ISRAEL JOURNAL OF MATHEMATICS, Vol. 52, No. 3, 1985

ON EQUIVALENCE OF NUMBER FIELDS

BY

JACK SONN

Department of Mathematics, Technion — Israel Institute of Technology, Haifa 32000, Israel

ABSTRACT

Let K be a field, G a finite group. G is called *K-admissible* iff there exists a finite dimensional K-central division algebra D which is a crossed product for G. Now let K and L be two finite extensions of the rationals Q such that for every finite group G, G is K-admissible if and only if G is L-admissible. Then K and L have the same degree and the same normal closure over Q.

There are two interesting notions of arithmetic equivalence of (finite) algebraic number fields which have been investigated in recent years. Two number fields K and L are called *arithmetically equivalent* iff their zeta functions ζ_K and ζ_L coincide. Gassmann [2] and more recently Perlis [7] have shown that arithmetically equivalent fields have the same classical invariants and the same normal closure over $\mathbf{Q}$, but are not necessarily isomorphic. A stronger notion of equivalence has been considered by Neukirch [5]. Let $\bar{\mathbf{Q}}$ denote the algebraic closure of $\mathbf{Q}$, $G_K = \mathrm{Gal}(\bar{\mathbf{Q}}/K)$ the absolute Galois group of K. Let $G_K \simeq G_L$ (as topological groups with the profinite topology). Neukirch [5] proved that if K, L are normal over $\mathbf{Q}$, then $K = L$, and asked if $K \simeq L$ in general. This was proved independently by Ikeda, Iwasawa and Uchida (see [12]). In this paper we introduce a third notion of equivalence of number fields, whose relation to arithmetic equivalence is not clear. A finite group G is called K-admissible iff there exists a finite dimensional K-central division algebra D which is a crossed product for G; i.e. D has a maximal subfield which is Galois over K and whose Galois group is isomorphic to G. The notion of admissibility was introduced by Schacher [8] and investigated by him and others, particularly the question of $\mathbf{Q}$-admissibility. (See [1, 10, 11] and the references cited there.) Schacher [8] showed that if G is $\mathbf{Q}$-admissible, then G is *Sylow-metacyclic*, i.e. all its Sylow subgroups are metacyclic (cyclic by cyclic). A conjecture has emerged that every

Received January 9, 1985

Sylow-metacyclic group is **Q**-admissible. This has been proved for solvable groups [10] and reduced to a list of "almost simple" groups in the nonsolvable case [1]. Thus conjecturally at least, the set of **Q**-admissible groups is known. If K is a number field different from **Q**, can one characterize the K-admissible groups? This seems hopelessly difficult in general. As we will see below, for any $K \neq \mathbf{Q}$, there is a group which is not Sylow-metacyclic and which is K-admissible. Thus Q is characterized among all number fields by the set of groups which are **Q**-admissible. We are thus led to the following question: is K characterized up to isomorphism by the set of K-admissible groups? Or, let K and L be number fields such that for every finite group G, G is K-admissible if and only if G is L-admissible. Are K and L isomorphic (conjugate)? In light of the work of Gassmann and Perlis mentioned above, the answer is probably no. However, we will show that K and L have the same normal closure and the same degree over **Q**. In particular, if K and L are normal over **Q**, then $K = L$. We use the following criteria for K-admissibility [8]: G is K-admissible iff there exists a Galois extension F/K with $G(F/K) \simeq G$, and for every prime $p \mid |G|$, there exist at least two primes v_1, v_2 of K, such that the local Galois group $G(F_{v_i}/K_{v_i})$ contains a Sylow p-subgroup of G, $i = 1, 2$.

In the course of the proof we will also use the following known facts:

(a) Tamely ramified Galois extensions of local fields have metacyclic Galois groups.

(b) If k is a finite extension of $\mathbf{Q}_p$ not containing the pth roots of unity, then the Galois group of the maximal p-extension of k over k is a free pro-p group on $[k : \mathbf{Q}_p] + 1$ generators [9, II-30].

