math. 342, Springer, 1973, 243–280.

[6] —, —, *K_2 of radical ideals and semilocal rings revisited*, in: Lecture Notes in Math. 342, Springer, 1973, 281–303.

[7] A. J. Hahn and O. T. O'Meara, *The Classical Groups and K-Theory*, Springer, 1989.

[8] K. Hutchinson, *Conditions under which $K_2(\mathcal{O}_F)$ is not generated by Dennis–Stein symbols*, Acta Arith. 89 (1999), 189–199.

[9] K. Ireland and M. Rosen, *A Classical Introduction to Number Theory*, Springer, 1982.

[10] W. Johnson, *The Diophantine equation $x^2 + 7 = 2^n$*, Amer. Math. Monthly 94 (1987), 59–62.

[11] W. van der Kallen, *Stability for K_2 of Dedekind rings of arithmetic type*, in: Lecture Notes in Math. 854, Springer, 1981, 217–248.
[12] F. Kirchheimer und J. Wolfart, *Explizite Präsentation gewisser Hilbertscher Modulgruppen durch Erzeugende und Relationen*, J. Reine Angew. Math. 315 (1980), 139–173.
[13] H. W. Lenstra, Jr., *K_2 of a global field consists of symbols*, in: Lecture Notes in Math. 551, Springer, 69–73.
[14] B. Liehl, *On the group SL_2 over orders of arithmetic type*, J. Reine Angew. Math. 323 (1981), 153–171.
[15] L. J. Mordell, *Diophantine Equations*, Academic Press, 1969.
[16] T. Mulders, *Generating the tame and wild kernels by Dennis–Stein symbols*, K-Theory 5 (1992), 449–470.
[17] L. N. Vasershteĭn, *On the group SL_2 over Dedekind rings of arithmetic type*, Mat. Sb. 89 (1972), 313–322.

Department of Mathematics
Harbin Institute of Technology
Harbin 150001, P.R. China
E-mail: hyou@hope.hit.edu.cn

Received on 10.12.2001
and in revised form on 18.3.2002 (4167)