J. Austral. Math. Soc. (*Series A*) **57** (1994), 17–34

KRONECKER CLASSES OF FIELDS AND COVERING SUBGROUPS OF FINITE GROUPS

CHERYL E. PRAEGER

(Received 7 September 1993)

Communicated by L. G. Kovács

Abstract

Kronecker classes of algebraic number fields were introduced by W. Jehne in an attempt to understand the extent to which the structure of an extension $K : k$ of algebraic number fields was influenced by the decomposition of primes of k over K. He found an important link between Kronecker equivalent field extensions and a certain covering property of their Galois groups. This paper surveys recent contributions of Group Theory to the understanding of Kronecker equivalence of algebraic number fields. In particular some group theoretic conjectures related to the Kronecker class of an extension of bounded degree are explored.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): 20B25, 12F10.

1. Introduction

1A. Covering subgroups of finite groups In undergraduate courses in Group Theory, students are often asked to prove the following assertion: If U is a proper subgroup of a finite group G then G is not equal to the set-theoretic union $\bigcup_{g\in G} U^g$ of the conjugates of U. This is very easy to prove since the number of distinct conjugates U^g, $g \in G$, is equal to the index $|G : N_G(U)|$ in G of the normaliser $N_G(U)$ of U, and this in turn is at most $|G : U|$. Then as all conjugates U^g have the same cardinality as U, and as each conjugate contains the identity element, we have $|\bigcup_{g\in G} U^g| < |G : U|.|U| = |G|$.

The reason why G cannot be 'covered' by the conjugates of U is simply that there are not enough of them. If we had available in G more subgroups isomorphic but not conjugate to U, might it then be possible to cover G using these subgroups in addition to the conjugates of U? This is certainly possible in some cases. For example, if G

is the additive group of a finite dimensional vector space over a finite field, and if U is the additive group of a non-zero proper subspace, then as every vector lies in some subspace of dimension $d := \dim U$, G is covered by the union of such subspaces. In this example, for each pair (U, U') of additive subgroups of d-dimensional subspaces, there is an automorphism of G, that is a nonsingular linear transformation of the vector space, which maps U to U', so G is covered by the union of all images of U under automorphisms of G. We shall call such subgroups U of G covering subgroups.

DEFINITION 1.1. Let G be a finite group, U a subgroup of G, and A a subgroup of the automorphism group Aut G of G containing the group Inn G of inner automorphisms. If the union $U^A = \bigcup_{a \in A} U^a$ of the images of U under elements of A is equal to G then U is said to be an *A-covering subgroup* of G. A subgroup is called a *covering subgroup* of G if it is an (Aut G)-covering subgroup.

Questions about set-theoretic unions of subgroups of groups arise naturally in connection with the Galois groups of certain extensions of algebraic number fields, and such applications will be discussed later in the paper.

Rolf Brandl [3] studied various properties of covering subgroups. He looked in particular at examples of covering subgroups of soluble groups and conjectured that a group with a soluble covering subgroup must itself be soluble. Brandl showed that a minimal counterexample to his conjecture had to be a non-abelian simple group. The proof of the conjecture was completed by Jan Saxl [29] who showed that finite non-abelian simple groups have no proper covering subgroups.

THEOREM 1.2. (Saxl) *A finite non-abelian simple group has no proper covering subgroups.*

COROLLARY 1.3. (Brandl, Saxl) *If a finite group G has a soluble covering subgroup, then G is soluble.*

It is easily seen that covering subgroups of a group G are those subgroups which contain at least one element from every (Aut G)-conjugacy class in G. In applications other than those discussed in the next subsection a generalisation of covering subgroups has arisen, namely subgroups which contain at least one element from every (Aut G)-conjugacy class of elements of prime power order in G (see [6, 9]).

DEFINITION 1.4. Let G be a finite group, U a subgroup of G, and A a subgroup of Aut G containing Inn G. If U contains an element from every A-conjugacy class of elements of prime power order in G, then U is said to be an *A-prime-power-covering subgroup* of G. A subgroup is called a *prime-power-covering subgroup* of G if it is an (Aut G)-prime-power-covering subgroup.

Bob Guralnick [9] noted that similar techniques to those used in [29] could be used to show that a finite non-abelian simple group has no proper prime-power-covering subgroups.

THEOREM 1.5. (Guralnick, Saxl) *A finite non-abelian simple group has no proper prime-power-covering subgroups.*

Theorems 1.2 and 1.5 have proved very useful in connection with the group theoretic problems discussed later in this paper. One easy application of them is the following result.

THEOREM 1.6. *Let G be a finite group, A a subgroup of* Aut G *containing* Inn G, *and L/K an A-chief factor of G. Suppose that L/K is a direct power of a simple group S. If U is an A-covering subgroup (respectively A-prime-power-covering subgroup) of G, then $(U \cap L)K/K$ is an $\bar{A}$-covering subgroup (respectively $\bar{A}$-prime-power-covering subgroup) of L/K and is a direct power of S, where $\bar{A}$ is the group of automorphisms of L/K induced by A.*

The case where U is an A-covering subgroup was proved in [25, Theorem 2.1], see also [4] and [9, Section 6]. The proof for A-prime-power-covering subgroups is similar; a sketch of the proof is given to illustrate the techniques, especially the way in which Theorem 1.5 can be used.

PROOF. Suppose that U is an A-prime-power-covering subgroup. Then UK/K is easily shown to be an A^*-prime-power-covering subgroup of G/K, where A^* is the group of automorphisms of G/K induced by A, and consequently we may assume that $K = \{1\}$. Then, since U contains a member of each A-conjugacy class in G of elements of prime power order, $U \cap L$ contains a member of each $\bar{A}$-conjugacy class in L of elements of prime power order, that is, $U \cap L$ is an $\bar{A}$-prime-power-covering subgroup of L. If L is soluble then L is an elementary abelian p-group for some prime p, $S \cong Z_p$, and $U \cap L$ is of course isomorphic to a direct power of S. So we may assume that $L = S_1 \times \ldots \times S_k \cong S^k$ for some finite non-abelian simple group S and integer $k \geq 1$. Let V_i be the projection of $U \cap L$ into S_i for $1 \leq i \leq k$. If $V_i < S_i$ for some i, then by Theorem 1.5, $V \cong V_i$ is not a prime-power-covering subgroup of $S \cong S_i$, and so there exists an element $s \in S$ of prime power order which does not lie in V^α for any $\alpha \in$ Aut S. It follows that the k-tuple $(s, \ldots, s)$ does not lie in any $\bar{A}$-conjugate of $U \cap L$. This contradiction proves that $V_i = S_i$ for all i, and hence that $U \cap L$ is isomorphic to some direct power of S.

