TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 331, Number 2, June 1992

GALOIS GROUPS AND THE MULTIPLICATIVE STRUCTURE OF FIELD EXTENSIONS

ROBERT GURALNICK AND ROGER WIEGAND

ABSTRACT. Let K/k be a finite Galois field extension, and assume k is not an algebraic extension of a finite field. Let K^* be the multiplicative group of K, and let $\Theta(K/k)$ be the product of the multiplicative groups of the proper intermediate fields. The condition that the quotient group $\Gamma = K^*/\Theta(K/k)$ be torsion is shown to depend only on the Galois group G. For algebraic number fields and function fields, we give a complete classification of those G for which Γ is nontrivial.

Let K/E be a proper extension of infinite fields. Brandis [B] proved in 1965 that K^*/E^*, the quotient of the multiplicative groups, is never finitely generated; and in 1984 Davis and Maroscia [DM] showed that the quotient group always has infinite torsion-free rank except in the following two situations where K^*/E^* is obviously torsion: (a) K is an algebraic extension of a finite field, or (b) K is purely inseparable over E. Suppose, now, that K/k is a finite algebraic extension and $E_1, \ldots, E_t$ are proper intermediate fields. For $t = 2$ it was shown in [W] that $K^*/E_1^*E_2^*$ always has infinite rank unless (a) or (b) holds for one of the E_i. The fact that this result did not appear to generalize to more than two intermediate fields was the starting point for this paper.

Assuming now that K/k is a finite Galois extension and that k is not an algebraic extension of a finite field, we examine in detail the structure of the groups $K^*/E_1^* \cdots E_t^*$. We determine in (1.4) exactly when this quotient group is torsion; and we show that if k is a "reasonable" field, e.g., an algebraic number field or a function field, then $K^*/E_1^* \cdots E_t^*$ either is torsion or has a free summand of infinite rank. (See (1.5) and (1.8).) The main results in this paper concern the quotient $K^*/\Theta(K/k)$, where $\Theta(K/k)$ is the compositum of the multiplicative groups of *all* proper intermediate fields. We will see, for example, that $K^* = \Theta(K/k)$ whenever the Galois group contains S_4. We also construct examples, one in characteristic 0 and one in characteristic 2, where the Galois group is $C(2) \times C(2)$ and $K^* = \Theta(K/k)$. Thus it *is* possible for K^* to be the product of the multiplicative groups of *three* intermediate fields.

We show in §2 that $K^*/\Theta(K/k)$ is torsion if and only if the Galois group of K/k is not a Frobenius complement. In §3 we show that if the group

Received by the editors April 17, 1989 and, in revised form, February 6, 1990.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 12F10, 20C15, 20C20; Secondary 20D05, 20G40.

Key words and phrases. Multiplicative group of a field, Galois group, representation, character, finite simple group.

Both authors were partially supported by grants from the National Science Foundation.

0002-9947/92 $1.00 + $.25 per page

$K^*/\Theta(K/k)$ is a nontrivial torsion group, then it is bounded, with prime power exponent p or p^2. Moreover, the prime p depends only on the Galois group. Section 4 addresses the delicate question of when $K^* = \Theta(K/k)$. (This can never happen when k is an algebraic extension of a finite field. See (1.12).) In the final section, §5, we relax the requirement that K/k be a finite Galois extension. We show that if E_1 and E_2 are subfields of K with K algebraic over $E_1 \cap E_2$, then $K^*/E_1^*E_2^*$ has infinite rank unless K is either algebraic over a finite field or purely inseparable over one of the E_i. On the other hand, *every* field K of infinite transcendence degree over its prime subfield satisfies $K^* = E_1^*E_2^*$ for suitable proper subfields E_i.

Some of the topics of this paper were discussed by Wiegand, William Haboush and other participants of the Mountain West Geometry Workshop held in Lincoln, Nebraska, in September, 1988. Subsequently, Wiegand and Haboush obtained some results in a series of letters. Haboush has since discovered some interesting connections with Galois cohomology, [H].

The authors are grateful to the referee, whose careful reading of the original version of this paper led to several improvements.