(c) A theorem of Neukirch [6, p. 115] which states that given a number field k, a prime p such that k does not contain the pth roots of unity, a finite p-group G, a finite set S of primes of k, and for each prime v in S, a finite Galois extension $K(v)/k_v$ with $G(K(v)/k_v)$ isomorphic to a subgroup of G, there exists a finite Galois extension K/k with $G(K/k) \simeq G$ such that $K_v = K(v)$ for each v in S, where K_v denotes the completion of K at a divisor of v in K.

We are indebted to Gary Seitz for the idea of the proof of the following lemma, and also to David Chillag for supplying a step in the proof.

LEMMA 1. *Let G be a finite group, N a normal subgroup $\neq G$, H a subgroup of G not containing N. Suppose that for every cyclic subgroup C of N, at most one double coset CgH of (C, H) in G is not an ordinary coset gH. Then for some such C, $CH = G$.*

PROOF. Let C be a cyclic subgroup of N not contained in H. Then $CH \neq H$

so for all $g \in G$ with $g \notin CH$, we have $CgH = gH$, $g^{-1}Cg \subset H$. If $NH \neq G$, then for $g \notin NH$, we have $g^{-1}Cg \subset H$ for *all* C. Since $C \subseteq N \lhd G$, we have also $g^{-1}Cg \subset N$, so $g^{-1}Cg \subset H \cap N$. Thus g conjugates $N \neg (H \cap N)$ into $H \cap N$. This is impossible unless $H \cap N = N$, i.e. $H \supset N$, contrary to hypothesis. We are therefore reduced to the case $NH = G$. Now N acts on the (left) cosets of H by left multiplication. $NH = G$ means that N acts transitively. By [4, p. 536, Satz 13.4] some element c of N acts fixed point free, so for $C = \langle c \rangle$, *no* double coset CgH is a left coset. But since at most one double coset is not a left coset, it follows that $CH = G$. □

THEOREM 1. *Let K and L be number fields such that for every finite group G, G is K-admissible if and only if G is L-admissible. Then K and L have the same normal closure over the rationals* **Q**.

PROOF. Assume that the normal closures $\bar{K}$ and $\bar{L}$ do not coincide. Without loss of generality assume $\bar{K} \not\subseteq \bar{L}$. Then $K \not\subseteq \bar{L}$.

Case 1. $L = \mathbf{Q}$. Then $\bar{L} = Q$. Take any odd prime p which splits completely in K. Let B be any two generator p-group which is not metacyclic, for example the wreath product $C_p \wr C_p$ where C_p is a cyclic group of order p. Then B is realizable as a Galois group over $\mathbf{Q}_p$ (see e.g. [9, II–30]) hence over K_v, K_w, where v, w are divisors of p in K, and $K_v \simeq K_w \simeq \mathbf{Q}_p$ are the respective completions. By a theorem of Neukirch [6, p. 115], there is a Galois extension F/K with $G(F/K) \simeq B \simeq G(F_v/K_v) \simeq G(F_w/K_w)$. Hence B is K-admissible. On the other hand, B is a nonmetacyclic p-group, hence is not Sylow-metacyclic, hence is not **Q**-admissible.

Case 2. $L \neq \mathbf{Q}$. Then $\bar{L} \neq \mathbf{Q}$. Let $M = \bar{K}\bar{L}$, $G = G(M/\mathbf{Q})$, $H = G(M/K)$, $N = G(M/\bar{L})$. Let C be a cyclic subgroup of N not contained in H (by hypothesis N is not contained in H). By Chebotarev's density theorem, there exists a prime V of M (unramified) whose decomposition group is C. Let p be the prime of **Q** dividing V. Then since $C \subset N$, p splits completely in $\bar{L}$. Since $C \not\subseteq H$, p does not split completely in K.