An immediate corollary of this result is that the set of composition factors of U is the same as that for G.

https://doi.org/10.1017/S1446788700036028 Published online by Cambridge University Press

COROLLARY 1.7. *Let G, A, U be as in Theorem* 1.6. *Then G and U have the same set of composition factors.*

Examples of covering subgroups arising from elementary abelian groups were given above. There are of course many examples of covering subgroups of insoluble groups also. One of the smallest of these is the following.

EXAMPLE 1.8. Let $G = G_1 \times \ldots \times G_5 \cong A_5^5$, $U = G_1 \times G_2 \times G_3 \times D$ where D is a diagonal subgroup of $G_4 \times G_5$, and $A = \text{Aut } G \cong S_5$ wr S_5. There are exactly four S_5-conjugacy classes of elements in A_5, and consequently at least two entries of each element $(g_1, \ldots, g_5) \in G$ are in the same S_5-class. This means that each element of G lies in some A-conjugate of U, and hence that U is an A-covering subgroup of G.

This example illustrates some fairly general features of insoluble groups with covering subgroups. Suppose that U is an A-covering subgroup of G. The largest A-invariant subgroup of U is the *A-core* $U_A := \bigcap_{a \in A} U^a$ of U, and the covering property might be expected to give structural information only about the quotient G/U_A. So let us assume that $U_A = \{1\}$, that is, that U is *A-core free*. Clearly any maximal subgroup of G containing U is also an A-covering subgroup so suppose that U is an A-core free maximal subgroup of G. If G has an insoluble minimal A-invariant subgroup L, then [27, Proposition 3.1] shows that L is the direct product of at least 5 minimal normal subgroups N_i of G, say $L = N_1 \times \ldots \times N_s$ with $s \geq 5$, and for some distinct i, j, $U = D \times \prod_{l \neq i,j} N_l$ with D a diagonal subgroup of $N_i \times N_j$. Example 1.8 is therefore a minimal example exhibiting this behaviour.

1B. Kronecker classes of algebraic number fields We shall consider algebraic number fields K (that is subfields of the field $\mathbb{C}$ of complex numbers which are finite extensions of the field $\mathbb{Q}$ of rational numbers) and their rings of integers $\mathcal{O}_K$. (Recall that $\mathcal{O}_K$ is the ring of algebraic integers contained in K.) If $K : k$ is an extension of algebraic number fields, then we have a corresponding inclusion $\mathcal{O}_k \subseteq \mathcal{O}_K$ for the rings of integers. Each prime ideal p of $\mathcal{O}_k$, often called a 'prime of k', corresponds to an ideal $p\mathcal{O}_K$ of $\mathcal{O}_K$ which factorises as a product $\prod P_i^{e_i}$ of a certain number of prime ideals P_i of $\mathcal{O}_K$ ('primes of K') and the prime ideals P_i and their multiplicities e_i are uniquely determined by p up to the order of the factors in the product. Each prime P of K occurs in the factorization of exactly one prime p of k, and P is called a *prime divisor* of p in K. Further, given P, the prime p can be recovered by means of the norm map $N\colon K \to k$. The image of P is $N(P) = p^f$ for a certain positive integer f, called the *(relative) degree* of P with respect to k.

This theory may be found in many standard reference books on algebraic number theory, for example Serge Lang's book [21]. The basic problem we shall discuss is: *to what extent is an extension $K : k$ of algebraic number fields determined by the nature of the prime factorization in K of the primes of k?* The first positive contribution was

due to Kronecker [20] who in 1880 showed that two extensions $K : k$ and $L : k$ of the same (rational) prime degree have the same Galois hull (sometimes called the normal closure) if every prime of k has the same number of prime divisors with relative degree 1 in K as in L. In particular, if $K : k$ is a Galois extension of prime degree, then $K : k$ is completely determined (among field extensions of k of the same prime degree) by the number of prime divisors in K of relative degree 1 of each prime p of k. This result led to a very fruitful development in algebraic number theory. We define the Kronecker set of a field extension as follows.

DEFINITION 1.9. The *Kronecker set* of an extension $K : k$ of algebraic number fields is the set $D(K : k)$ of all primes of k having at least one prime divisor of relative degree 1 in K.

Kronecker showed that a Galois extension of prime degree is determined by its Kronecker set, and in 1916 Bauer [1] was able to show that all finite Galois extensions are characterised (in the class of Galois extensions) by their Kronecker sets. However in 1926 Gassmann [8] produced an example of two nonconjugate extensions of the field of rational numbers, each of degree 180, which had the same Kronecker set. This example of Gassmann effectively stopped work in the area for almost 40 years until, in the 1960's, Kronecker's basic concepts and ideas were again studied by several mathematicians (see [13]). Wolfram Jehne [13] introduced the concept of Kronecker equivalence of algebraic number fields.

DEFINITION 1.10. Two extensions K and L of an algebraic number field k are said to be *Kronecker equivalent over* k, written $K \sim_k L$, if the Kronecker sets $D(K : k)$ and $D(L : k)$ differ by only a finite set of primes, that is, $K \sim_k L$ if and only if $D(K : k)$ and $D(L : k)$ have finite symmetric difference.

Clearly Kronecker equivalence is an equivalence relation; the equivalence classes are called *Kronecker classes*, and the Kronecker class over k containing K is denoted by $\mathscr{K}_k(K)$.

1C. Kronecker classes and groups Wolfram Jehne [13] showed that it is possible to translate the notion of Kronecker equivalence into a precise statement about Galois groups. Suppose that K and L are finite extensions of an algebraic number field k, and let M be a finite Galois extension of k containing K and L. Let A be the Galois group of $M : k$ and let U, V be the 'fixed groups' of K, L (that is the Galois groups of $M : K$, $M : L$) respectively. Then Jehne showed that

$$K \sim_k L \qquad \text{if and only if} \qquad U^A = V^A,$$

where we write $U^A = \bigcup_{a \in A} U^a$ and $V^A = \bigcup_{a \in A} V^a$. In particular, if $K : k$ is Galois then $U^A = U$ and in this case K and L are Kronecker equivalent over k if and only if $U = V^A$, that is, V is an A-covering subgroup of U.

https://doi.org/10.1017/S1446788700036028 Published online by Cambridge University Press

Moreover, this group theoretic condition is a sufficient condition for the existence of Kronecker equivalent extensions of algebraic number fields in the following sense. If A is a group with subgroups U, V such that $U^A = V^A$, then there is an algebraic number field k and a finite Galois extension M of k such that the fixed fields K, L of U, V respectively are Kronecker equivalent over k. However, given A and its subgroups U, V, and given an algebraic number field k, it is not clear whether a Galois extension M of k exists with these properties. Certainly, if U is a normal subgroup of A, and if an extension $K : k$ of algebraic number fields is given with Galois group A/U, then a Galois extension $M : k$ with M containing K and with Galois group A may or may not exist; its existence may depend on arithmetic properties of $K : k$. Examples of this have been given by Norbert Klingen (see Theorem 3.2) for $K : k$ of degree 4.

