HILBERT CLASS FIELDS AND SPLIT EXTENSIONS

BY

ROBERT GOLD

1. Let k be a number field and K a finite normal extension of k. Let K' denote the Hilbert class field of K. Then K'/k is a finite normal field extension and the group $U = \mathrm{Gal}\,(K'/k)$ is a group extension of $C = \mathrm{Gal}\,(K'/K)$ by $G = \mathrm{Gal}\,(K/k)$:

$$(1) \qquad 1 \to C \to U \to G \to 1.$$

We are interested in knowing when this sequence splits; i.e., when U is a semi-direct product of C by G. The splitting of (1) is equivalent to the existence of an extension F of k such that $F \cap K = k$ and $F \cdot K = K'$.

Using local class field theory and the Weil-Shafarevich theorem, Wyman gave a sufficient condition for splitting, [4, p. 145]. In Theorem 1 we give a simpler and more elementary proof of this result. Theorem 2 is its corollary for cyclic G [4, p. 147]. Theorem 3 provides a necessary and sufficient condition for the splitting of (1) when G is a cyclic group. In Section 3 we give some group-theoretic examples and an interesting special case.

2. Assume that K/k has a totally ramified prime. Let T' be the inertia group in the extension K'/k of some prime lying over this one. Then $T' \cap C = \{1\}$ and $T'C/C = G$. Hence T' is a complement for C in U and (1) splits. Theorem 1 and its proof are elaborations of this basic construction.

THEOREM 1. *Let r be the least common multiple of the ramification indices of all primes in K/k. If $r = [K: k]$, then*

$$1 \to \mathrm{Gal}\,(K'/k) \to \mathrm{Gal}\,(K'/k) \to \mathrm{Gal}\,(K/k) \to 1$$

splits.

Proof. Let T be the inertia group in K/k of some ramified prime and let k_T be the fixed field of T. By the remarks immediately preceding the statement of the theorem, the group extension

$$(2) \qquad 1 \to C \to \mathrm{Gal}\,(K'/k_T) \to T \to 1$$

is split. Here (2) is the restriction of (1) to T. That is, if we let $\pi: U \to G$ be the surjection in (1), then (2) may be written

$$1 \to C \to \pi^{-1}(T) \to T \to 1.$$

In cohomological terms, (2) is the image of (1) under $\mathrm{Res}: H^2(G, C) \to H^2(T, C)$ [3, p. 213].

Received August 18, 1975.

Thus each restriction of (1) *to an inertia subgroup of G is split. When does this imply that G itself is split*?

Note that restriction is transitive. In particular, (1) restricted to a subgroup of an inertia subgroup is split. We invoke a theorem of Gaschütz: (1) is split if and only if for every prime p, the restriction to some p-Sylow subgroup of G is split [2, p. 246]. Hence in order to split (1) it suffices to have for every prime p some inertia subgroup T containing a p-Sylow subgroup of G. But since the orders of the inertia subgroups are given by the ramification indices in K/k, this last condition is clearly implied by the hypothesis of the theorem, $r = [K: k]$.

THEOREM 2. *If K/k is cyclic and $k' \cap K = k$, then* (1) *is split.*

Proof. It suffices to show that if G is cyclic, then $k' \cap K = k$ implies $r = [K: k]$. Since G is cyclic and r is the least common multiple of the orders of the inertia subgroups of G, r is the order of the subgroup $\hat{T}$ of G generated by all inertia subgroups. The fixed field of $\hat{T}$ is exactly $K \cap k'$, the maximal unramified extension of k in K. Hence we have $r = [K: K \cap k']$ and so $r = [K: k]$ iff $K \cap k' = k$.