1. The ideal $\mathbf{I}(G)$

Let G be a finite group, and let $\mathbb{Z}G$ denote the integral group ring. Given a subgroup H of G, let $\sum H$ be the sum, in $\mathbb{Z}G$, of the members of H. If $\mathscr{H}$ is a set of subgroups of G, let $L(\mathscr{H})$ be the left ideal of $\mathbb{Z}G$ generated by $\{\sum H | H \in \mathscr{H}\}$. Finally, put $\mathbf{I}(G) = L(\mathscr{S})$, where $\mathscr{S}$ is the set of all nontrivial subgroups. Since $H_1 \leq H_2 \Rightarrow L(\{H_1\}) \supseteq L(\{H_2\})$, it follows that we could just as well take $\mathscr{S}$ to be the set of subgroups of prime order. Note that $\mathbf{I}(G)$ is a two-sided ideal of $\mathbb{Z}G$, since $(\sum H)g = g(\sum (g^{-1}Hg))$.

We will be primarily interested in the ideal $\mathbf{I}(G) \cap \mathbb{Z}$ of $\mathbb{Z}$; and we will make repeated use of the following easy observation: If G_1 is a subgroup of G_2, then $\mathbf{I}(G_1)$ is contained in $\mathbf{I}(G_2)$. Thus, for example, if it is known that $1 \in \mathbf{I}(H)$ for a certain group H, it follows that $1 \in \mathbf{I}(G)$ for every group G containing an isomorphic copy of H.

Now let K/k be a finite Galois extension with Galois group G. Let G act on the right, so that K^* is a right $\mathbb{Z}G$-module. If $\alpha \in K^*$ and $r \in \mathbb{Z}G$, we write α^r instead of αr. (Thus α^r has its usual meaning if $r \in \mathbb{Z}$.) For any set $\mathscr{H}$ of subgroups of G, let $\Theta(\mathscr{H})$ be the product (compositum) of the multiplicative groups of the fixed fields of the groups in $\mathscr{H}$, and let $\Theta(K/k) = \Theta(\mathscr{S})$, where $\mathscr{S}$ consists of all nontrivial subgroups. Thus $\Theta(K/k)$ is the product of the multiplicative groups of the maximal intermediate fields.

If $\alpha \in K^*$ and $r \in L(\mathscr{H})$ for some set $\mathscr{H}$ of subgroups, we see that $\alpha^r \in \Theta(\mathscr{H})$; more succinctly: $(K^*)^{L(\mathscr{H})} \leq \Theta(\mathscr{H})$. On the other hand, if $\beta \in E^*$, where E is the fixed field of some $H \in \mathscr{H}$, we have $\beta^{|H|} = \beta^{\sum H} \in (K^*)^{L(\mathscr{H})}$. We summarize these observations.

1.1. **Proposition.** *Let $\mathscr{H}$ be a set of subgroups of G. Then $(K^*)^{L(\mathscr{H})} \leq \Theta(\mathscr{H})$, and the quotient $\Theta(\mathscr{H})/(K^*)^{L(\mathscr{H})}$ is a bounded group with exponent dividing the least common multiple of the orders of the groups in $\mathscr{H}$. In particular, $\Theta(K/k)/(K^*)^{\mathbf{I}(G)}$ is bounded with exponent dividing the largest square-free factor of $|G|$.*

We remark that $\Theta(K/k)/(K^*)^{\mathbf{I}(G)}$ can be nontrivial. See (1.11).

1.2. **Example.** Let $k = \mathbb{Q}$ (the rationals) and let K be the splitting field of $x^4 - 4$. Then $G = C(2) \times C(2)$, and it is easy to check that $\mathbb{Z}G/\mathbf{I}(G)$ has order 2. (If σ and τ are generators of G, we have $2 = (1 + \sigma) - \sigma(1 + \tau) + (1 + \sigma\tau) \in \mathbf{I}(G)$.) Therefore $\alpha^2 \in \Theta(K/k)$ for all $\alpha \in K^*$. Using the fact that the K/k-norm of everything in $\Theta(K/k)$ is a square, one can show directly that $K^*/\Theta(K/k)$ is infinite. Thus $K^*/\Theta(K/k)$ is an infinite elementary abelian 2-group. (If G is any noncyclic elementary abelian 2-group, it follows that $2 \in \mathbf{I}(G)$. Therefore $\mathbf{I}(G)$ is the kernel of the augmentation map modulo 2; hence $\mathbb{Z}G/\mathbf{I}(G)$ has order 2.)