Case 2.1. For some choice of C as above, p remains prime in K. Then p has only one divisor in K, hence K has at most one completion over which a nonmetacyclic p-group is realizable as a Galois group. Let B, as in Case 1, be a two generator nonmetacyclic p-group. Then exactly as in Case 1, B is L-admissible but not K-admissible.

Case 2.2. For every choice of C, p does not remain prime in K. We claim that p has in K at least two prime divisors of degree greater than 1. It is known that the degrees f_i of the prime divisors v_i of p in K have the following characterization in terms of Galois groups [3, II, §23]: let $Cg_1H, \dots, Cg_tH$ be the double cosets of (C, H) in G. Then p has t prime divisors $v_1, \dots, v_t$ in K of degrees $f_1, \dots, f_t$ respectively, where $f_i = |Cg_iH|/|H|$, $i = 1, \dots, t$. Since for every choice of C, p does not remain prime in K we have $CH \neq G$ for every choice of C. By the lemma, we conclude that for some C, at least two double cosets are not ordinary left cosets of H, hence at least two of the f_i are greater than 1, say f_1, f_2, and let v_1, v_2 be the corresponding primes. Take any three generator p-group (even abelian) A. Since K_{v_i} does not contain the pth roots of unity, and $f_1, f_2 > 1$, A is realizable as a Galois group over K_{v_i}, $i = 1, 2$. As before, we conclude that A is K-admissible. On the other hand, A is not L-admissible, since it is not realizable over any completion of L. Indeed, since A is not metacyclic, the only completions over which it could appear are the divisors of p in L. But p splits completely in L, and three generator p-groups are not realizable over $\mathbf{Q}_p$. □

REMARK. It is perhaps worthwhile to record the following arithmetic version of Lemma 1, which follows immediately from the preceding proof.

COROLLARY. *Let K and L be number fields with L normal over $\mathbf{Q}$ and K not contained in L. Then there exist (infinitely many) rational primes p which split completely in L, such that p either remains prime in K or has at least two divisors in K of degree bigger than* 1.

Let G be a finite group, C, D subgroups of G. Let $Cx_1D, \dots, Cx_rD$ be the double cosets of the pair (C, D) in G, ordered in terms of decreasing size (cardinality):

$$|Cx_1D| \geqq |Cx_2D|\,| \geqq \cdots \geqq |\,|Cx_rD|.$$

Set $n(C, D) = |Cx_2D|$. (If $r = 1$, set $n(C, D) = 1$.)

If H is a subgroup of G, then $\mathrm{core}(H) = \bigcap_{x \in G} xH\bar{x}^1$.

LEMMA 2. *Let G be a finite group, H, H' subgroups of G such that* $\mathrm{core}(H) = \mathrm{core}(H') = 1$. *If $n(C, H) = n(C, H')$ for every cyclic subgroup C of G, then* $|H| = |H'|$.

PROOF. (D. Chillag). The proof will only use the assumption $n(C, H) = n(C, H')$ for all subgroups C of prime order. We first note that

$$|CxH| = |CxHx^{-1}| = |C|\,|H|/|C \cap xHx^{-1}|$$

$$= \begin{cases} |C|\,|H| = p\,|H| & \text{if } C \cap xHx^{-1} = 1 \\ |C|\,|H|/p = |H| & \text{if } C \cap xHx^{-1} \neq 1 \end{cases}$$

where $p = |C|$. Thus

$$n(C, H) = |H| \text{ or } p\,|H| \quad \text{and} \quad n(C, H') = |H'| \text{ or } p\,|H'|.$$

Case 1. For some C, $n(C, H) = |H|$ and $n(C, H') = |H'|$.

Case 2. For some C, $n(C, H) = p\,|H|$ and $n(C, H') = p\,|H'|$. In both cases we are done.

