Elementary Proof of 'The Class Number of Q(√e) is odd when l is prime,

Elementary Proof of 'The Class Number of $Q(\sqrt{\ell})$ is odd when ℓ is prime,

Akira TAKAKU*

1. It is well known that the class number** of a real quadratic field $Q(\sqrt{\ell})$ is odd when ℓ is prime. This fact readily proved by applying the genus theory for $\ell \equiv 1 \pmod 4$ and by applying the class field theory for $\ell \equiv 3 \pmod 4$. (Redei and Reichardt [1] treated more general cases.) In this note, we give an elementary proof without applying the class field theory in the case $\ell \equiv 3 \pmod 4$. It is also possible to prove the fact in the case $\ell \equiv 1 \pmod 4$ by our method. In § 2 we prove some preliminary lemmas and in § 3 we give our proof.

NOTATIONS : we denote by **Z**,**Q** the ring of rational integers and the rational number field, respectively. Let a,b be integers, then we denote by (a,b) the highest common facror of a and b.

2. Preliminary.

Let m be a positive square-free integer. Let $d=d(m)$ and $h=h(m)$ be the discriminant and the class number of a real quadratic field $K=Q(\sqrt{m})$, respectively. For an integral basis of K,we take 1, ω where $\omega=\sqrt{m}$ if $m\equiv 2,3 \pmod 4$ and $\omega=(-1+\sqrt{m})/2$ if $m\equiv 1 \pmod 4$ and we fix it. If an ideal A of K has an integral basis $a, b+c\omega$ $(a,b,c \in Z)$, then we write $A=[a, b+c\omega]$. Any ideal A is expressed by a product of a rational integer and a primitive ideal. If ideals A and B are in the same class, then we denote $A \sim B$.

LEMMA 1. *Let* $A=[a,b+\omega]$, $B=[c,e+\omega]$ *be two primitive ideals of* $K=Q(\sqrt{m})$. *Then* $A\sim B$ *if and only if there exists an modular transformation* $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ (*i.e.*, $\det \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \pm 1$, $p,q,r,s \in Z$) *such that*

$$\frac{b+\omega}{a} = \left(p\,\frac{e+\omega}{c}+q\right)\Big/\left(r\,\frac{e+\omega}{c}+s\right).$$

Proof. See [2,Theorem 5.27], for instance.

Let $z_1, z_2 \in Q(\sqrt{m})$. If there exists a modular transformation $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ such that $z_2=(pz_1+q)/(rz_1+s)$, then we say that z_1 and z_2 are equivalent to each other and write $z_1 \sim z_2$.

LEMMA 2. *Any element of* $Q(\sqrt{m})$ *is equivalent to an element* $x+y\sqrt{m}$ *of Gm.*

Received October 31, 1974

* Dept. of Math., Sci.& Eng. Div., Ryuku Univ.

** This is the class number in wide sense.

Here Gm is a set of the form $x + y\sqrt{m}$:
(G*m*) $-1/2 \leq x < 1/2,\ 0<y,\ x^2 - my^2 \leq -1$,
where $-1/2 \leq x \leq 0$ *if* $x^2 - my^2 = -1$.

Proof. The proof of Lemma 2 is similar to the case in which we determine a fundamental region of the modular group operating on the complex upper halfplane. See [2, Theorem 2.13], for instace.

LEMMA 3. *Let* ℓ *be a prime. If* $\ell \equiv 3 \pmod 8$ (*resp.* $\ell \equiv 7 \pmod 8$)), *then eqn* $X^2 - \ell Y^2 = 2$(*resp.* $X^2 - \ell Y^2 = -2$) *has no solution.*

Proof. Let $\ell \equiv 3 \pmod 8$. Since $(\ell^2 - 1)/8 \equiv 1 \pmod 2$, the Kronecker symbol $(8 \mid \ell) = -1$. ℓ is prime in a real quadratic field $\mathbf{Q}(\sqrt{2})$. Hence eqn $\ell Y^2 = (X+\sqrt{2})(X-\sqrt{2})$ has no solution. In the case $\ell \equiv 7 \pmod 8$, the proof is similar.

LEMMA 4. *If a prime* $\ell \equiv 3 \pmod 4$, *then* $[2, -1+\sqrt{\ell}] \sim [1, \sqrt{\ell}]$.