1.3. **Example.** Let $k = \mathbb{Q}$ and let K be the splitting field of $x^3 - 2$. Then $G = S_3$, and $\mathbb{Z}G/\mathbf{I}(G)$ has order 3; therefore $K^*/\Theta(K/k)$ is an elementary abelian 3-group. This time there seems to be no direct way of showing even that $K^* \neq \Theta(K/k)$. It follows from (1.5) below, however, that $K^*/\Theta(K/k)$ is infinite.

It follows from (1.1) and the proofs of (1.2) and (1.3) that $\Theta(K/k)$ is equal to K^* if the Galois group contains S_4 or A_5. We will show in §4 that $\Theta(K/k) = K^*$ whenever the Galois group contains a nonabelian simple group. On the other hand, if K/k has Galois group $\mathrm{SL}_2(5)$, then $K^*/\Theta(K/k)$ always has elements of infinite order, even though $\mathrm{SL}_2(5)$ is not solvable. (See §2.)

1.4. **Proposition.** *Assume k is not an algebraic extension of a finite field, and let $\mathscr{H}$ be any set of subgroups of G. These conditions are equivalent:*

(a) $K^*/\Theta(\mathscr{H})$ *is a bounded group.*
(b) $K^*/\Theta(\mathscr{H})$ *is a torsion group.*
(c) $K^*/\Theta(\mathscr{H})$ *has finite torsion-free rank.*
(d) $L(\mathscr{H}) \cap \mathbb{Z} \neq 0$.

Proof. (a) $\Rightarrow$ (b) $\Rightarrow$ (c) trivially, and (d) $\Rightarrow$ (a) by (1.1). Suppose (c) holds, and let r be the rank of $K^*/\Theta(\mathscr{H})$. There are infinitely many rank-one (but not necessarily discrete) valuations v_i of k that split completely in K. (See [NNT], in particular, the footnote on the first page.) For each positive integer i, let V_i be one of the valuations of K lying over v_i. Define $V_i^g(\alpha^g) = V_i(\alpha)$ for $g \in G$ and $\alpha \in K^*$. Then the V_i^g, $g \in G$, are exactly the valuations of K lying over v_i. Let $\mathbb{R}$ be the reals and define $\Phi_i\colon K^* \to \mathbb{R}G$ by

$$\Phi_i(\alpha) = \sum_{g \in G} (V_i^g(\alpha))g. \tag{1.4.1}$$

It is easily checked that Φ_i is a $\mathbb{Z}G$-module homomorphism. Moreover, we claim that Φ_i carries $\Theta(\mathscr{H})$ into $\mathbb{R}L(\mathscr{H})$. To prove this, it is enough to show that if $H \in \mathscr{H}$ and E is the fixed field of H, then $\Phi_i(\alpha) \in \mathbb{R}L(\mathscr{H})$ for every $\alpha \in E^*$. Let T be a complete set of left coset representative for H in G. For $g \in T$ and $h \in H$ we have $V_i^{gh}(\alpha) = V^g(\alpha^{h^{-1}}) = V^g(\alpha)$. Therefore $\Phi_i(\alpha) = \sum_{g \in T} \sum_{h \in H} (V_i^{gh}(\alpha))gh = (\sum_{g \in T} (V_i^g(\alpha))g)(\sum H) \in \mathbb{R}L(\mathscr{H})$.

Now choose, by the approximation theorem, $\alpha_1, \ldots, \alpha_{r+1}$ such that $t_i := V_i(\alpha_i) > 0$, but $V_i^g(\alpha_j) = 0$ if $i \neq j$ or $g \neq 1$. If $K^*/\Theta(\mathscr{H})$ has rank r, there are integers n_i, with, say, $n_1 > 0$, such that $\beta := \alpha_1^{n_1} \cdots \alpha_{r+1}^{n_{r+1}} \in \Theta(\mathscr{H})$. Then

$\mathbb{R}L(\mathscr{H})$ contains $\Phi_1(\beta) = n_1 t_1$, a positive real number. Therefore $\mathbb{R}L(\mathscr{H}) = \mathbb{R}G$, and it follows that $\mathbb{Q}L(\mathscr{H}) = \mathbb{Q}G$, that is, $L(\mathscr{H}) \cap \mathbb{Z} \neq 0$. =

Actually, one can work with the rational group ring $\mathbb{Q}G$ from the start, rather than with $\mathbb{R}G$. The reason is that the valuations v_i can be chosen to have subgroups of the additive group of rationals as their value groups. (See [Ji].)

