ACTA ARITHMETICA
XXXV (1979)

Kuroda's class number relation*

by

C. D. WALTER (Dublin)

Kuroda's class number relation [5] may be derived easily from that of Brauer [2] by eliminating a certain module of units, but the technique is applicable to a much wider class of relations which are obtained from norm relations. The main aim here is to treat the case in which several radicals of the same prime degree are adjoined to the rational field.

1. Norm relations. Let G be the Galois group of a normal extension K/k of algebraic number fields and $\tilde{H}$ the sum of the elements in a subgroup H. Then a relation of the form

$$(1.1)\qquad \sum_H b(H)\tilde{H} = 0 \qquad (b(H) \in \mathbb{Q})$$

is called a *norm relation*. These have been studied by Rehm in [7] and are so-called because Artin has established in [1] that the relation holds precisely when

$$\prod_H \left(N_{K/HK}(x)\right)^{b(H)} = 1 \qquad \text{for all } x \in K^*.$$

Here HK is the subfield fixed by H and N is the relative norm. If 1_H^G denotes the character on G induced by the unit character on H then the equation

$$(1.2)\qquad \sum_{g\in G} 1_H^G(g)g = |H|^{-1} \sum_{g\in G} g\tilde{H}g^{-1}$$

may be used to convert the norm relation (1.1) into the character relation

$$(1.3)\qquad \sum_H b(H)\,|H|\,1_H^G = 0.$$

The most interesting relations satisfy two further conditions :

(1.4) DEFINITION. $\sum b(H)H = 0$ is called a *direct* norm relation if

(i) there is an $H_0 \in S = \{H \mid b(H) \neq 0\}$ such that $H_0 \subset H$ for all $H \in S$, and

(ii) distinct $H_1, H_2 \in S_0 = \{H \in S \mid H \neq H_0, H \neq G\}$ satisfy

$$|H_1|^{-1}\tilde{H}_1 \cdot |H_2|^{-1}\tilde{H}_2 = |G|^{-1}\tilde{G}.$$

* Work completed under a Rouse Ball studentship from Trinity College, Cambridge.

This definition and its notation will be subsumed from here on. All sums and products will extend over $H \in S$ and ' will indicate their restrictions to $H \in S_0$. For any left (resp. right) $\mathbb{Z}[G]$-module M let HM (resp. MH) be the submodule fixed under the action of H and write M_0 for $\sum' HM$. If M is torsion-free over $\mathbb{Z}$ and $GM = 0$ then

(1.5) $$M_0 = \sum{}' HM \quad \text{is a direct sum.}$$

For suppose $H, H' \in S_0$ are distinct. Then $\tilde{H}\tilde{H}' \in \mathbb{Z}\tilde{G}$ and so H provides $|H||H'|/|G|$ representatives for each coset of H' in G. Thus $\tilde{H}$ acts a multiple of the trace on $H'M/GM$. Consequently if $m = \sum m_H \in M_0$ with $m_H \in HM$ then $\tilde{H}m = |H|m_H$ because $GM = 0$. Hence, m_H is unique as M is torsion-free.

(1.6) THEOREM. *A direct norm relation has the form*

$$\sum{}' \left(\tilde{H}/|H| - \tilde{G}/|G|\right) = \tilde{H}_0/|H_0| - \tilde{G}/|G|$$

and its associated character relation is

$$\sum{}' \left(1_H^G - 1\right) = 1_{H_0}^G - 1\ .$$

Moreover

$$H_0 = \cap\{H \in S_0\}\ , \qquad G = \cup\{H \in S_0\}\ ,$$

and S_0 completely specifies the relation.

Proof. When $\sum a(H')|H'|^{-1}\tilde{H}' = 0$ is multiplied by $\tilde{H}/|H|$ for $H \in S_0$ or $H = G$ one obtains

$$(a_0 + a(H))|H|^{-1}\tilde{H} + \sum a(H')|G|^{-1}\tilde{G} = 0$$

where $a_0 = a(H_0)$ and the sum extends over $H' \neq H$ in $S_0 \cup \{G\}$. This gives $a_0 + \mathrm{a}(H) = 0$ for $H \in S_0$ and $\sum a(H') = 0$ for $H = G$. Thus the form of the norm relation is established. (1.3) gives the character equation which will henceforth usually be written

(1.3') $$\sum a(H) 1_H^G = 0\ .$$

(1.7) EXAMPLE. If G is an elementary abelian group of prime exponent p and order p^n and T is the set of $(p^n - 1)/(p - 1)$ maximal subgroups then

$$\sum_{H \in T} \tilde{H} = (p^{n-1} - 1)/(p-1) \cdot \tilde{G} + p^{n-1} \cdot \tilde{1}$$

is a direct norm relation.