Proof. We prove only the case $\ell \equiv 3 \pmod 8$, the proof of the case $\ell \equiv 7 \pmod 8$ is similar. Eqn $X^2 - \ell Y^2 = 1$ has a solution $\{X, Y\} = \{x_0, y_0\}$ such that $y_0 \neq 0$ (for example, take the fundamental unit of $\mathbf{Q}(\sqrt{\ell})$). Since $\ell y_0^2 = (x_0 + 1)(x_0 - 1) \neq 0$, there are integers y_1, y_2 such that $y_0 = y_1 y_2$ and (i) $\ell y_1^2 = x_0 - 1, y_2^2 = x_0 + 1$ or (ii) $\ell y_1^2 = x_0 + 1, y_2^2 = x_0 - 1$. In the case (i), we have $y_2^2 - \ell y_1^2 = 2$, but this contradicts Lemma 3. Hence the case (ii) holds. We have $y_2^2 - \ell y_1^2 = -2$. Put $s = y_2$, $r = y_1$, $p = (y_2 - y_1)/2$ and $q = (\ell y_1 - y_2)/2$. Since y_1, y_2 are odd, p, q are integers. Then we have $\det \begin{pmatrix} p & q \\ r & s \end{pmatrix} = -1$ and $(-1 + \sqrt{\ell})/2 = (p\sqrt{\ell} + q)/(r\sqrt{\ell} + s)$. By Lemma 1, $[2, -1+\sqrt{\ell}] \sim [1, \ell]$.

LEMMA 5. *Let* $\ell \equiv 3 \pmod 4$ *be a prime and* $A = [a, -b+\sqrt{\ell}]$ $(a \geq 3,\ b > 0)$ *be an ideal of the real quadratic field* $K = \mathbf{Q}(\sqrt{\ell})$. *Suppose* $(-b+\sqrt{\ell})/a \in G_\ell$. *Then* $[a, -b + \sqrt{\ell}] \sim [a, b+\sqrt{\ell}]$ *if and only if the following condition* (*) *is satisfied.* (*) *Eqn* $X^2 - \ell Y^2 = a^2$ *has a solution* $\{x_0, y_0\}$ *such that* $(x_0, y_0) = 1$ *if a is odd,* $(y_0, a) = 2$ *if a is even and*

(i) $x_0 - by_0 \equiv 0 \pmod a$,

(ii) $\ell y_0 - bx_0 \equiv 0 \pmod a$.

Proof. We first prove preliminary facts in (I), (II). (I) We have $b/a < 1/2$. In fact, if $b/a = 1/2$, then $b^2 - \ell \equiv 0 \pmod{2b}$. Hence $\ell \equiv 0 \pmod b$ and we have $b=1$ or ℓ. If $b=1$, then $a=2$, this contradicts our assumption $a \geq 3$. If $b = \ell$, then $a = 2\ell$ and $(-b+\sqrt{\ell})/a \notin G_\ell$, this contradicts our assumption. (II) We have $(b^2 - \ell)/a^2 \neq -1$. In fact, if above equality holds, then $\ell = a^2 + b^2 \equiv 1$ or $2 \pmod 4$. Since $\ell \equiv 3 \pmod 4$, this is impossible. From (I), (II), we have $(b+\sqrt{\ell})/a \in G_\ell$ and $(b^2-\ell)/a^2 \neq -1$. (III) Let $[a, -b+\sqrt{\ell}] \sim [a, b+\sqrt{\ell}]$. Our proof is divided into three parts (A), (B), (C). (A) Let $z=(b+\sqrt{\ell})/a$. By Lemma 1, there exists a modular transformation $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ such that $-\bar{z}=(pz+q)/(rz+s)$. Here $\bar{z}$ is the complex conjugate of z. We have

(1) $\quad rz\bar{z}+s\bar{z}+pz+q=0,$

hence $p=s$. Substituting $z\bar{z}=(b^2-\ell)/a$ and $z+\bar{z}=2b/a$ into the formula (1), we have

(2) $\quad -q=r\dfrac{b^2-\ell}{a^2}+\dfrac{2pb}{a}.$

Therefore $\pm 1=\det\begin{pmatrix} p & q \\ r & s \end{pmatrix}=p^2-qr=(p+br/a)^2-\ell r^2/a^2$, i.e., p, r satisfy

$$(ap+br)^2-\ell r^2=\pm a^2.$$

Now we put $x_0=ap+br$, $y_0=r$. An equation

$$X^2-\ell Y^2=\pm a^2$$

has a solution $\{x_0, y_0\}$ for one of $\pm$. But eqn $X^2-\ell Y^2=-a^2$ has no solution. In fact, if $X^2-\ell Y^2=-a^2$ has a solution $\{X, Y\}$, then $\ell Y^2=(X+a\sqrt{-1})(X-a\sqrt{-1})$. As $(-4 \mid \ell)=-1$, ℓ is prime in $\mathbf{Q}(\sqrt{-1})$. Hence $a\equiv 0 \pmod{\ell}$ and $\sqrt{\ell}/a<1$. Hence $(-b+\sqrt{\ell})/a \notin G_\ell$, this contradicts our assumption. Therefore $\{x_0, y_0\}$ is a solution of