The next result is a necessary and sufficient condition for splitting when G is cyclic. First we must introduce some Galois cohomology. The group $C = \mathrm{Gal}\,(K'/K)$ is G-isomorphic to C_K, the ideal class group of K. The elements of $H^2(G, C)$ correspond one-one with the equivalence classes of extensions of C by G with the given action of G on C. The identity of $H^2(G, C)$ corresponds to the split extension of C by G. Let $\mathscr{C}_K$ denote the idele class group of K. There is a natural surjection $f\colon \mathscr{C}_K \to C_K$ and an induced map $f_2\colon H^2(G, \mathscr{C}_K) \to H^2(G, C_K)$. Furthermore, $H^2(G, \mathscr{C}_K)$ is cyclic of order $[K: k]$ and has a distinguished generator, the fundamental class μ. The theorem of Weil and Shafarevich states that $f_2(\mu) \in H^2(G, C)$ is the class of the group extension (1) [1, p. 246]. Therefore this extension splits if and only if $f_2(\mu) = 0$ if and only if f_2 is the zero map.

Now let G be cyclic; it thus has periodic cohomology. Therefore (1) is split if and only if $f_0\colon H^0(G, \mathscr{C}_K) \to H^0(G, C_K)$ is the zero map. This is the map $f_0\colon \mathscr{C}_k/N_{K/k}\mathscr{C}_K \to C_K^G/N_{K/k}C_K$ induced by $f\colon \mathscr{C}_K \to C_K$ where $N_{K/k} = \sum_{\sigma \in G} \sigma$. Let $\mathscr{N}$ denote the map $C_K \to C_k$ induced by taking the norm of ideals from K to k. We then have two commutative diagrams:

$$\begin{tikzcd} C_K \arrow[r, "N"] \arrow[dr, "\mathscr{N}"'] & C_K \\ & C_k \arrow[u, "e"'] \end{tikzcd} \qquad \begin{tikzcd} \mathscr{C}_K \arrow[r, "f"] & C_K \\ \mathscr{C}_k \arrow[u, "e"] \arrow[r, "f"] & C_k \arrow[u, "e"] \end{tikzcd}$$

Here e is the usual extension map. It is an imbedding of idele class groups but on C_k has as kernel the set of classes which capitulate in K. The image of $f_0\colon \mathscr{C}_k/N\mathscr{C}_K \to C_K^G/NC_K$ is

$$f(\mathscr{C}_k) \cdot NC_K/NC_K = e(C_k)NC_K/NC_K.$$

Hence f_0 is trivial if and only if $e(C_k) \subseteq N(C_K) = e(\mathcal{N}(C_K))$, i.e., if and only if $C_k = \text{Ker } e \cdot \mathcal{N}(C_K)$. We have proved:

THEOREM 3. *Let $G = \text{Gal }(K/k)$ be cyclic, $e\colon C_k \to C_K$ the extension map, $\mathcal{N}\colon C_K \to C_k$ the norm map. Then $1 \to C_K \to \text{Gal }(K'/k) \to G \to 1$ is split if and only if $C_k = \text{Ker } e \cdot \mathcal{N}(C_K)$.*

Theorem 2 follows from this since $K \cap k' = k$ precisely when $C_k = \mathcal{N}(C_K)$.

COROLLARY 1. *If K is a cyclic extension of k, $k \subseteq K \subseteq k'$, and every ideal of k becomes principal in K, then the extension*

$$1 \to \text{Gal }(k'/K) \to C_k \to \text{Gal }(K/k) \to 1$$

is split and $C_k \cong \text{Gal }(k'/K) \oplus \text{Gal }(K/k)$.

Proof. Since $e\colon C_k \to C_K$ is the zero map, Theorem 3 implies that Gal (K'/k) is split over Gal (K/k). It follows easily that the quotient group Gal $(k'/k) \cong C_k$ is split over Gal (K/k).

In the same manner, letting $k'' = (k')'$, we have:

COROLLARY 2. *If k'/k is cyclic, then*

$$1 \to \text{Gal }(k''/k') \to \text{Gal }(k''/k) \to \text{Gal }(k'/k) \to 1$$

is split.

Note that a necessary condition for the splitting of (1) for arbitrary G can be derived from Theorem 3. If (1) is split, then

$$1 \to \text{Gal }(K'/K) \to \text{Gal }(K'/E) \to \text{Gal }(k/E) \to 1$$

is split for every field E between k and K. To those E such that K/E is cyclic Theorem 3 is applicable.