Proof. Any isomorphism between G and its character group G^* provides a bijection between maximal and minimal subgroups, namely

$$H \leftrightarrow H^{\perp} = \{g \in G \mid h(g) = 0\ \forall h \in H^*\}$$

where H^* is the image of H in G^*. The order of T is the number $(p^n-1)/(p-1)$ of minimal subgroups. Now $g \in H$ if and only if $\langle g\rangle^{\perp} \supset H^{\perp}$. So the number of maximal H containing g is the number of minimal subgroups of $\langle g\rangle^{\perp}$, namely $(p^{n-1}-1)/(p-1)$ if $g \neq 1$. Thus the norm relation holds. It is direct because distinct maximal subgroups H and H' satisfy $\tilde{H}\tilde{H}' = p^{n-2}\tilde{G}$.

There are several ways of constructing new relations from given ones by passing from the whole group to a subgroup or quotient group and *vice versa* (see [8]). In particular,

(1.8) LEMMA. *Suppose G and G' are subgroups of G_0 such that $\tilde{G}\tilde{G}' = \tilde{G}_0$ and $\sum b(H)\tilde{H} = 0$ is a direct norm relation for G. If $HG' = \{hg' \mid h \in H, g' \in G'\}$ is a subgroup of G_0 for every $H \in S$ then $\sum b(H)\widetilde{HG'} = 0$ is a direct norm relation for G_0.*

This is clear because $\widetilde{HG'} = \tilde{H}\tilde{G}' = \tilde{G}'\tilde{H}$ for $H \in S$.

2. Brauer's class number relation. Let U be the unit group of K ; W its subgroup of roots of unity; $w_2(H)$ the 2-component in the order of HW; $h(H)$ the class number of HK; $r(H)$ the rank of HU/HW ; and $n(H)$ the degree of HK/k. A bar will denote the natural map $U \to U/W$.

Choose one prime divisor in K of each infinite prime in k and suppose $\{C_i \mid 1 \le i \le r\}$ is the set of their decomposition groups in K/k. So $r = r(G) + 1$ and each C_i is determined up to conjugacy. If L is defined by the exact sequence

$$(2.1) \qquad 0 \to \mathbb{Z} \to \bigoplus_{i=1}^{r} \mathbb{Z}[G]C_i \to L \to 0$$

of $\mathbb{Z}[G]$-modules where $n \in \mathbb{Z} \mapsto n \oplus_i \tilde{G}$ then Brauer's theorem may be formulated as follows.

(2.2) THEOREM ([9], Theorem 4.1). *Suppose $\sum a(H)1_H^G = 0$. If the submodule M of $\overline{U}$ is $\mathbb{Z}[G]$-isomorphic to L then*

$$\prod h(H)^{a(H)} = \prod \big(n(H)w_2(H)[\overline{HU} : HM]\big)^{a(H)}.$$

Unit groups may be written in either additive or multiplicative notation but the context will clarify the choice. Suppose

$$(2.3) \qquad \mathbb{Q}GU = \{\varepsilon \in U \mid \exists n \in \mathbb{Z},\ n \neq 0, \text{ with } n\varepsilon \in GU\}$$

is the group of units with powers in k. Then $G\overline{V} = \overline{V \cap \mathbf{Q}GU}$ for any subset $V \subset U$ and so the equalities hold in the definitions below.

$$Q^* = [H_0L : L_0],$$

$$Q = [H_0U : H_0W+U_0] = [\overline{H_0U} : \overline{U_0}],$$

$$Q_0 = [H_0U : (H_0U \cap \mathbb{Q}GU) + U_0] = [\overline{H_0U} : G\overline{H_0U} + \overline{U_0}],$$

$$I(H) = [HU \cap \mathbb{Q}GU : HW+GU] = [G\overline{HU} : G\overline{U}],$$

$$I_0 = [U_0 \cap \mathbb{Q}GU : W_0 + GU] = [G\overline{U_0} : \overline{GU}].$$