$$X^2-\ell Y^2=a^2.$$

(B) If $(x_0, y_0)>1$, then $(y_0, a)=2$. Hence in this case, a is even. In fact, assume that there exists a prime ℓ_1 such that $\ell_1 \mid (y_0, a)$. We treat two cases (B_1) $\ell_1\neq 2$ and (B_2) $\ell_1=2$. (B_1) Let $\ell_1\neq 2$. From the fromula (2) of(A), we have

$$-aq=y_0\frac{b^2-\ell}{a}+2pb.$$

Hence $2pb\equiv 0 \pmod{\ell_1}$. We have $(a, b)=1$. In fact, if there is a prime ℓ_2 such that $\ell_2 \mid (a, b)$, then $b^2\equiv \ell \pmod{\ell_2}$ since $b^2\equiv \ell \pmod{a}$. Hence $\ell_2=\ell$ and $\ell=\ell_2<|b|<2a$. If $\ell=3$, there is not an ideal $[a, -b+\sqrt{\ell}]$ such that $a\geq 3$, $b>0$ and $(-b+\sqrt{\ell})/a \in G_\ell$. If $\ell\neq 3$, then we have $(-b+\sqrt{\ell})/a \notin G_\ell$. Therefore we have $(p, \ell_1)=\ell_1$. Hence $\det\begin{pmatrix} p & q \\ r & s \end{pmatrix}=\det\begin{pmatrix} p & q \\ y_0 & s \end{pmatrix}\equiv 0 \pmod{\ell_1}$, this is a contradiction. (B_2) Let $\ell_1=2$. If there exist a prime $\ell_2\neq 2$ such that $\ell_2 \mid (y_0, a)$, then the proof is reduced to the above case (B_1). We may assume that (y_0, a) is a power of 2. But we have $a\not\equiv 0 \pmod{4}$. (In fact, if $a\equiv 0 \pmod{4}$, then we have $b^2\equiv \ell\equiv 3 \pmod{4}$ since $b^2\equiv \ell \pmod{a}$. This is impossible.) Hence $(y_0, a)=2$. Since $r=y_0$ and $ap+br=x_0$, we have $x_0-by_0\equiv 0 \pmod{a}$. From (2), we have $-\ell y_0+2bx_0-b^2y_0\equiv 0 \pmod{a}$. Hence $-\ell y_0+bx_0\equiv 0 \pmod{a}$. (C) Let $(x_0, y_0)=1$, then a is odd. In fact, if a is even, we have $4(a/2)^2=(x_0+y_0\sqrt{\ell})(x_0-y_0\sqrt{\ell})$. Let P be a prime ideal of

$Q(\sqrt{\ell})$ such that $(2)=P^2$, then $P^2 \mid x_0+y_0\sqrt{\ell}$ or $P^2 \mid x_0-y_0\sqrt{\ell}$. In any case, we have $2 \mid (x_0, y_0)$. This contradicts our assumption. The proof that $\{x_0, y_0\}$ satisfies eqns (i), (ii) of Lemma 5 is similar to the case (B). Sufficiency part of Lemma 5 is provd in § 3.

3. Proof.

By Lemma 1 and 2, we may count non equivalent ideals $A=[a, b+\sqrt{\ell}]$ of $Q(\sqrt{\ell})$ such that $a>0$ and $(b+\sqrt{\ell})/a \in G\ell$. (i) If $b=0$ and $(-b+\sqrt{\ell})/a \in G\ell$, then ideal $[a, -b+\sqrt{\ell}]=[1, \omega]$. If $a<3$ and $(-b+\sqrt{\ell})/a \in G\ell$, then $[a, -b+\sqrt{\ell}]=[1, \omega]$ or $[2, -1+\sqrt{\ell}]$. (In fact, we have $a=1$ or 2. If $a=1$, then $|b/a| \leqq 1/2$ and $b=0$. If $a=2$, then $b=0$ or $b=1$. Since $b^2 \equiv \ell \pmod a$, b is odd. Hence $b=1$.) By Lemma 4, $[2, -1+\sqrt{\ell}] \sim [1, \sqrt{\ell}]$,i.e., these two ideals are in the principal class. (ii) Let $[a, -b+\sqrt{\ell}]$ be an ideal such that $a \geq 3$, $b>0$ and $(-b+\sqrt{\ell})/a \in G\ell$. Then if we prove