3. By the italicized remark in the proof of Theorem 1, it would seem that (1) would be split if we could produce enough inertia subgroups in G. Some simple group theoretic counterexamples show the limitations of such an approach. For odd prime p let U_3 be the nonabelian group of order p^3 and exponent p. Let $Z(U_3)$ be the center of U_3, isomorphic to C_p. Then we have $1 \to Z(U_3) \to U_3 \to G \to 1$ where the quotient G is isomorphic to $C_p \times C_p$. This is a nonsplit extension which splits on restriction to every proper subgroup of G. For a 2-group example, let $D_8 = \langle a, b \mid a^4 = b^2 = (ab)^2 = 1\rangle$ = the dihedral group, $C_4 = \langle x \mid x^4 = 1\rangle$, and $U_2 = D_8 \times C_4/\langle a^2x^2\rangle$, a group of order 16. Then $Z(U_2) \cong C_4$, $U_2/Z(U_2) \cong C_2 \times C_2$, and the extension $1 \to Z(U_2) \to U_2 \to C_2 \times C_2 \to 1$ is not split. But once again this extension splits on restriction to every proper subgroup of $C_2 \times C_2$. We have not attempted to determine if these groups U_p are realized as Gal (K'/k) for some K and k.

As an example of a positive result, we give:

THEOREM 4. *The extension* (1) *is split if*

(i) $G \simeq C_2 \times C_2$,

(ii) *the extension splits on restriction to every proper subgroup of* G, *and*

(iii) *at least one element of* G *acts on the* 2*-primary part of* C *by inversion.*

Proof. As a G-module, C is the direct sum of its 2-primary part and its odd-primary part, $C = {}_2C \oplus C'$. Hence $H^2(G, C) \cong H^2(G, {}_2C) \oplus H^2(G, C')$. But $H^2(G, C') = 0$, since these groups have relatively prime orders, and therefore $H^2(G, C) \simeq H^2(G, {}_2C)$ under the map induced by the projection $C \to {}_2C$. Consequently in the remainder of the proof we may assume that C itself is a 2-group.

Let $G = \{1, y_1, y_2, y_3\}$. By (ii) there exist $x_1, x_2, x_3 \in U$ such that $y_i = x_i \cdot C$ and $x_i^2 = 1$ in U. Assume that y_3 acts on C by inversion, $x_3cx_3 = c^{-1}$ for all $c \in C$. Since $x_1x_2x_3 \to y_1y_2y_3 = 1, x_1x_2x_3 = c \in C$. Hence $x_1x_2 = cx_3 = x_3'$ and if $(x_3')^2 = 1$, then $\{1, x_1, x_2, x_3'\} \subseteq U$ splits the extension. We have $(x_3')^2 = (cx_3)^2 = cx_3cx_3 = cc^{-1} = 1$ and the proof is complete.

COROLLARY. *If* $G = \text{Gal}\,(K/k)$ *is isomorphic to* $C_2 \times C_2$, *every proper subgroup of* G *is an inertia subgroup, and at least one of the three fields between* K *and* k *has odd class number, then* $\text{Gal}\,(K'/k)$ *splits over* G.

Proof. It suffices to verify requirement (iii) of the theorem. Let E lying between K and k have odd class number. Since $N_{K/E} = e \circ \mathcal{N}\colon C_K \to C_E \to C_K$, $N_{K/E}$ annihilates the 2-part of C_K. If $\text{Gal}\,(E/E) = \{1, \sigma\}$, then $N_{K/E} = 1 + \sigma$. Therefore σ acts as inversion on the 2-part of C_K.

REFERENCES

1. E. ARTIN AND J. TATE, *Class field theory*, W. A. Benjamin, New York, 1967.
2. M. HALL, *The theory of groups*, Macmillan, New York, 1959.
3. E. WEISS, *Cohomology of groups*, Academic Press, New York, 1969.
4. B. F. WYMAN, *Hilbert class fields and group extensions*, Scripta Math., vol. 29 (1973), pp. 141–149.

OHIO STATE UNIVERSITY
COLUMBUS, OHIO