By comparing ranks $I(H)$ and I_0 are finite. If $x \in H_0X$ for some $\mathbb{Z}[G]$-module X then (1.1) gives

$$-b(H_0)x = b(G)\widetilde{G/H_0}x + {\sum}' b(H)\widetilde{H/H_0}\,x$$

As $\widetilde{H/H_0}$ is the trace for H_0X/HX so (1.6) shows that $[G{:}H_0]x \in X_0$. Thus

(2.4) $$[H_0X : X_0] \text{ is finite}$$

if X is finitely generated, and all the indices above are finite. The basic simplification of (2.2) for direct norm relations is :

(2.5) LEMMA.

$$\prod[\overline{HU} : HM]^{a(H)} = (Q_0/Q^*)^{a_0} \prod I(H)^{a(H)}.$$

Proof. $(G\overline{H_0U} + \overline{U_0})/\overline{U_0} \cong G\overline{H_0U}/G\overline{U_0}$ whence

(2.6) $$Q/Q_0 = I(H_0)/I_0.$$

Let $V = G\overline{U_0}$. Then

$$\begin{aligned}
&Q^*[\overline{H_0U} : H_0M]/[\overline{GU} : GM]I(H_0)Q_0 \\
&= [H_0M : M_0][\overline{H_0U} : H_0M][GM : \overline{GU}][\overline{GU} : V][\overline{U_0} : \overline{H_0U}] \\
&= [\overline{U_0} : M_0][GM : V] = [\overline{U_0} : M_0 + V] \quad \text{since } (M_0+V)/M_0 \cong V/GM \\
&= [\overline{U_0}/V : (M_0+V)/V] = {\prod}'[(\overline{HU}+V)/V : (HM+V)/V] \text{ by (1.5)} \\
&= {\prod}'[\overline{HU} : (HM+V) \cap \overline{HU}] \\
&= {\prod}'[\overline{HU} : HM]/[HM + G\overline{HU} : HM] \\
&= {\prod}'[\overline{HU} : HM]/[G\overline{HU} : HM \cap G\overline{HU}] \\
&= {\prod}'[\overline{HU} : HM]/[\overline{GU} : GM]I(H) .
\end{aligned}$$

Theorem (1.6) completes the proof.

3. The index Q^*. Let L_i be defined to make the $\mathbb{Z}[G]$-module sequence

$$(3.1)\qquad 0 \to \mathbb{Z} \to \bigoplus_{i=1}^{r} \mathbb{Z}[G]C_i \to L_i \to 0$$

exact. Associated with it is the submodule $L_{i0} = \sum' HL_i$ and the index $Q_i^* = [H_0L_i : L_{i0}]$ which is finite by (2.4). Both (2.1) and (3.1) are exact when restricted to the submodules fixed by a subgroup H because this is a left exact functor and any pre-image of an element in HL or HL_i is certainly fixed by H. Hence

$$H_0L/L_0 \cong \{H_0(\bigoplus_i \mathbb{Z}[G]C_i)\}/\{\textstyle\sum' H(\bigoplus_i \mathbb{Z}[G]C_i)\}$$

$$\cong \bigoplus_i \left(H_0\mathbb{Z}[G]C_i \,/\, \textstyle\sum' H(\mathbb{Z}[G]C_i)\right) \cong \bigoplus_i H_0L_i/L_{i0}$$

and so

$$(3.2)\qquad Q^* = \prod_i Q_i^* .$$

Now define a pairing on $\mathbb{Q}L_i \times \mathbb{Q}L_i$ by $(x, y) = |G|^{-1}(1_1^G - 1)(xy^*)$ where $*$ is the involution induced by $g \mapsto g^{-1}$ for $g \in G$. If N is a $\mathbb{Z}$-submodule of L_i with basis $\{n_r\}$ let $R(N) = |\det((n_r, n_s))|$ be the regulator of N. This is independent of the choice of basis and for another submodule N' it satisfies

$$(3.3)\qquad R(N') = [N : N']^2 R(N)$$

whenever $[N : N']$ is defined.