Jehne [13, 14] began a systematic investigation of Kronecker classes using this link with group theory, aiming to understand their structure and the behaviour of some of their fundamental invariants. He observed [13, p. 286] that each Kronecker class $\mathscr{K}$ over k contains only a finite number of minimal fields (that is, minimal by inclusion) and that each of these minimal fields generates the same Galois hull $M(\mathscr{K})$ over k, called the *Galois hull of* $\mathscr{K}$. Thus two important invariants of $\mathscr{K}$ are the *width* $\omega(\mathscr{K})$, that is the number of $M(\mathscr{K})$-conjugacy classes of minimal fields in $\mathscr{K}$, and the *socle number* $\mu(\mathscr{K})$, that is the number of $M(\mathscr{K})$-conjugacy classes of subfields of $M(\mathscr{K})$ which lie in $\mathscr{K}$.

We illustrate these concepts with two examples. The first one, related to Gassmann's example, gives three Kronecker equivalent pairwise nonconjugate extensions of the rationals, two of which are extensions of degree 180 and one of degree 360. The second example shows that, even if the width and the socle number are both equal to 1, the Kronecker class may have more than one element, that is it may contain fields outside of its Galois hull. Thus the Galois hull of $\mathscr{K}$ cannot always provide complete information about the Kronecker class $\mathscr{K}$.

EXAMPLE 1.11. In the symmetric group $A = S_6$ of degree 6, the subgroups

$$U_1 = \{1, (12)(34)\},$$
$$U_2 = \{1, (12)(34), (13)(24), (14)(23)\}, \text{ and}$$
$$U_3 = \{1, (12)(34), (12)(56), (34)(56)\},$$

are such that $U_1^A = U_2^A = U_3^A$ is the union of the identity permutation and the set of all permutations which are products of two cycles of length 2. Let $M : \mathbb{Q}$ be a Galois extension of the rationals of degree 720 with Galois group A. Then the fixed fields K_1, K_2, K_3 of U_1, U_2, U_3 respectively are all in the same Kronecker class $\mathscr{K}$ over $\mathbb{Q}$ and $\mathscr{K}$ has Galois hull M. Moreover $\mathscr{K}$ has width 2, K_2 and K_3 being representatives of the two classes of minimal fields in $\mathscr{K}$ (each of degree 180 over $\mathbb{Q}$), and $\mathscr{K}$ has

socle number 3, K_1, K_2, K_3 being representatives of the classes of subfields of M lying in $\mathscr{K}$.

EXAMPLE 1.12. In the alternating group $A = A_4$, the subgroup $V = \{1, (12)(34)\}$ is an A-covering subgroup of the normal subgroup $U = \{1, (12)(34), (13)(24), (14)(23)\}$ of A. There is a Galois extension $M : k$ with Galois group A. Let K, L be the fixed fields of U, V respectively. Then K and L are in the same Kronecker class $\mathscr{K}$ despite the fact that $\mathscr{K}$ has Galois hull $M(\mathscr{K}) = K$, width 1 and socle number 1. In fact K is the only minimal field in $\mathscr{K}$.

Jehne [13, pp. 294-297] has constructed Kronecker classes with arbitrarily large width.

2. Infinite Kronecker classes versus quadratic extensions

In [13] Jehne proved the existence of infinite Kronecker classes.

THEOREM 2.1. [13, Theorem 3] *Let $\mathscr{K}$ be the Kronecker class of K over k, where $K : k$ is a finite extension of algebraic number fields. If either*

(a) *$K : k$ admits a nontrivial automorphism of odd order, or*

(b) *$K : k$ admits a cyclic or quaternion subgroup of automorphisms of order 8,*

then $\mathscr{K}$ is infinite.

This very general result left open the question of whether extensions having automorphism groups of exponent 2 or 4 could give rise to infinite Kronecker classes. Much effort was expended on the case of quadratic extensions $K : k$.

Suppose that $K : k$ is a quadratic extension and that L is Kronecker equivalent to K over k, with $L \neq K$. Then $K : k$ is a Galois extension and so L contains K. Choose L to be minimal with respect to the property

$$K \sim_k L, \qquad K \neq L.$$

Let M be the Galois hull of $L : k$, let A be the Galois group of $M : k$, and let G, U be the fixed groups of K, L respectively. Then G is a normal subgroup of A of index 2 and U is a proper $\bar{A}$-covering subgroup of G, where $\bar{A}$ is the group of automorphisms of G induced by A. Wolfram Jehne and Norbert Klingen [13, 16, 17] were able to show that the group G must be simple, and that it could not belong to several of the infinite families of finite simple groups. Finally the result of Saxl, Theorem 1.2, proved several years later, showed that no such proper subgroup U of G exists.

THEOREM 2.2. (Jehne, Klingen, Saxl) *Let $K : k$ be a quadratic extension of algebraic number fields. Then the Kronecker class of K over k contains only the field K.*

This was the first situation where a nontrivial extension of algebraic number fields was proved to generate a finite Kronecker class. The general case of extensions of algebraic number fields admitting a nontrivial Galois group of exponent dividing 4 remains open; it is not known when the corresponding Kronecker class is infinite. Some results are available for extensions of small degree and will be discussed in the next section.

3. Quartic Galois extensions

In an attempt to discover if there were other types of extensions which guaranteed a finite Kronecker class, quartic Galois field extensions $K : k$ were investigated. Suppose that there is a second field L in the Kronecker class $\mathscr{K}_k(K)$ of such an extension. Let M be the Galois hull of $\langle K, L\rangle$ over k, let A be the Galois group of $M : k$, and let G, U be the fixed groups of K, L respectively. Then G is a normal subgroup of A of index 4, and $G = U^A = \bigcup_{a\in A} U^a$ by the result of Jehne [13]. In particular U is a subgroup of G, or equivalently K is a subfield of L. Further, any subgroup U_1 such that $U \leq U_1 \leq G$ clearly satisfies $G = U_1^A$, and hence any intermediate field L', $K \leq L' \leq L$, lies in $\mathscr{K}_k(K)$. Thus we may assume that L is an atomic extension of K, or equivalently that U is a maximal subgroup of G. It was shown in [25] that there were essentially two group theoretic possibilities.