$$[a, -b+\sqrt{\ell}] \sim [a, b+\sqrt{\ell}] \longleftrightarrow [a, -b+\sqrt{\ell}] \sim [2, -1+\sqrt{\ell}],$$

then our conclusion is obtained. The sufficiency part ($\Leftarrow$) is obvious. To prove the necessity part ($\Rightarrow$), we may prove the following lemma, since the necessity part of Lemma 5 holds. The following lemma also prove the sufficiency part of Lemma 5.

LEMMA 6. *Let $\ell \equiv 3 \pmod 4$ be a prime. Let $A=[a, -b+\sqrt{\ell}]$ be an ideal of $Q(\sqrt{\ell})$ such that $a \geq 3$, $b>0$ and $(-b+\sqrt{\ell})/a \in G\ell$. If the condition (*) of Lemma 5 holds, then $[a, -b+\sqrt{\ell}] \sim [2, -1+\sqrt{\ell}]$.*

Proof. Let $\{x_0, y_0\}$ be a solution of eqn $X^2-\ell Y^2=a^2$ which satisfies the condition (*) of Lemma 5. (I) Let a be even, i.e., $(y_0, a)=2$. If $a=2$, then $b=1$. Hence we may assume $a \neq 2$. We have $a \not\equiv 0 \pmod 4$ since eqn $X^2 \equiv \ell \equiv 3 \pmod 4$ has no solution. From $\ell y_0^2=(x_0+a)(x_0-a) \neq 0$, there exist positive integers y_1, y_2 snch that $y_0=y_1 y_2$ and (A) $\ell y_1^2=x_0+a, y_2^2=x_0-a$ or (B) $\ell y_1^2=x_0-a, y_2^2=x_0+a$. We treat only about the case (A) and write (resp....) about the corresponding fact of the case (B). Since $(y_0, a)=2$, we have $(x_0, a)=2$ and $(y_1, a)=(y_2, a)=2$. We have

(3) $\quad y_2^2-\ell y_1^2=-2a$ (resp. $y_2^2-\ell y_1^2=2a$.)

Put $r=y_1$, $s=(y_1+y_2)/2$. From the formula (3), y_1 and y_2 are both even or both odd. Hence $s \in Z$. From eqn (i) of the condition (*) of Lemma 5, we have

$$x_0-by_0 \equiv y_2(y_2-by_1) \equiv 0 \pmod a.$$

Put $a=2a_1$, then we have $(y_2, a_1)=1$ since $(a_1, 2)=1$. Hence

(4) $\quad y_2-by_1 \equiv 0 \pmod{a_1}$.

From eqn (ii) of the condition (*) of Lemma 5, we have $y_2(\ell y_1-by_2) \equiv 0 \pmod a$. Hence

(5) $\quad \ell y_1-by_2 \equiv 0 \pmod{a_1}$.

Put $p=(-rb-r+2s)/a, q=(-r+2s+r\ell-2bs)/(2a)$. From the formulas (4), (5), we have

$$-r+2s+r\ell-2bs=y_0(\ell-1)+(y_1+y_2)(1-b)\equiv 0 \pmod 4,$$
$$-r+2s+r\ell-2bs\equiv(\ell y_1-by_2)+(y_2-by_1)\equiv 0 \pmod{a_1}$$

and $-rb-r+2s\equiv y_2-by_1\equiv 0 \pmod{a_1}$,
since $y_0\equiv 0 \pmod 4$, $y_1+y_2\equiv 0 \pmod 2$ and $1-b\equiv 0 \pmod 2$. Hence $p, q\in \mathbf{Z}$ since b is odd. We have $\det\begin{pmatrix} p & q \\ r & s\end{pmatrix}=(y_2^2-\ell y_1^2)/(2a)=-1$ (resp. $=1$) and $(-b+\sqrt{\ell})/a=(pz+q)/(rz+s)$, where $z=(-1+\sqrt{\ell})/2$. (II) In the case in which a is odd, the proof is similar to one of the case (I).

References

1. Redei, L. and Reichardt, H., Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlk¨rpers, J. für reine und angew. Math. 170 (1934) 69-74.

2. Takagi, T., Shoto Seisuron Kogi (2nd ed.) (in Japanese) Kyoritsu, Tokyo, 1971.