Case 3. For every C, $n(C, H) = p\,|H|$ and $n(C, H') = |H|$, or $n(C, H) = |H|$ and $n(C, H') = p\,|H'|$. Suppose $|H| < |H'|$. Then $|H'| = p\,|H|$, and this holds for every prime p dividing $|G|$, by Cauchy's theorem. Thus we may assume that G is a p-group, in which case we may take C in the center of G. Then $C \cap H = C \cap H' = 1$, so

$$n(C, H) = |C|\,|H|/|x^{-1}Cx \cap H| = p\,|H|,$$

$$n(C, H') = |C|\,|H|/|x^{-1}Cx \cap H'| = p\,|H'|,$$

hence $|H| = |H'|$, contradiction.

THEOREM 2. *Let K and L be number fields such that for every finite group G, G is K-admissible if and only if G is L-admissible. Then K and L have the same degree over* $\mathbf{Q}$.

PROOF. Let N be the common normal closure of K and L over $\mathbf{Q}$, by virtue of Theorem 1. Let $H = G(N/K)$, $H' = G(N/L)$. Then $\operatorname{core}(H) = \operatorname{core}(H') = 1$. Assume the theorem false. Then $|H| \neq |H'|$, so by Lemma 2, there exists a cyclic subgroup C of G such that $n(C, H) \neq n(C, H')$. Let V be an unramified prime of N whose decomposition group is C, by virtue of Chebotarev's density theorem. Let p be the prime of $\mathbf{Q}$ below V. Assume without loss of generality that $n(C, H) < n(C, H')$. Let $v_1, \dots, v_r$ be the primes of K dividing p, $v'_1, \dots, v'_t$ the primes of L dividing p, $f_i = \deg v_i$, $f'_i = \deg v'_i$. We argue as in the proof of Theorem 1: we may assume that p was chosen so that the completions K_{v_i} and $L_{v'_i}$ do not contain the pth roots of unity. Thus the Galois group of the maximal p-extension of K_{v_i} (resp. $L_{v'_i}$) over K_{v_i} (resp. $L_{v'_i}$) is free pro-p of rank $f_i + 1$ (resp. $f_{i'} + 1$) [9, II–30]. Take B to be any non-metacyclic p-group of rank $f'_2 + 2$. Then B is realizable over $L_{v'_1}$ and $L_{v'_2}$, and is therefore L-admissible by [6, p. 115]. On the other hand, since $f_2, \ldots, f_r < f_2'$, B is realizable over at most one completion (K_{v_1}) of K, hence B is not K-admissible, contradiction. □

REFERENCES

1. D. Chillag and J. Sonn, *Sylow-metacyclic groups and* **Q**-*admissibility*, Israel J. Math. **40** (1981), 307–323.

2. F. Gassmann, *Bemertungen zu der vorstehenden Arbeit von Hurwitz*, Math. Z. **25** (1926), 665–675.

3. H. Hasse, *Zahlbericht*, Physica-Verlag, Wurzburg/Vienna, 1970.

4. B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.

5. J. Neukirch, *Kennzeichung der p-adischen und der endlichen algebraischen Zahlkorper*, Inv. Math. **6** (1969), 296–314.

6. J. Neukirch, *Uber das Einbettungsproblem der algebraischer Zahlentheorie*, Inv. Math. **21** (1973), 59–116.

7. R. Perlis, *On the equation* $\zeta_k(s) = \zeta_{k'}(s)$, J. Number Theory **9** (1977), 342–360.

8. M. Schacher, *Subfields of division rings I*, J. Algebra **9** (1968), 451–477.

9. J. P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Math. No. 5, Springer-Verlag, Berlin, 1965.

10. J. Sonn, **Q**-*admissibility of solvable groups*, J. Algebra **84** (1983), 411–419.

11. L. Stern, **Q**-*admissibility of* S_5^+, Comm. Alg., to appear.

12. K. Uchida, *Isomorphisms of Galois groups*, J. Math. Soc. Japan **28** (1976), 617–620.