THEOREM 3.1. [25, Theorem 4.3] *Let A be a finite group with a normal subgroup G of index 4 such that G has an A-covering maximal subgroup U with trivial A-core $U_A = \bigcap_{a\in A} U^a = \{1\}$. Then $A = N.S$ where $N \cong Z_3 \times Z_3$ is normal in A and S is Z_8 or Q_8 according as A/G is Z_4 or $Z_2 \times Z_2$. Further $G = N.Z_2$ and $U \cong S_3$.*

Thus if $\mathscr{K}_k(K) \neq \{K\}$, that is if $K : k$ is not *absolutely rigid* in the sense of Klingen [18], then K must be Kronecker equivalent over k to some non-Galois cubic extension of itself. Norbert Klingen (see [18] or [25, Remark 4.2]) showed that there exist quartic Galois extensions $K : k$ of algebraic number fields such that K is Kronecker equivalent to some cubic extension of itself both in the case where $K : k$ is a cyclic extension and also where $K : k$ is an elementary abelian extension. Moreover he obtained an explicit characterisation of absolutely rigid quartic Galois extensions.

THEOREM 3.2. (Klingen) *Let $K : k$ be a quartic Galois extension of algebraic number fields. Then $\mathscr{K}_k(K) = \{K\}$ if and only if one of the following holds.*

(a) *$K : k$ is a cyclic extension and in some local extension $K_p : k_p$, where p is a finite or infinite place, -1 is not a norm, or*

(b) *$K = k(\sqrt{d_1}, \sqrt{d_2})$ with d_1, d_2 nonzero elements of k, and the quadratic form*

$$d_1x^2 + d_2y^2 + (d_1d_2)^{-1}z^2$$

https://doi.org/10.1017/S1446788700036028 Published online by Cambridge University Press

is not k-isomorphic to $x^2 + y^2 + z^2$.

An analogue to Theorem 3.1 for octic Galois extensions was proved in [27].

4. Bounded degree extensions

The examples of infinite Kronecker classes over an algebraic number field k constructed by Jehne in [13] consist entirely of extensions of k of bounded degree. These examples, together with the results discussed in the previous sections, suggest that the Kronecker class $\mathscr{K}_k(K)$ of an extension $K : k$ of degree n might have the property that the degree of $L : k$, for fields $L \in \mathscr{K}_k(K)$, is bounded by some function of n. The corresponding conjecture for groups was made by Peter Neumann and the author in 1988.

CONJECTURE 4.1. (Neumann, Praeger) *There is an integer function f such that, if A is a finite group with subgroups U, V such that $|A : U| = n$ and $\bigcup_{a\in A} U^a = \bigcup_{a\in A} V^a$, then $|A : V| \leq f(n)$.*

CONJECTURE 4.1′. *There is an integer function f such that, if $K : k$ is an extension of degree n of algebraic number fields and $L \sim_k K$, then $|L : k| \leq f(n)$.*

Theorem 2.2 implies that we may take $f(2) = 2$. A proof of Conjecture 4.1′ would follow from a proof of Conjecture 4.1 on taking A to be the Galois group of some Galois extension of k containing both K and L, and taking U, V to be the fixed groups of K, L respectively.

The results about extensions of small degree and a theorem of Bob Guralnick suggest that bounds on the degrees of extensions in a Kronecker class $\mathscr{K}$ may be provable under certain additional assumptions on the Galois group of $M(\mathscr{K}) : k$. The following theorem about the case where $|K : k| = n$ and the Galois group of $M(\mathscr{K}) : k$ is A_n or S_n was proved by Guralnick [9] for $n \geq 5$, follows from [27, Corollary to Theorem 3] for $n = 3, 4$, and from Theorem 2.2 for $n = 2$. Guralnick's proof relies heavily on group representation theory.

THEOREM 4.2. *Let $K : k$ be an extension of algebraic number fields of degree $n \geq 2$ such that the Galois hull $M(\mathscr{K}) : k$ of the Kronecker class $\mathscr{K}$ of K over k has Galois group A_n or S_n. Then either $\mathscr{K}$ consists entirely of the conjugates of K, or $n = 3$ or 5 and the Galois group is A_n.*

Further work [10] in this direction is proceeding for other families of potential Galois groups of $M(\mathscr{K}) : k$. A conjecture closely related to Conjecture 4.1 is the following about covering subgroups.

https://doi.org/10.1017/S1446788700036028 Published online by Cambridge University Press

CONJECTURE 4.3. (Neumann, Praeger [19, 11.71]) *There is an integer function g such that, if G is a finite group, A is a group of automorphisms of G containing* Inn G *as a subgroup of index n, and U is an A-covering subgroup of G, then $|G : U| \leq g(n)$.*

Clearly Conjecture 4.3 is just a special case of Conjecture 4.1, namely the case where the subgroup of index n is a normal subgroup of A and contains the second subgroup. In fact these two conjectures are equivalent. To see this, suppose that Conjecture 4.3 is true. Let A, U, V be as in Conjecture 4.1. If the A-core $U_A := \bigcap_{a \in A} U^a$ of U is trivial then $|A : V| \leq |A| \leq n!$. Suppose that this not the case, and set $G = U_A$. Then $|A : G| \leq n!$ and $V \cap G$ is an A-covering subgroup of G, whence $|G : V \cap G| \leq g(n!)$. Then $|A : V| \leq |A : V \cap G| \leq n!\, g(n!)$.

The conjecture for prime-power-covering subgroups equivalent to Conjecture 4.3 is also of interest.

CONJECTURE 4.3′. *There is an integer function g such that, if G is a finite group, A is a group of automorphisms of G containing* Inn G *as a subgroup of index n, and U is an A-prime-power-covering subgroup of G, then $|G : U| \leq g(n)$.*

These conjectures remain open. However we can prove Conjecture 4.3 in the case where U is a maximal subgroup of G.

THEOREM 4.4. *Conjecture* 4.3 *is true in the case where U is a maximal subgroup of G.*

The proof of this theorem relies on the finite simple group classification, in that it uses the following result.

