COLLOQUIUM MATHEMATICUM

VOL. XLI 1979 FASC. 1

REAL CHARACTERS OF THE IDEAL CLASS-GROUP AND THE NARROW IDEAL CLASS-GROUP OF $Q(\sqrt{d})$

BY

SUDESH K. GOGIA AND INDAR S. LUTHAR (CHANDIGARH)

Introduction. Let $k = Q(\sqrt{d})$ be a quadratic field of discriminant d. In a recent paper [2] we prove that the most general quadratic unramified extension of k is of the form $k(\sqrt{u})$, where u ($u \neq 1, d$) is a discriminantal divisor of d. This result allows us to give a quick construction of the (already known) real characters of the ideal class-group $C(k)$ (see [3]) and the narrow ideal class-group $C^+(k)$ (see [1] and [4]) of k. Our construction is different from those referred to above, and it has the possibility of being applicable to the construction of characters of order four, if there are any.

1. The real characters of $C(k)$. Let P denote the set of infinite places of k; put

$$\Omega = \prod_{w \in P} k_w^\times \cdot \prod_{w \notin P} r_w^\times,$$

where $r_w^\times$ is the group of units of the maximal compact subring r_w of the completion k_w of k at w. It is well known that the natural morphism from the group $k_A^\times$ of ideles of k onto the group of ideals of k determines an isomorphism, say l, of $k_A^\times / k^\times \Omega$ with $C(k)$. Thus

$$\chi \to \chi \circ l \tag{1}$$

is an isomorphism of the group of real characters of $C(k)$ with the group of real characters of $k_A^\times$ which are trivial on $k^\times \Omega$.

In what follows, the unexplained notation is as in Chapters 12 and 13 of [5]; in particular, $\mathfrak{a}$ is the canonical morphism of $k_A^\times$ into $\mathrm{Gal}(k_{ab}/k)$ defined by

$$\chi \circ \mathfrak{a}(z) = (\chi, z)_k$$

(z in $k_A^\times$, and χ in the character-group of $\mathrm{Gal}(k_{ab}/k)$).

Let G^* denote the group of those real characters χ of $\mathrm{Gal}(k_{ab}/k)$ which are such that χ_w is trivial if w is in P and χ_w is unramified if w is not in P. By using well-known results of class-field theory [5], it is easy to check that

$$\chi \to \chi \circ a$$

is an isomorphism of G^* with the group of real characters of $k_A^\times$ which are trivial on $k^\times \Omega$.

Let χ be any real non-trivial character of $\mathrm{Gal}(k_{ab}/k)$ and let k' be the associated quadratic extension of k, i.e., the fixed field of the kernel of χ. Clearly,

$$\chi \to k'$$

is a one-to-one correspondence between the non-trivial real characters of $\mathrm{Gal}(k_{ab}/k)$ and the quadratic extensions (contained in C) of k. For χ and k' being as above, it is trivial to check that χ is in G^* if and only if k' satisfies the following two properties:

(i) There lie two infinite places of k' above each infinite place of k. In other words, k' is a totally real field in case where k is a real field.

(ii) $k_w \cdot k'$ is an unramified extension of k_w for all finite places w of k, i.e., the discriminant of the extension k'/k is the unit ideal.

Thus we have proved the following

LEMMA 1. *Let k' be a quadratic unramified extension of $k = Q(\sqrt{d})$ which, in case $d > 0$, is a totally real extension of Q. Let χ be the character of $\mathrm{Gal}(k_{ab}/k)$ with kernel $\mathrm{Gal}(k_{ab}/k')$; denote by $\psi_{k'} = \psi$ the character of $k_A^\times$ defined by*

$$\psi(z) = (\chi, z)_k \quad (z \text{ in } k_A^\times).$$

Then ψ is a non-trivial real character of $k_A^\times / k^\times \Omega$; moreover,

$$k' \to \psi$$

is a one-to-one correspondence between the extensions k'/k of the above kind and the non-trivial real characters of $k_A^\times$ which are trivial on $k^\times \Omega$.

In view of the result [2] that the most general quadratic unramified extension of $Q(\sqrt{d})$ is $Q(\sqrt{d}, \sqrt{u})$, where u is a discriminantal divisor of d other than 1 and d, the following lemma is immediate.