Let HgC_i denote the sum of the distinct elements in $\{hgc \mid h \in H, c \in C_i\}$, $|HgC_i|$ the number of such elements, and $\overline{HgC_i}$ its image in L_i under (3.1). If H and $H' \in S_0$ are distinct then there are $h \in H$ and $h' \in H'$ such that $hh' = g$ for any given $g \in G$. So $h^{-1}gh'^{-1} = 1$ and $\tilde{H}g\tilde{H}' = \tilde{H}\tilde{H}'$. Thus

$$(HgC_i)(H'g'C_i)^* \in \mathbb{Z}\tilde{G} \quad \text{and} \quad (\overline{HgC_i}, \overline{H'g'C_i}) = 0 .$$

However, the $\overline{HgC_i}$ form a basis of L_{i0} for $H \in S_0$ and suitable $g \in G$ because $L_{i0} = \sum' HL_i$ is a direct sum by (1.5). Hence the corresponding matrix for $R(L_{i0})$ is zero except for blocks of determinant $R(HL_i)$ on the diagonal. This gives

$$(3.4)\qquad R(L_{i0}) = \textstyle\prod' R(HL_i) .$$

The number of HgC_i which have $|H|$ elements is

$$|\{g \in G \mid g\gamma_i g^{-1} \in H\}| \,/\, |H| = 1_H^G(\gamma_i)$$

where γ_i generates C_i. Thus the number with $2|H|$ elements is $r_{2i}(H) = 1_H^G(1-\gamma_i)/2$. Set $r_i(H) = \dim H\mathbb{Z}[G]C_i - 1$. As (3.1) is exact when fixed by H so $\{\overline{HgC_i}\}$ is a basis of HL_i when g runs over representatives of the non-principal double cosets $H\backslash G/C_i$. If $HgC_i \neq HhC_i$ then

$$(\overline{HgC_i}, \overline{HhC_i}) = -|HgC_i||HhC_i| / |G|$$

and

$$(\overline{HgC_i}, \overline{HgC_i}) = |HgC_i| - |HgC_i|^2 / |G| .$$

Hence

$$R(HL_i) = |H|^{r_i(H)+1} 2^{r_{2i}(H)} |H1C_i|^{-1} \det A$$

where $A = I - (|HgC_i| / |G|)_{g,h}$ for the identity matrix I. Add together the rows of A to obtain the constant row $|H1C_i| / |G|$ and use it to eliminate $(|HgC_i| / |G|)_{g,h}$. Thus $\det A = |H1C_i| / |G|$ and

$$R(HL_i) = |H|^{r_i(H)+1} 2^{r_{2i}(H)} / |G| . \tag{3.5}$$

Equation (3.3) gives $Q_i^{*2} = R(L_{i0})/R(H_0L_i)$ and combining this with (3.4) and (3.5) produces

$$Q_i^{*2} = \Big(\prod{}' |H|^{r_i(H)+1} / |G|\Big) / \Big(|H_0|^{r_i(H_0)+1} / |G| \Big) \tag{3.6}$$

because $\sum{}' r_{2i}(H) = \sum{}' 1_H^G (1-\gamma_i)/2 = 1_{H_0}^G (1-\gamma_i)/2 = r_{2i}(H_0)$ removes the power of 2. Now

$$r(H) + 1 = \dim HL + 1 = \sum_i \dim H\mathbb{Z}[G]C_i = \sum_i (r_i(H) + 1) .$$

Thus (3.6), (3.2), and (1.6) together yield

$$Q^{*-2a_0} = \prod |H|^{a(H)(r(H)+1)} . \tag{3.7}$$

4. The Einheitenindex $I(H)$. $I(H)$, which will be written $I(HK/k)$ in this section, is a generalization of Hasse's Einheitenindex ([3], §20) for an abelian extension of $\mathbb{Q}$ over its maximal real subfield. Let $k_2 \supset k_1 \supset k_0$ be a tower of fields. The basic property is

(4.1) THEOREM. *$I(k_2/k_0)$ divides $[k_2:k_0]$.*

This is clear from the next lemma because $I(k_2/k_0)$ divides $I(k_2/k_1) \times I(k_1/k_0)$.