THEOREM 4.5. *There is an integer function h such that, if T is a finite non-abelian simple group containing at most n* Aut T*-conjugacy classes of elements, then $|T| \leq h(n)$.*

A proof of Theorem 4.5 expressed in a different form can be found in [28, Lemma 4.4]. Laci Pyber shows that

$$n \geq 2^{\gamma \sqrt{\log h(n)/\log\log h(n)}}$$

for some constant γ. This implies that $h(n)$ can be taken as a function of the form

$$h(n) = 2^{c(\log n)^2 \log\log n}$$

for some constant c. To illustrate the basic ideas we sketch a proof below.

PROOF OF THEOREM 4.5. The proof of Theorem 4.5 is a matter of checking cases. Since there are only a finite number of sporadic simple groups these need not be

considered. The alternating group A_c contains involutions which are products of $2, 4, \ldots$ cycles of length 2, and so, at least when $c > 6$, the number of S_c-conjugacy classes of involutions contained in A_c is at least $(c-3)/4$ so $|A_c| = c!/2 \leq (4n+3)!$.

For the classical simple groups T the number of Aut T-classes of unipotent elements increases with the rank of the group and hence the rank is bounded above by a function of n. This leaves several families of simple groups of Lie type with bounded Lie rank d over a finite field GF(q). Each of these groups contains a maximal torus H which is self-centralising and such that $|N_{\mathrm{Aut}\,T}(H) : H|$ is at most $kd \log q$ for some (small) constant k. Moreover all cyclic subgroups of G of order $|H|$ are conjugate to H, see [7]. Now H contains $\varphi(|H|) \geq |H|/\log|H|$ generators (where $\varphi(|H|)$ is the number of positive integers less than $|H|$ and relatively prime to $|H|$) and in all cases $|H| > q/2$, whence H contains at least $q/k' \log q$ generators for some constant k'. It follows that the number of Aut T-classes which contain generators of H is at least $q/kk'd \log^2 q$, and hence q is bounded by some function of n. Hence $|T|$ is bounded by some function of n.

We show in the proof of Theorem 4.4 that the function $g(n)$ may be chosen as $h(n)^{(6n)^{1/3}}$. Using the function $h(n)$ obtained by Pyber, given above, this gives a function $g(n)$ of the form

$$g(n) = 2^{c' n^{1/3} (\log n)^2 \log\log n}$$

for some constant c'. It was Laci Pyber who pointed out how to improve the original proof to give a sub-exponential bound here.

PROOF OF THEOREM 4.4. Let G be a finite group, A a group of automorphisms of G containing Inn G as a subgroup of index n, and U a maximal subgroup of G which is an A-covering subgroup of G. We must find an upper bound on $|G : U|$ in terms of n. Consider the permutation action induced by G on the set Ω of all A-conjugates of U. Let $\Omega_1, \ldots, \Omega_{n'}$ be the G-orbits in Ω, where U is the stabilizer of a point of Ω_1. Then A permutes these orbits transitively, and consequently they are of equal length $|\Omega_i| = |G : N_G(U)|$ and their number n' is a divisor of $n = |A : \mathrm{Inn}\, G|$. Let K be the kernel of this action of G. Suppose first that $G = UK$. Then U is normal in G and U fixes Ω_1 pointwise, so there are at most $n' \leq n$ distinct images of U under elements of A and all of them contain the identity element. Thus $|G| = |\bigcup_{a \in A} U^a| < n|U|$ whence $|G : U| < n$.

Suppose now that $G \neq UK$. Then since U is a maximal subgroup of G, $K \subseteq U$ and hence $|G^\Omega : U^\Omega| = |G : U|$, where G^Ω, U^Ω denote the permutation groups induced on Ω by G, U respectively. Thus we may assume that the action on Ω is faithful, that is, that $K = \{1\}$. Since A permutes the G-orbits regularly, it follows that all the groups G^{Ω_i} are conjugate by elements of A. Since U is maximal in G, G induces a primitive group G^{Ω_1} on Ω_1, and hence G induces a primitive group G^{Ω_i} on

Ω_i for each i. It follows from these remarks together with the O'Nan-Scott Theorem (see [22]) that the socles of the G^{Ω_i}, and also the socle S of G is a direct power of the same finite simple group T say. Also, since each G^{Ω_i} is primitive, S^{Ω_i} is transitive.

Suppose first that G^{Ω_1} has an elementary abelian normal p-subgroup for some prime p, so that $T = Z_p$. Then $(U \cap S)^A = S$. Also, as the socle S acts regularly on each Ω_i, the intersection $U \cap S$ is the kernel of the action of S on Ω_1, and in particular is normal in G. Thus there are at most $n' \leq n$ distinct images of $U \cap S$ under elements of A, and so $|S| = |(U \cap S)^A| < n|U \cap S| = n|S|/|G : U|$, whence $|G : U| < n$.

Thus we may assume that T is a non-abelian simple group. Then, by [27, Proposition 3.1], $S = N_1 \times \ldots \times N_s$ is the direct product of $s \geq 5$ minimal normal subgroups N_i of G, and for some distinct i, j, the intersection $U \cap S$ has the form $D \times (\prod_{l \neq i,j} N_l)$ where D is a diagonal subgroup of $N_i \times N_j$. Now $N_i \cong T^k$ for some $k \geq 1$ independent of i, and so $|G : U| = |S : U \cap S| = |T|^k$. Thus we must bound $|T|^k$ by a function of n.

Appealing again to [27, Proposition 3.1], we have $n \geq st/2$, where t is the number of Aut N_1-conjugacy classes of elements of N_1, and since $s \geq 5$ this means that $t < n$. Clearly the number of Aut N_1-conjugacy classes of elements of N_1 with at most one non-identity entry is equal to the number of Aut T-conjugacy classes of elements of T. Thus the number c of Aut T-conjugacy classes of elements of T is at most t, which in turn is less than n. It then follows from Theorem 4.5 that $|T| \leq h(n)$.

Let $\mathscr{C}_1, \ldots, \mathscr{C}_c$ be the Aut T-classes of elements of T. Then each element x of N_1 determines an ordered c-tuple $a(x) := (a_1, \ldots, a_c)$ of non-negative integers with sum $\sum_{1 \leq i \leq c} a_i = k$, such that a_i of the entries of x lie in $\mathscr{C}_i$ for each i. Clearly, if $x, y \in N_1$ are in the same Aut N_1-class, then $a(x) = a(y)$. Hence the number of Aut N_1-classes of elements of N_1 is at least the number of ordered c-tuples of non-negative integers with sum k, namely $\binom{k+c-1}{c-1}$. Since $c \geq 4$, we have $\binom{k+c-1}{c-1} > k^3/6$, and hence $k^3/6 < t \leq n$. Thus we have $|G : U| = |T|^k < h(n)^{(6n)^{1/3}}$.