In order to get more precise information about $K^*/\Theta(\mathscr{H})$, we need some discrete valuations. If k is an algebraic number field or a function field (see (1.8) below), there are always infinitely many inequivalent discrete rank-one valuations that split completely in K. Recall that a set $\mathscr{V}$ of valuations of K has *finite character* if for every $\alpha \in K^*$ there are only finitely many $v \in \mathscr{V}$ for which $v(\alpha) \neq 0$. For $0 \leq r \leq \omega$, let $A^{(r)}$ denote the direct sum of r copies of A.

1.5. **Theorem.** *Assume k has infinitely many pairwise inequivalent discrete rank-one valuations v_i, $1 \leq i < \infty$, that split completely in K. Let $\mathscr{H}$ be a set of subgroups of G, and let $L(\mathscr{H}) \cap \mathbb{Z} = (n)$, $n \geq 0$.*

(a) *If $n = 1$ then $\Theta(\mathscr{H}) = K^*$.*

(b) *For each finite r, $K^*/\Theta(\mathscr{H})$ has a direct summand isomorphic to $(\mathbb{Z}/(n))^{(r)}$.*

(c) *If $n = p$, a prime, then $K^*/\Theta(\mathscr{H})$ is an infinite elementary abelian p-group.*

(d) *If $n > 0$ or $\{v_i\}$ has finite character, then $K^*/\Theta(\mathscr{H})$ has a direct summand isomorphic to $(\mathbb{Z}/(n))^{(\omega)}$.*

Proof. (a) follows from (1.1). Choose, for each i, a valuation V_i of K lying over v_i, and define the valuations V_i^g, for $g \in G$, as in the proof of (1.4). We may assume each v_i has value group $\mathbb{Z}$. The same is then true for each V_i^g, since there can be no ramification. Define $\Phi_i : K^* \to \mathbb{Z}G$ by formula (1.4.1). Then, for each $r < \omega$, the map $\Phi : K^* \to (\mathbb{Z}G)^{(r)}$ induced by $\Phi_1, \ldots, \Phi_r$ is surjective, by the approximation theorem. As in the proof of (1.4) we see that Φ_i carries $\Theta(\mathscr{H})$ into $L(\mathscr{H})$. Thus we have a surjection $K^*/\Theta(\mathscr{H}) \to (\mathbb{Z}G/L(\mathscr{H}))^{(r)}$. But $\mathbb{Z}G/L(\mathscr{H})$ is a faithful, finitely generated $\mathbb{Z}/(n)$-module, so it has $\mathbb{Z}/(n)$ as a homomorphic image. Therefore we have a surjection $K^*/\Theta(\mathscr{H}) \to (\mathbb{Z}/(n))^{(r)}$. Since $K^*/\Theta(\mathscr{H})$ is a $\mathbb{Z}/(n)$-module, (b) and (c) follow.

To prove (d) when $n > 0$, we note that $K^*/\Theta(\mathscr{H})$, being a $\mathbb{Z}/(n)$-module, is a direct sum of cyclic groups. By (b), $K^*/\Theta(\mathscr{H})$ has infinitely many elements of order n, and (d) follows. Finally, assume $n = 0$ and $\{v_i\}$ has finite character. Then the whole family $\{V_i^g\}$ has finite character (see [Ji], for example), and the Φ_i define a map $\Psi : K^*/\Theta(\mathscr{H}) \to (\mathbb{Z}G/L(\mathscr{H}))^{(\omega)}$. But each $\mathbb{Z}G/L(\mathscr{H})$ maps onto $\mathbb{Z}$, and when we compose these maps with Ψ we get a map $\Xi : K^*/\Theta(\mathscr{H}) \to \mathbb{Z}^{(\omega)}$. Moreover, the image of Ξ has a nonzero projection on each coordinate of $\mathbb{Z}^{(\omega)}$, so the image of Ξ is isomorphic to $\mathbb{Z}^{(\omega)}$. Then Ξ splits, and the proof is complete.