LEMMA 2. *The most general quadratic unramified extension k' of k, which is totally real in case $d > 0$, is given by*

$$k' = Q(\sqrt{d}, \sqrt{u}),$$

where $u > 0$ is a discriminantal divisor of d other than 1 and d.

Now write

$$d = p_1^* \dots p_s^*$$

as a product of prime discriminants. The number of positive discriminantal divisors of d, other than 1 and d, is clearly

(i) $2^{s-1}-1$ if $d<0$,

(ii) 2^s-2 if each $p_i^*>0$,

(iii) $2^{s-1}-2$ if $d>0$ and some $p_i^*<0$.

In the first case, any two different positive discriminantal divisors of d give rise to different quadratic extensions of $Q(\sqrt{d})$ of the required kind. In the second and third cases, two different positive discriminantal divisors $u \neq d \neq u'$ give rise to the same extension if and only if $u' = d/u$. Taking into account the trivial character, the discussion above gives, in view of Lemma 1 and in view of isomorphism (1), the following theorem:

THEOREM 1. *Let s denote the number of distinct rational primes dividing d. Then the number r of real characters of the group $C(k)$ of ideal classes of k is the following:*

(i) *If $d<0$, then $r = 2^{s-1}$.*

(ii) *If $d>0$, then $r = 2^{s-1}$ or 2^{s-2} according as all the odd primes dividing d are congruent to* 1 (mod 4) *or not.*

Remark. This statement of the above result is simpler than (but, of course, equivalent to) the one in Hilbert's Theorem 100 [3].

To determine explicitly the real characters of $C(k)$, we first determine the real characters of $k_A^\times$ which are trivial on $k^\times\Omega$. By Lemma 1 and Theorem 1, the most general non-trivial real character of $k_A^\times/k^\times\Omega$ is obtained as follows.

Let u ($u \neq 1, d$) be a positive discriminantal divisor of d, let k' be the quadratic extension of k given by $k' = Q(\sqrt{d}, \sqrt{u})$, and let $\chi = \chi_u$ be the character of $\mathrm{Gal}(k_{ab}/k)$ whose kernel is $\mathrm{Gal}(k_{ab}/k')$. Then the corresponding character $\psi = \psi_u$ of $k_A^\times/k^\times\Omega$ is

$$\psi(z) = (\chi, z)_k = \prod_{w\nmid\infty} (\chi_w, z_w)_w. \tag{2}$$

Moreover, as we have shown above, different choices for such integers u lead to different characters ψ of $k_A^\times/k^\times\Omega$ except when $d>0$, in which case two distinct positive discriminantal divisors u and u' (different from 1 and d) lead to the same character ψ if and only if $uu' = d$.

If u and ψ are as above, then to determine ψ it clearly suffices to determine $(\chi_w, t_w)_w$ for all finite places w of k, t_w being a prime element of the field k_w. Since χ_w is an unramified character of $\mathrm{Gal}(k_{w,ab}/k_w)$, we see that

$$(\chi_w, t_w)_w = \chi_w(\varphi_w),$$

where φ_w is a Frobenius automorphism of $k_{w,ab}/k_w$ (see [5], Chapter 12). Since the kernel of χ is $\mathrm{Gal}(k_{ab}/k')$, that of χ_w is $\mathrm{Gal}(k_{w,ab}/k'\cdot k_w)$. Thus $\chi_w(\varphi_w)$ is $+1$ or -1 according as $k'\cdot k_w$ is equal to k_w or not. In other

words, denoting by $v = v_p$ the place of Q below w, we have

$$(3) \qquad (\chi_w, t_w)_w = \begin{cases} +1 & \text{if } u \text{ is a square in } k_w = Q_p(\sqrt{d}), \\ -1 & \text{otherwise.} \end{cases}$$

Let $f = f_p$ denote the modular degree of k_w/Q_p. We shall prove that

$$(3') \qquad (\chi_w, t_w)_w = \left(\frac{u'}{f_p}\right),$$

where u' is either u or d/u, the only requirement being that it is not divisible by p. To prove (3'), we distinguish three cases.