Although Conjecture 4.3 remains open in general, the basic ideas of the proof of Theorem 4.4 can be used to show that the index of an A-covering subgroup U of G is bounded by some function $g(n, c)$ of both $n = |A : \text{Inn } G|$ and the length c of an A-chief series of G/U_A. (Recall that an *A-chief series* of G is a maximal chain of A-invariant subgroups, each a proper subgroup of the next.) The proof will show that we can take g to be any function such that

$$g(n, 1) = h(n)^n,$$

where h is as in Theorem 4.5, and, for $c > 1$,

$$g(n, c) = h(n)^n g(nh(n)^n, c - 1).$$

This result demonstrates that the basic problem in verifying Conjecture 4.3 is proving that the length of an A-chief series is bounded by a function of n.

THEOREM 4.6. *There is a function $g(n, c)$ such that, if G is a finite group, A is a group of automorphisms of G containing* Inn G *as a subgroup of index n, and U is an A-covering subgroup of G such that an A-chief series of G/U_A has length c, then $|G : U| \leq g(n, c)$.*

PROOF. Let A, G, U be as in the statement. We may assume that $U_A = \bigcap_{a \in A} U^a = \{1\}$, so that an A-chief series of G has length c. The proof is by induction on c. Suppose first that $c = 1$. Then $G \cong T^k$ for some simple group T and positive integer k, and there is no proper nontrivial A-invariant subgroup of G. If $T = Z_p$ for some prime p, then U is a normal subgroup of G and hence there are at most n distinct conjugates of U by elements of A. Since $G = U^A$, $|G| < n|U|$ and $|G : U| < n \leq h(n)^n$. So suppose that T is a non-abelian simple group. Then the simple direct factors of G are uniquely determined by G, and by Theorem 1.6, U is a product $D_1 \times \ldots \times D_l$, where each $D_i \cong T$ and D_i is a diagonal subgroup of T^{k_i} with $\sum_{1 \leq i \leq l} k_i = k$. (The proof of Theorem 1.6 shows that U projects onto each simple direct factor of G.) Since $U_A = \{1\}$, we have in particular that $U \neq G$. Thus at least one of the k_i is greater than 1. This means that each element of U has at least two entries from the same Aut T-conjugacy class. In particular, since $G = U^A$, the number of Aut T-conjugacy classes in T is at most k (else we would have an element of G with all entries from different Aut T-conjugacy classes in T and no A-conjugate of this element would lie in U). Also since G has no proper nontrivial A-invariant subgroups, $k \leq n$. Then by Theorem 4.5, $|T| \leq h(n)$, and hence $|G : U| < |G| \leq h(n)^n$. Thus the result holds if $c = 1$ with $g(n, 1) = h(n)^n$.

Now suppose that $c > 1$ and that the result holds when the length of an A-chief series of G is less than c. Let L be an A-invariant subgroup of G such that $\bar{G} := G/L$ has no proper nontrivial A-invariant subgroups and the length of an A-chief series for L is $c - 1$. Then $\bar{U} := UL/L$ contains at least one element from each $\bar{A}$-class of elements of $\bar{G}$, where $\bar{A}$ is the group of automorphisms of $\bar{G}$ induced by A . Also $U \cap L$ contains at least one element from each A_L-class of elements of L, where A_L is the group of automorphisms of L induced by A. Let $m := |A_L : \text{Inn } L|$. Then by induction on c, $|L : U \cap L| = |UL/L| \leq g(m, c - 1)$. Consider the results of the previous paragraph.

If $\bar{G} \cong Z_p^k$ for some prime p and positive integer k, we showed that $p \leq |\bar{G} : \bar{U}| < n$, and as $\bar{A}$ acts irreducibly on $\bar{G}$ we must have $k \leq n - 1$. Thus in this case $|\bar{G}| = |G : L| < n^{n-1}$ so that $m \leq |A : \text{Inn } G|.|G : L| < n^n$ and

$$|G : U| = |G : UL|.|UL : U| = |\bar{G} : \bar{U}|.|L : U \cap L| < n.g(n^n, c - 1).$$

Since $n \leq h(n)$, this is less than $h(n)^n g(nh(n)^n, c - 1)$.

Now suppose that $\bar{G} \cong T^k$ for some non-abelian simple group T and positive integer k. We showed that $k \leq n$ and $|T| \leq h(n)$ and hence that $|\bar{G} : \bar{U}| < |\bar{G}| \leq$

https://doi.org/10.1017/S1446788700036028 Published online by Cambridge University Press

$h(n)^n$. It follows that $m \leq nh(n)^n$ and hence $|G : U| = |G : UL|.|UL : U| \leq h(n)^n g(nh(n)^n, c-1)$. Theorem 4.6 now follows by induction on c.

We note that the recursive definition of $g(n, c)$ given before the statement of Theorem 4.6 can be "unpacked". Set $k(n) := h(n)^n$, $l(n) := n.h(n)^n$, and let $k \circ l$ denote the composition of the functions k and l, and for $i \geq 0$ let $l^{(i)}$ denote the composition of l with itself i times, where $l^{(0)}$ denotes the identity function $l^{(0)}(n) = n$. Then it is straightforward to show that, for $c \geq 1$,

$$g(n, c) = \prod_{i=0}^{c-1} k \circ l^{(i)}(n).$$

Exploring the techniques used in proving Proposition 3.1 of [27] (the crucial result used in the proof of Theorem 4.4) a proof of Conjecture 4.3′ in the case where U is a maximal subgroup of G can be constructed provided that the following strengthening of Theorem 4.5 is true.

There is an integer function h such that, if T is a finite non-abelian simple group, and for each prime p there are at most n Aut T*-conjugacy classes of p-elements in T, then $|T| \leq h(n)$.*

This assertion is probably true, and it is currently being investigated by Laci Babai and the author. Moreover a proof of this assertion would lead to a result analogous to Theorem 4.6 for A-prime-power-covering subgroups.