We now know the precise structure of $K^*/\Theta(K/k)$ for the two examples above: $\mathbb{Q}(i, \sqrt{2})^*/\Theta(K/\mathbb{Q})$ is an infinite elementary abelian 2-group, and if K is the splitting field of $x^3 - 2$ over $\mathbb{Q}$, then $K^*/\Theta(K/\mathbb{Q})$ is an infinite elementary abelian 3-group. The following result puts these examples into a general framework.

1.6. **Proposition.** *Let p and q be primes with $p > q$, and let G be a noncyclic group of order p^2 or pq. Then $\mathbf{I}(G) \cap \mathbb{Z} = (p)$.*

Proof. Suppose $G = C(p) \times C(p) = \langle x \rangle \times \langle y \rangle$. Then, for each i, $0 \leq i < p$, $\mathbf{I}(G)$ contains $h_i := \sum\langle xy^i \rangle = 1 + xy^i + x^2y^{2i} + \cdots + x^{p-1}y^{(p-1)i}$. Then $\sum_{i=0}^{p-1} h_i = p + \sum_{i=1}^{p-1} x^i \sum\langle y \rangle$, and it follows that $p \in \mathbf{I}(G)$. If G is a nonabelian group of order pq, then $G = \langle x, y | x^q = 1, y^p = 1, yx = xy^a \rangle$, where $a^q \equiv 1 \pmod{p}$. Let $h_i = \sum\langle xy^i \rangle$, for $0 \leq i < q$, and proceed almost exactly as above, to deduce that $p \in \mathbf{I}(G)$. All that remains is to show that $\mathbf{I}(G) \neq \mathbb{Z}(G)$. In either case G has a normal subgroup of order p, which we kill, getting a map onto $\mathbb{Z}C(\pi)$, where π is either p or q. Now let ζ be a primitive πth root of unity, and map $\mathbb{Z}C(\pi)$ onto $\mathbb{Z}[\zeta]$ by sending a generator of $C(\pi)$ to ζ. One checks easily that the composition of these two surjections carries $\mathbf{I}(G)$ into $p\mathbb{Z}[\zeta]$, so $\mathbf{I}(G)$ is indeed a proper ideal of $\mathbb{Z}G$.

Although we will prove a much more general result in the next section, we will push the cyclotomic idea a little further here.

1.7. **Corollary.** *Let G be abelian. Then $\mathbf{I}(G) \cap \mathbb{Z} = 0$ if and only if G is cyclic.*

Proof. If G is not cyclic then G contains a noncyclic group of order p^2, and we can apply (1.6). If G is cyclic of order n, let ζ be a primitive nth root of unity, and check that $\mathbf{I}(G)$ dies under the natural map $\mathbb{Z}G \to \mathbb{Z}[\zeta]$.

Now we will exhibit lots of fields to which we can apply the full strength of (1.5). It is well known that for any algebraic number field K there are infinitely many rational primes that split completely. (This is a weak form of the Tchebotarev Density Theorem. See [Ja].) Now let k be an algebraic number field and let K/k be Galois. If $\mathfrak{p}$ is a prime of k lying over a rational prime that splits completely in K, then of course $\mathfrak{p}$ itself must split in K. Therefore there are infinitely many such $\mathfrak{p}$, and the corresponding set of discrete valuations of K has finite character.

Next, let k be a *function field*, that is, a finite extension of $F(X)$, where F is a field and X is an indeterminate. Jia Bao-Ping has shown [Ji] that for any finite separable extension K/k, there is an infinite set of finite character, consisting of inequivalent discrete valuations of k that split completely in K. (If F is infinite and $k/F(X)$ is separable, this follows from [G].) We summarize these results in the following:

1.8. **Proposition.** *Let K/k be a finite Galois extension. Assume k is either an algebraic number field or a function field (as defined above). Then there is an infinite set, of finite character, consisting of inequivalent discrete rank-one valuations of k, each of which splits completely in K. In particular $K^* = \Theta(K/k)$ if and only if $\mathbf{I}(G) \supseteq \mathbb{Z}$.*

If, for some prime p, the field k is closed under extraction of pth roots (e.g., if k is a perfect field of characteristic p), then clearly k has no discrete valuations. The last assertion of (1.8) can also fail, as we will see in (1.10).