Suppose first that p divides d; then there is only one place w of k above the place $v = v_p$ of Q and $f = f_p = 1$. In particular, d is not a square in Q_p. By (3), $(\chi_w, t_w)_w = +1$ if and only if u is a square in $k_w = Q_p(\sqrt{d})$, i.e.,

$$u = (a_p + b_p\sqrt{d})^2$$

with a_p and b_p in Q_p. This is equivalent to saying that either $u = a_p^2$ or $u/d = b_p^2$. Denote by u' that one of u or d/u which is not divisible by p, and by u'' the other one. Since u'' cannot be a square in $Q_p(\sqrt{d})$, it now follows that u is a square in $Q_p(\sqrt{d})$ if and only if u' is a square in Q_p, which, by Hensel's lemma, is equivalent to

$$\left(\frac{u'}{p}\right) = +1.$$

This proves (3') in the present case.

Suppose next that $(d/p) = +1$; then there are two places of k above the place $v = v_p$ of Q and $f_p = 1$. In particular, d is a square in Q_p. Arguing as before, we see that

$$(\chi_w, t_w)_w = \left(\frac{u}{p}\right) = \left(\frac{d/u}{p}\right)$$

as desired.

Finally, suppose that $(d/p) = -1$; then there is only one place of k above the place v_p of Q and $f_p = 2$, so that the right-hand side of (3') is $+1$. Thus in the present case we have only to show that u is a square in $Q_p(\sqrt{d})$. Since $(d/p) = -1$, either

$$\left(\frac{u}{p}\right) = +1$$

or

$$\left(\frac{d/u}{p}\right) = +1.$$

It follows that either u or d/u is a square in Q_p. As d is a square in $k_w = Q_p(\sqrt{d})$, u is a square in k_w as desired.

In view of the discussion above and in view of isomorphism (1) we obtain

THEOREM 2. *Let $k = Q(\sqrt{d})$ be a quadratic field with the discriminant d. Let u ($u \neq 1$, d) be a positive discriminantal divisor of d. For any prime ideal $\mathfrak{p}$ of k, put*

$$\chi_u(\mathfrak{p}) = \begin{cases} \left(\frac{u}{N\mathfrak{p}}\right) & \text{if } \mathfrak{p} \nmid u, \\ \left(\frac{d/u}{N\mathfrak{p}}\right) & \text{if } \mathfrak{p} \mid u. \end{cases} \tag{4}$$

Then χ_u determines a non-trivial real character of $C(k)$. All the non-trivial real characters of $C(k)$ are obtained in this way; moreover, different choices of such divisors u of d lead to different characters of $C(k)$ except when $d > 0$, in which case two distinct divisors u_1 and u_2 of d of the above type lead to the same character of $C(k)$ if and only if $u_1 u_2 = d$.

2. The real characters of $C^+(k)$. As before, let $k = Q(\sqrt{d})$ be a quadratic field with the discriminant d. In th is section, we shall determine the real characters of the narrow ideal class-group $C^+(k) = I/J$ of k, where I denotes the group of all ideals of k, and J the congruence subgroup consisting of all principal ideals of k which are generated by totally positive elements of k. If $\mathfrak{A} \in I$, we shall denote by $\mathrm{cl}(\mathfrak{A})$ the corresponding element of $C^+(k)$. For each finite place w of k, let $\mathfrak{p}_w$ denote the corresponding prime ideal of k and let t_w denote a prime element of the completion k_w; we shall also denote by t_w the idele which has t_w in the w-th coordinate and 1 everywhere else. Denote by G the set of all ideles z of k for which $z_w = 1$ at all infinite places w of k. Define $\mathrm{id}: G \to I$ by

$$\mathrm{id}(z) = \prod_{w \nmid \infty} \mathfrak{p}_w^{\mathrm{ord}_w(z_w)};$$

this mapping is obviously surjective. Let us denote by U the closure of $k^\times \cdot \mathrm{id}^{-1}(J)$ in $k_A^\times$. The mapping

$$z \to \mathrm{cl}\left(\mathrm{id}(z)\right)$$

of G onto $I/J = C^+(k)$ can be extended uniquely to a homomorphism φ of $k_A^\times$ onto $C^+(k)$ which is trivial on $k^\times$ (see [5], Chapter 7). Clearly, for any finite place w of k,

$$\varphi(t_w) = \mathrm{cl}(\mathfrak{p}_w);$$

moreover, φ determines an isomorphism of $k_A^\times/U$ with $C^+(k)$ (see [5], Chapter 13); this isomorphism will also be denoted by φ. Therefore, $\chi \to \chi \circ \varphi$ is an isomorphism of the group of characters of $C^+(k)$ with the

group of characters of $k_A^\times/U$. We shall first determine the real characters of $k_A^\times$ which are trivial on U. In what follows we give another characterization of such characters.