5. Bounds on the depth of a Kronecker class

Jehne [13] studied the *socle* of a Kronecker class $\mathscr{K}_k(K)$, that is the lattice of subfields of $M(\mathscr{K}) : k$ which lie in $\mathscr{K}_k(K)$. We know from Example 1.12 that $\mathscr{K}_k(K)$ may contain elements which are not subfields of the Galois hull $M(\mathscr{K})$. To what extent does the socle determine $\mathscr{K}_k(K)$? Under what conditions (on $K : k$ or on the Galois groups) can we be certain that all elements of $\mathscr{K}_k(K)$ lie in the socle? These are very difficult and important questions.

Some exploratory investigations of Kronecker classes $\mathscr{K}_k(K)$ for small degree extensions $K : k$ showed that, when $|K : k| \leq 8$, the socle number and width of $\mathscr{K}_k(K)$ are equal and are at most 2 ([27, Theorem 1]). Exploring the existence of elements of $\mathscr{K}_k(K)$ outside of the Galois hull proved to be much more difficult and complete information about the corresponding Galois groups was only obtained in general when $|K : k| \leq 4$ ([27, Theorem 3]) and in the case of Galois extensions $K : k$ of degree at most 8 ([26] for degree 8, and [27, Theorem 3.3] for degrees 5,

6, and 7). This very restricted data indicates that the Galois group of the Galois hull $M(\mathscr{K}) : k$ is not very restricted, but for the existence of some $L \sim_k K$ with $L \not\subseteq M(\mathscr{K})$, there are strong restrictions on the Galois group of the Galois hull of $L : k$.

The only general result shedding light on these questions is the result of Guralnick [9] mentioned previously which, together with the small degree results shows that, when $K : k$ has degree n and the Galois group of $M(\mathscr{K}) : k$ is as large as it can be, namely S_n, or (if $n \neq 3, 5$) A_n, then all elements of $\mathscr{K}_k(K)$ lie in the socle and indeed are conjugate to K (Theorem 4.2 above).

6. Other types of equivalence of algebraic number fields

Several other kinds of equivalence of algebraic number fields, with corresponding group theoretic conditions have been studied. Some are stronger than Kronecker equivalence while others are weaker. Several of these will be mentioned here.

6A. Arithmetical Equivalence Two extensions K and L of an algebraic number field k are said to be *arithmetically equivalent* if they have equal zeta functions: $\zeta_K(s) = \zeta_L(s)$. Gassmann [8] and Perlis [24] showed that arithmetically equivalent fields have the same Galois closure over the rational numbers, and Perlis [24] proved that, if M is a finite Galois extension of k containing K and L, A is the Galois group of $M : k$ and U, V are the fixed groups of K, L respectively, then K and L are arithmetically equivalent if and only if $|x^A \cap U| = |x^A \cap V|$ for every conjugacy class x^A of A. Thus arithmetical equivalence is a stronger condition than Kronecker equivalence. (For an extensive investigation and comparison of these two kinds of equivalence, see the work of N. Klingen, for example [15, 18].) Moreover the arithmetical equivalence of K and L has a strong conection with the permutation characters for the permutation representations of A (by right multiplication) on the sets of right cosets of U and V. Observe that, for $a, x \in A$,

$$Uax = Ua \quad \text{if and only if} \quad axa^{-1} \in U \quad \text{if and only if} \quad x \in U^a.$$

For a fixed element $x \in A$, the number of elements $a \in A$ such that $axa^{-1} \in U$ on the one hand is equal to $|C_A(x)|.|x^A \cap U|$, and on the other hand is equal to $|U|.\pi_U(x)$, where $\pi_U(x)$ is the number of cosets Ua such that $Uax = Ua$, that is, π_U is the permutation character for the representation of A on the right cosets of U. Thus two finite extensions K and L *of the same degree* of an algebraic number field k are arithmetically equivalent if and only if, for the corresponding subgroups U and V, the permutation characters π_U, π_V are equal.

Examples of groups A with nonconjugate subgroups U, V giving the same permutation characters π_U, π_V have been known for a long time, and in 1979, H. Wielandt

asked if it was possible to have $\pi_U = \pi_V$ for U a maximal subgroup of A and V a non-maximal subgroup, see [19, 6.6]. In 1989, A. Borovik [2] produced two different nonconjugate embeddings of the alternating group A_6 in $E_8(\mathbb{C})$, which, while not answering Wielandt's question (for $E_8(\mathbb{C})$ is an infinite group), inspired Guralnick and Saxl [11] to construct examples which gave an affirmative answer. Guralnick and Saxl constructed several infinite families of simple groups A, each with two subgroups U, V, one maximal in A and one not maximal, with equal permutation characters π_U, π_V. Thus there are infintely many finite Galois extensions $M : k$ of algebraic number fields having intermediate fields K, L, of the same degree over k, which are arithmetically equivalent, and are such that $K : k$ is a minimal extension and $L : k$ is not.

R. Odoni asked if it might be the case that, for Galois extensions $M : k$ with Galois group a p-group, for some prime p, Kronecker equivalence of intermediate extensions $K : k$ and $L : k$ implies arithmetical equivalence. Examples to show that this is not true can be found in [27, Theorem 2(e)(iii) or (iv)]. The first of these examples corresponds to the wreath product $A = Z_2$ wr Z_4 and two elementary abelian subgroups U, V of order 8 in the base group of A. A. Caranti, N. Gavioli and S. Mattarei [5] have produced examples similar to this one for all primes p.

6B. Norm Groups The *norm group* $N_{K:k}(K^*)$ of a finite extension $K : k$ of fields is the group of nonzero norms from K to k. Here K^* is the multiplicative group of K. Let $K : k$, $L : k$ be two finite extensions of an algebraic number field k, let M be a finite Galois extension of k containing K and L, let A be the Galois group of $M : k$ and let U, V be the fixed groups of K, L respectively. L. Stern [30, Theorem 1.8] showed that if $N_{K:k}(K^*) = N_{L:k}(L^*)$ then U and V have non-empty intersection with the same sets of A-conjugacy classes of elements of prime power order. So the group theoretical translation of Kronecker equivalence is stronger than this necessary group theoretic condition for equality of norm groups. However equality of the norm groups depends on the arithmetic of the fields as well as this condition on the Galois groups.

L. Stern [30] and M. Lochter [23] have studied several kinds of equivalence of algebraic number fields which are weaker than Kronecker equivalence. In particular one of these, weak Kronecker equivalence, may be formulated in terms of norm groups. The two number fields K and L above are *weakly Kronecker equivalent* if and only if the indices

$$|N_{K:k}(K^*) : N_{K:k}(K^*) \cap N_{L:k}(L^*)| \quad \text{and} \quad |N_{L:k}(L^*) : N_{K:k}(K^*) \cap N_{L:k}(L^*)|$$

are both finite, that is, if and only if the norm groups $N_{K:k}(K^*)$ and $N_{L:k}(L^*)$ are *almost equal*. This in turn is equivalent to the corresponding subgroups U and V meeting exactly the same sets of A-conjugacy classes of elements of prime power order (proved by Stern [30, Theorem 1.8], and later, but independently, by Lochter [23, Satz 4.2]).