(4.2) LEMMA. *If k_1/k_0 has no intermediate fields and $[k_1:k_0] = p$ then $I(k_1/k_0) = 1$ or p. In the latter case p is prime and $k_1 = k_0(\varepsilon)$ for some unit ε such that $\varepsilon^p \in k_0$. Conversely, if p is prime and $k_1 \neq k_0(\sqrt{-1})$ has this form then $I(k_1/k_0) = 1$ or p according to whether or not k_1 is the unique extension of k_0 with the form $k_1 = k_0(\omega)$ where $\omega^p \in k_0$ is a root of unity with p-power order.*

Proof. Let U_i and W_i be the groups of units and roots of unity in k_i, W_{ip} the p-Sylow subgroup of W_i, and V_1 the subgroup of units in k_1 with some power in $V_0 = U_0W_1$. Then $I(k_1/k_0) = [V_1 : V_0]$. The norm N for k_1/k_0

induces the pth power map on V_1/W_1 and maps V_1 into U_0. Hence V_1 / V_0 has exponent p.

Assume $V_1 \neq V_0$. If $\varepsilon \in V_1-V_0$ then there is an $m \in \mathbb{Z}$ such that $\varepsilon^m \notin U_0$ but $\varepsilon^{mp} \in U_0$. So $k_1 = k_0(\varepsilon^m)$ and p is prime. Moreover, if is ζ a primitive pth root of unity and $k'_i = k_i(\zeta)$ then k'_1/k'_0 is cyclic with generating automorphism α, say. The norm N extends to k'_1/k'_0. Let $q = [W_1 : W_{1p}]$. Then $\varepsilon^{q(1-\alpha)} \in W_{1p}\langle\zeta\rangle$ for $\varepsilon \in V_1$. Thus if $\varepsilon_1, \varepsilon_2 \in V_1$ then a, $b \in \mathbb{Z}$ can be chosen such that $p \nmid a$ or $p \nmid b$, and $(\varepsilon_1{}^a\varepsilon_2{}^b)^{q(1-\alpha)} = 1$. So $\varepsilon_1{}^{aq}\varepsilon_2{}^{bq} \in U_0$ and $\varepsilon_1{}^a\varepsilon_2{}^b \in V_0$. Hence $\varepsilon_1 \notin V_0$ implies $p \nmid b$ and $\varepsilon_2 \in V_0\langle\varepsilon_1\rangle$. Therefore V_1/V_0 is cyclic of order p.

Suppose $k_1 \neq k_0(\sqrt{-1})$ but $k_1 = k_0(\varepsilon)$ where $\varepsilon^p \in U_0$. Then $\omega \in W_{1p}\langle\zeta\rangle$ and $N\omega = 1$ give $\omega \in \langle\zeta\rangle$. So putting $\omega = \varepsilon_1{}^{q(1-\alpha)}$ for $\varepsilon_1 \in V_1$ yields $V_1{}^{q(1-\alpha)} \subset \langle\zeta\rangle$. In fact, ε gives $V_1{}^{q(1-\alpha)} = \langle\zeta\rangle$. The last part of the lemma holds because in this case $V_0{}^{q(1-\alpha)} = 1$ if and only if $W_{1p} = W_{0p}$.

5. The indices Q_0 and Q .

(5.1) LEMMA. *Q_0 divides* $\prod' [H : H_0]^{r(H)-r(G)}$.

Proof. Q_0 is the order of

$$H_0U/(U_0+H_0U\cap \mathbb{Q}GU) \cong (H_0U+ \mathbb{Q}GU)/(U_0+\mathbb{Q}GU) \cong \varphi(H_0U)/\varphi(U_0)$$

where φ: $U \to U/\mathbb{Q}GU$ is the natural map. For $\varepsilon \in H_0U$ the norm equation (1.6) gives

$$[G:H_0]\varepsilon = (1-|S_0|)\widetilde{G/H_0}\varepsilon + \sum{}' [G:H]\widetilde{H/H_0}\varepsilon$$

so that

(5.2) $\sum' [G:H_0]\varphi(HU)$

$$= [G:H_0]\varphi(U_0) \subset [G:H_0]\varphi(H_0U) \subset \sum{}' [G:H]\varphi(HU)$$

because $\varphi(GU) = 0$. Since the sums $\sum'$ are direct by (1.5) and each $\varphi(HU)$ is torsion-free, Q_0 divides the index $\prod' [H:H_0]^{\dim\varphi(HU)}$ between the end modules. Finally $\dim \varphi(HU) = r(H)-r(G)$.