Any real character χ of $k_A^\times$ being trivial on squares, we have

$$\chi(z) = 1$$

for every idele z for which

$$z_w \begin{cases} = 1 & \text{if } w \text{ is a finite place,} \\ > 0 & \text{if } w \text{ is a real infinite place of } k. \end{cases}$$

Since U is the closure of $k^\times \cdot \mathrm{id}^{-1}(J)$ in $k_A^\times$, a character of $k_A^\times$ is trivial on U if and only if it is trivial on $k^\times \cdot \mathrm{id}^{-1}(J)$. It can easily be checked that an idele z in G belongs to $\mathrm{id}^{-1}(J)$ if and only if it can be represented in the form

$$z = \xi z',$$

where ξ is a totally positive element of k and where, for every finite place w, z'_w is a unit in the maximal compact subring of k_w. If z, ξ and z' are as above (notice that $z_w = 1$ if $w \mid \infty$), then, for each real infinite place w,

$$z'_w = j_w(\xi^{-1}) > 0$$

(j_w is the embedding of k in k_w). It follows from these remarks that a real character of $k_A^\times$ is trivial on U if and only if it is trivial on $k^\times \cdot \prod_{w \nmid \infty} r_w^\times$ ($r_w^\times$ being the group of units of the maximal compact subring of k_w). The following lemma can now be proved in the same way as Lemma 1.

LEMMA 3. *The non-trivial real characters of $k_A^\times$, which are trivial on U, are in a one-one correspondence with the unramified quadratic extensions k' (contained in C) of k. The character of $k_A^\times/U$ attached to the quadratic extension k' of k is given by*

$$z \to (\chi, z)_k \quad (z \text{ in } k_A^\times),$$

where χ denotes the (real) character of $\mathrm{Gal}(k_{ab}/k)$ *whose kernel is* $\mathrm{Gal}(k_{ab}/k')$.

Since [2] the most general quadratic unramified extension of $Q(\sqrt{d})$ is of the form $Q(\sqrt{d}, \sqrt{u})$ with u ($u \neq 1, d$) being a discriminantal divisor of d, we see that the number of quadratic unramified extensions of $Q(\sqrt{d})$ is $2^{s-1}-1$, where s is the number of distinct rational primes dividing d. Combining this fact with Lemma 3, we get

THEOREM 3. *The number of real characters of $k_A^\times/U$, i.e., the number of real characters of the narrow ideal class-group $C^+(k)$ of $k = Q(\sqrt{d})$, is 2^{s-1}, where s is the number of distinct rational primes dividing d.*

Using Lemma 3 and the result of [2], and keeping in view the discussion at the beginning of this section, we can prove the following theorem in exactly the same way as Theorem 2.

THEOREM 4. *Let $k = Q(\sqrt{d})$ be a quadratic field with the discriminant d. Let u $(u \neq 1, d)$ be a discriminantal divisor of d. For any prime ideal $\mathfrak{p}$ of k, let χ_u be defined by* (4). *Then χ_u determines a non-trivial real character of the narrow ideal class-group $C^+(k)$ of k. All the non-trivial real characters of $C^+(k)$ are obtained in this way; moreover, two such divisors $u_1 \neq u_2$ of d lead to the same character of $C^+(k)$ if and only if $u_1 u_2 = d$.*

REFERENCES

[1] Z. I. Borewicz and I. R. Shafarevich, *Number theory*, New York 1966.

[2] S. K. Gogia and I. S. Luthar, *Quadratic unramified extensions of $Q(\sqrt{d})$*, Journal für die reine und angewandte Mathematik (accepted for publication).

[3] D. Hilbert, *Gesammelte Abhandlungen. I. Zahlentheorie*, New York 1965.

[4] C. L. Siegel, *Analytische Zahlentheorie, II*, Mathematisches Institut der Universität, Göttingen 1964.

[5] A. Weil, *Basic number theory*, 2nd edition, Springer Verlag 1973.

CENTRE OF ADVANCED STUDY IN MATHEMATICS
PANJAB UNIVERSITY, CHANDIGARH

Reçu par la Rédaction le 4. 6. 1977