A finite extension $K : k$ is said to be *k-solitary* if, for any finite extension L of k, $N_{K:k}(K^*) = N_{L:k}(L^*)$ implies that K and L are conjugate over k. Guralnick and Stern [12] proved that, if a finite Galois extension $K : k$ of algebraic number fields is k-solitary, then $K : k$ is of degree a power of 2 [12, Theorem 2.7]. Further, they showed that all extensions $K : k$ of degree 1 or 2 are k-solitary, and they classified all k-solitary Galois extensions of degree at most 8.

Acknowledgements

Karl Gruenberg suggested in 1988 that I write a paper of this nature, and on several occasions Laci Pyber requested details of the results in Section 4. But for these two the paper may never have been written. A first draft of the manuscript was prepared while I was a Visiting Fellow at the Australian National University. It was Peter Neumann who first brought to my attention some of the group theoretic problems associated with Kronecker equivalence, and I am grateful to him for many discussions about the conjectures in Section 4. I also thank Wolfram Jehne and Norbert Klingen for their generous encouragement of a group theorist's contribution to the area. Finally the paper has benefited enormously from careful readings of the first draft by Bob Guralnick, Wolfram Jehne, Laci Kovács, Peter Neumann, Laci Pyber, Jan Saxl and Leonid Stern.

References

[1] M. Bauer, 'Zur Theorie der algebraischen Zahlkörper', *Math. Ann.* **77** (1916), 353–356.
[2] A. Borovik, 'The structure of finite subgroups of simple algebraic groups', *Algebra and Logic* (3) **28** (1989), 249–279 (in Russian).
[3] R. Brandl, *Eine Überdeckungseigenschaft endlicher Gruppen* (Diplomarbeit, Würzburg, 1976).
[4] ———, 'A covering property of finite groups', *Bull. Austral. Math. Soc.* **23** (1981), 227–235.
[5] A. Caranti, N. Gavioli and S. Mattarei, 'Subgroups of finite p-groups inducing the same permutation character', *Comm. in Algebra*, to appear.
[6] B. Fein, W. M. Kantor and M. Schacher, 'Relative Brauer groups, II', *J. reine angew. Math.* **328** (1981), 39–57.
[7] W. Feit and G. M. Seitz, 'On finite rational groups and related topics', *Illinois J. Math.* **33** (1988), 103–131.
[8] F. Gassmann, 'Bemerkungen zur vorstehenden Arbeit von Hurwitz', *Math. Z.* **25** (1926), 665–675.
[9] R. M. Guralnick, 'Zeros of permutation characters with applications to prime splitting and Brauer groups', *J. Algebra* **131** (1990), 294–302.
[10] R. M. Guralnick, M. W. Liebeck and C. E. Praeger, 'Covering subgroups and arithmetic properties of number fields', in preparation.
[11] R. M. Guralnick and J. Saxl, 'Primitive permutation characters', in: *Groups, combinatorics and geometry* (eds. M. W. Liebeck and J. Saxl), London Math. Soc. Lecture Notes Ser. 165 (Cambridge Univ. Press, Cambridge, 1992) pp. 364–367.
[12] R. M. Guralnick and L. Stern, 'Solitary Galois extensions of algebraic number fields', *J. Number Theory*, to appear.

[13] W. Jehne, 'Kronecker classes of algebraic number fields', *J. Number Theory* **9** (1977), 279–320.
[14] ———, 'On Kronecker classes of atomic extensions', *Proc. London Math. Soc.* (3) **34** (1977), 32–64.
[15] N. Klingen, 'Zahlkörper mit gleicher Primzerlegung', *J. reine angew. Math.* **299** (1978), 342–384.
[16] ———, 'Atomare Kronecker-Klassen mit speziellen Galoisgruppen', *Abh. Math. Sem. Univ. Hamburg.* **48** (1979), 42–53.
[17] ———, 'Ueber schwache quadratische Zerlegungsgesetze', *Comment. Math. Helv.* **55** (1980), 645–651.
[18] ———, 'Rigidity of decomposition laws and number fields', *J. Austral. Math. Soc. (Series A)* **51** (1991), 171–186.
[19] 'The Kourovka Notebook', (Mathematics Institute of the Siberian Division of the Academy of Sciences of the USSR, Novosibirsk, 1990).
[20] L. Kronecker, 'Über die Irreductibilität von Gleichungen', *Werke, II*, 85-93, *Monatsber. Deut. Akad. Wiss.* (1880), 155–163.
[21] S. Lang, *Algebraic Number Theory* (Springer-Verlag, New York, 1986).
[22] M. W. Liebeck, C. E. Praeger and J. Saxl, 'On the O'Nan-Scott Theorem for finite primitive permutation groups', *J. Austral. Math. Soc. (Series A)* **44** (1988), 389–396.
[23] M. Lochter, *Neue zahlentheoretische Aspekte der Kronecker-Äquivalenz* (Doctoral thesis, University of Köln, Köln, 1992).
[24] R. Perlis, 'On the equation $\zeta_K(s) = \zeta_{K'}(s)$', *J. Number Theory* **9** (1977), 342–360.
[25] C. E. Praeger, 'Covering subgroups of groups and Kronecker classes of fields', *J. Algebra* **118** (1988), 455–463.
[26] ———, 'On octic extensions and a problem in group theory', in: *Group Theory, Proceedings of the 1987 Singapore Group Theory Conference* (eds. K. N. Cheng and Y. K. Leong) (De Gruyter, Berlin, 1989) pp. 443–463.
[27] ———, 'Kronecker classes of field extensions of small degree', *J. Austral. Math. Soc. (Series A)* **50** (1991), 297–315.
[28] L. Pyber, 'Finite groups have many conjugacy classes', *J. London Math. Soc.* (2) **46** (1992), 239–249.
[29] J. Saxl, 'On a question of W. Jehne concerning covering subgroups of groups and Kronecker classes of fields', *J. London Math. Soc.* (2) **38** (1988), 243–249.
[30] L. Stern, 'On the equality of norm groups of global fields', *J. Number Theory* **36** (1990), 108–126.

University of Western Australia
Nedlands, WA 6009
Australia