(5.3) LEMMA. *If $[H:H_0] = n$ is the same for all $H \in S_0$ then Q divides $I'n^{r(H0)-r(H')}$ for each $H' \in S_0$ where*

$$I' = [H_0U\cap\mathbb{Q}H'U : H_0W + U_0\cap\mathbb{Q}H'U].$$

I' divides $I(H_0K/H'K)$ which divides n.

Proof. Let φ': $U \to U/\mathbb{Q}H'U$ be the natural map. Then (5.2) yields

$$\sum{}' n\varphi'(HU) = n\varphi'(U_0) \subset n\varphi'(H_0U) \subset \sum{}' \varphi'(HU) .$$

The sums $\sum'$ are direct. Hence $Q' = [H_0U + \mathbb{Q}H'U : U_0+\mathbb{Q}H'U]$ divides the index $\prod' n^{\dim \varphi'(HU)}$ between the end modules. As

$$\dim \varphi'(HU) \;=\; \dim \varphi(HU) = r(H) - r(G) \quad \text{for} \quad H \in S_0, H \neq H',$$

and

$$\sum{}'(r(H) - r(G)) \;=\; r(H_0) - r(G)$$

so Q' divides $n^{r(H_0)-r(H')}$. Now

$$\begin{aligned} Q &= [H_0U : H_0W + U_0] \\ &= [H_0U : U_0+(H_0U\cap\mathbb{Q}H'U)][U_0+(H_0U\cap\mathbb{Q}H'U):H_0W+U_0] = Q'I'. \end{aligned}$$

Thus the proof is completed by (4.1).

6. Kuroda's relation.

(6.1) MAIN THEOREM. *Suppose the subgroups of the Galois group G of a normal extension K/k of number fields satisfy a direct norm relation* ((1.4) *and* (1.6)) *whose corresponding character relation is* (1.3'). *Then the class numbers $h(H)$ of the fields HK fixed by the subgroups H are related by*

$$\prod_H h(H)^{a(H)} \;=\; (w_iQ_0)^{a_0} \prod_H \{I(H)\,[H : H_0]^{(r(H)-1)/2}\}^{a(H)}\,. \tag{6.2}$$

The unit indices Q_0 and $I(H)$ are defined in §2 *and bounded by* (5.1) *and* (4.1). *Further, $w_i = 1$ unless $k \subsetneq k(\sqrt{-1}\,) \subset H_0K$ when $w_i = w_2(H_0)/w_2(H_i)$ for the unique subgroup $H_i \in S_0$ whose fixed field contains $k(\sqrt{-1}\,)$.*

Let $C(H)$ be the subgroup of the ideal class group of HK composed of classes with orders prime to $[G : H_0]$. Then the part of the class number relation (6.2) *prime to $[G : H_0]$ is induced by the direct sum decomposition*

$$C(H_0)/C(G) \;=\; \sum_{H\in S_0} C(H)/C(G)$$

given by $\gamma = \sum' [H:H_0]^{-1}\widetilde{H/H_0}\gamma$ for $\gamma \in C(H_0)/C(G)$ and the natural identification of $C(H)$ as a subgroup of $C(H_0)$.

Proof. Define w_i by $w_i^{a_0} = \prod w_2(H)^{a(H)}$. Then Theorem 2.3 of [9] gives $w_i = 1$ if $\sqrt{-1} \in k$ or $\sqrt{-1} \notin H_0K$. Otherwise, if J is the Galois group of $K/k(\sqrt{-1}\,)$ then (1.6) yields

$$\sum{}'(\tilde{J}\tilde{H} / |J||H| - \tilde{G} / |G|) \;=\; \tilde{J} / |J| - \tilde{G} / |G|.$$

Consequently $\tilde{J}\tilde{H} / |J||H| \neq \tilde{G} / |G|$ for at least one $H \in S_0$, say H_i, and $H_i \subset J$ for such a subgroup. However, if J also contains $H'_i \in S_0$ then $H_iH'_i \neq G$ and so $H_i = H'_i$. As $w_2(H) = 2$ for all $H \in S_0$ except $H = H_i$ the value of w_i is $w_2(H_0)/w_2(H_i)$.

Now $\sum a(H)r(H) = 0$ is apparent from equating the ranks of H_0U and U_0. Hence (6.2) is obtained from (2.2), (2.5) and (3.7). The class group relation holds because the norm equation gives

$$\gamma \;=\; \sum{}' [H : H_0]^{-1} \widetilde{H/H_0}\gamma\,.$$

A particularly useful special case of this theorem is a generalization of Kuroda's result [5], which includes the formulae of Herglotz [4] and Parry [6].

(6.3) THEOREM. *Let p be a rational prime, $n \geq 2$ an integer, and a_i $(1 \leq i \leq n)$ elements of a number field k. Suppose*

$$k_* \;=\; k\left(\sqrt[p]{a_i} \mid 1 \leq i \leq n \right)$$

has degree p^n over k and let $\{k_t \mid t \in T\}$ be the set of $(p^n-1)/(p-1)$ subfields of degree p over k. Denote by h_*, h_t, h_k; U_*, U_t, U_k; and W_*, W_t, W_k the class numbers, unit groups, and groups of roots of unity of k_*, k_t, and k respectively. Set

$$Q \;=\; [\, U_* : W_* \prod_{t\in T} U_t\,]\,.$$

Let u be the number of algebraically independent fields k_t of the form $k(\varepsilon)$ where $\varepsilon^p \in U_k$. If one of the k_t is $k(\sqrt{-1})$ let v satisfy $2^v = w_{2*}/w_{2i}$ where w_{2*} and w_{2i} are the 2-components of the numbers of roots of unity in k_* and $k(\sqrt{-1})$. Otherwise put $v = 0$. Let r_*, r_t, and r_k be the $\mathbb{Z}$-ranks of U_*/W_*, U_t/W_t, and U_k/W_k. Then

$$\frac{h_*}{h_k}\prod_{t\in T}\frac{h_k}{h_t} \;=\; Qp^{-A}$$

where

$$A \;=\; \tfrac{1}{2}(n-1)(r_*-1) - \tfrac{1}{2}\left(\frac{p^n-1}{p-1}-1\right)(r_k-1) + \left(\frac{p^u-1}{p-1}-u\right) - v\,.$$

The index Q divides p^B for $B = B_t = (n-1)(r_*-r_t+1)$ and any field k_t; and the p^{n-1}-th power of every unit of k_* lies in $W_*\prod U_t$.

For $\Omega = k_*$, k_t, or k let $C(\Omega)$ be the natural embedding into $C(k_*)$ of the part of the ideal class group of Ω formed from classes whose orders are prime to p. Then there is a direct sum decomposition

$$C(k_*)/C(k) \;=\; \sum_{t\in T} C(k_t)/C(k)\,.$$

Remarks. The same theorem holds more generally provided only that the Galois group concerned is isomorphic to the one here.

When applied to different relative extensions within k_*/k the theorem produces all relations between the class numbers of intermediate fields which can be deduced from relations between induced principal characters.

The value of B cannot in general be improved beyond

$$B' = \tfrac{1}{2}(r_* +1)(n-1) - \tfrac{1}{2}(r_k+1)\left((p^n-1)/(p-1)-1\right)$$

because $p^{B'}$ is the value of Q when U_*/W_k is isomorphic to the lattice L of (2.1).

Proof. Example (1.7) gives a relation between the Galois groups of the fields $k_*(\sqrt[p]{1})$, $k_t(\sqrt[p]{1})$, and $k(\sqrt[p]{1})$, and Lemma (1.8) allows this to be lifted to a direct norm relation between the groups of the fields k_*, k_t, and k. (6.2) gives the required relation once the following equalities are proved:

(6.4) $$w_i = p^v,$$

(6.5) $$\prod [H:H_0]^{a(H)(r(H)-1)/2} = p^{-a_* x}$$

$$\text{for } x = \tfrac{1}{2}(n-1)(r_*-1) - \tfrac{1}{2}\{(p^n-1)/(p-1)-1\}\{r_k-1\},$$

(6.6) $$Q_0^{a_*}\prod I(H)^{a(H)} = Q^{a_*}p^{-a_* y} \qquad \text{for } y = (p^u-1)/(p-1)-u\,.$$

The first is trivial and for the second note that

$$\prod [H:H_0]^{a(H)(r(H)-1)/2} = \prod ([H:H_0]p^{1-n})^{a(H)(r(H)-1)/2} = p^{-a_* x}\,.$$

By (2.6) the last is equivalent to

$$I_0^{a_*}\prod I(H)^{a(H)} = I(H_0)^{a_*}p^{-a_* y}\,,$$

that is,

$$I_0^{-1}\prod_{t\in T} I_t = p^y$$

in the obvious notation.

By (4.2) the index I_t is 1 or p. If $k(\varepsilon_1)$ and $k(\varepsilon_2)$ are two of the k_t with ε_1^p and ε_2^p in U_k then $k(\varepsilon_1\varepsilon_2)$ is k or another such k_t. Thus if there are u algebraically independent such fields then the total number is the number of subfields k_t of their composition k_c, *viz.* $(p^u-1)/(p-1)$, and, by (4.2),

$$\prod I_t = p^{y+u-\delta} \qquad \text{where } \delta = 0 \text{ or } 1.$$

Precisely, $\delta = 0$ if no field k_t has the form $k(\omega)$ where $\omega \in W_*$ has p-power order, or if one of the k_t is $k(\sqrt{-1})$ and it has corresponding index $I_t = p$. Otherwise $\delta = 1$.

Let us suppose that if one of the k_t is $k(\sqrt{-1})$ then $I_t = 1$ for it. The linear combinations of u algebraically independent generators ε of the k_t with $\varepsilon^p \in U_k$ generate each $U_t \cap \mathbb{Q}U_k$ over W_tU_k and so generate

$U_0 \cap \mathbb{Q} U_k$ over $W_0 U_k$. No linear combination which is not a pth power can lie in U_k because of their algebraic independence. Therefore any combination in $W_0 U_k$ lies in the equivalence class modulo U_k of a root of unity $\omega \notin k$ with $\omega^p \in k$ and yields a subfield k_t of k_c with $I_t = 1$. Conversely, such a k_t in k_c leads to a linear combination in $W_0 U_k$. Hence $I_0 = p^{u-\delta}$.

Now suppose that $k_i = k(\sqrt{-1})$ is one of the k_t and that $I_i = p$. Then the u algebraically independent ε generate each $U_t \cap \mathbb{Q} U_k$ over $W_t U_k$ except when $t = i$. Thus they generate over $W_0 U_k$ a subgroup of index p in $U_0 \cap \mathbb{Q} U_k$. On the other hand there is a linear combination of them which lies in the same class modulo U_k as $\sqrt{-1}$. Thus again $I_0 = p^{u-\delta}$ and $I_0^{-1} \prod I_t = p^y$ which proves (6.6).

The bounds on the order and exponent of $U_*/W_* \prod U_t$ come from (5.3) and from applying (1.6). The first remark is clear; for the second see [8]; and for the last use (3.7).

References

[1] E. Artin, *Linear mappings and the existence of a normal basis*, Volume for Courant's 60th Birthday, Interscience, New York 1948.

[2] R. Brauer, *Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers*, Math. Nachr. 4 (1951), pp. 158–174.

[3] H. Hasse, *Über die Klassenzahl abelscher Zahlkorper*, Akad. Verlag, Berlin 1952.

[4] G. Herglotz, *Über einen Dirichletschen Satz*, Math. Zeitschr. 12 (1922), pp. 225–261.

[5] S. Kuroda, *Über die Klassenzahlen algebraischer Zahlkörper*, Nagoya Math. J. 1 (1950), pp. 1–10.

[6] C. J. Parry , *Class number formulae for bicubic fields*, Illinois J. Math. 21 (1977), pp. 148–163.

[7] H. P. Rehm, *Über die gruppentheoretische Struktur der Relationen zwischen Relativnormabbildungen in endlichen Galoisschen Körpererweiterungen*, J. Number Theory 7 (1975), pp. 49–70.

[8] C. D. Walter, *Class number relations in algebraic number fields*, Doctoral thesis, Cambridge University, 1976.

[9] – *Brauer's class number relation*, Acta Arith., this volume, pp. 33–40.

DEPARTMENT OF MATHEMATICS
UNIVERSITY COLLEGE
Be1field, Dublin 4, Ireland

Received on 13. 2. 1976
and in revised form on 2. 11. 1976 (814b)