Suppose G is an arbitrary subgroup of S_n and p is a prime number. Let E be any field of characteristic p, let $L = E(X_1, \ldots, X_n)$, and let G act on L by permuting the X_i. Let F be the fixed field of G, let k be the purely inseparable closure of F (in an algebraic closure of L) and let $K = kL$. Since

$k \cap L = F$, the Galois group of K/k maps isomorphically onto that of L/F. We record the result of this construction:

1.9. **Proposition.** *Let G be any finite group, and let p be a prime. Then there exist a perfect field k of characteristic p and a Galois extension K/k with Galois group G.*

1.10. **Corollary.** *If $\mathbf{I}(G) \cap \mathbb{Z} = (p^e)$, p prime, there exist a perfect field of characteristic p and a Galois extension K/k with Galois group G such that $K^* = \Theta(K/k)$.*

Proof. Let K/k be as in (1.9). Then K is perfect, and each element of K^* is a (p^e)th power. Now apply (1.1).

The conclusion of (1.10) is still valid under the formally weaker condition that $\mathbf{I}(G) \neq 0$, since, for every finite group G, $\mathbf{I}(G) \cap \mathbb{Z}$ is either (0), (1), or a prime power. (This is the main theorem of §3.)

Even in characteristic 0 there are examples with $\mathbf{I}(G) \neq G$ but with $\Theta(K/k) = K^*$.

1.11. **Example.** For any field F, let $F((t))$ denote the field of Laurent power series over F, that is, the quotient field of $F[[t]]$. Let p be a prime, and let $K = \mathbb{C}((t))$, $k = \mathbb{R}((t^p))$. The Galois group G of K/k is $C(2) \times C(2)$ if $p = 2$ and is the dihedral group of order $2p$ if $p > 2$. By (1.6), $\mathbf{I}(G) \cap \mathbb{Z} = (p)$. Given $f \in K^*$, write $f = t^j g$, where $g = a + bt + ct^2 + \cdots$, and $a \neq 0$. Then g is a pth power (Hensel's lemma), so $g \in \Theta(K/k)$ by (1.1). Of course $t^j \in \Theta(K/k)$, and it follows that $\Theta(K/k) = K^*$.

If E is the fixed field of a subgroup H of the Galois group G of K/k, then $\alpha^r = N_E^K(\alpha)$ for $\alpha \in K$ and $r = \sum H$. Thus $\mathbf{I}(G) = \mathbb{Z}G$ implies that K^* is actually generated by K/E-norms, for the various proper intermediate fields E. The example above shows that this need not hold when $K^* = \Theta(K/k)$, as t is not a product of norms.

It would be interesting to know whether there is a general source of examples like (1.11) in characteristic 0. More precisely, given a group G with $\mathbf{I}(G) \neq 0$, is there a Galois extension K/k in characteristic 0, with $K^* = \Theta(K/k)$?

So far we have avoided finite fields and their algebraic extensions. Since these fields have no nontrivial valuations, our main tool is not applicable. Fortunately there is another way to show that $K^* \neq \Theta(K/k)$.

1.12. **Proposition.** *Let K/k be a finite extension, where k is an algebraic extension of a finite field. If $K \neq k$ then $K^* \neq \Theta(K/k)$.*

Proof. Note that $K = kL$ (the field compositum) for a suitable finite extension $L/GF(p)$. Putting $F = L \cap K$, we see that K/k and L/F have isomorphic lattices of intermediate fields. Let α generate L^*, and let $|L^*| = p^e - 1$. If $e = 2$, clearly $\Theta(K/k) = k^* \neq K^*$. If $e = 6$ there are at most 2 maximal subfields, and we see (by counting if k is finite, and by appealing to [W, 1.3] if k is infinite) that $K^* \neq \Theta(K/k)$. If e is not equal to 2 or 6, we appeal to Zsigmondy's Theorem, [Z] or [F2], in the form stated below, to produce a prime q such that p has order e modulo q.

Suppose, now, that $\alpha = \beta_1 \cdots \beta_t$, where each β_i belongs to a proper intermediate field E_i, and let m_i be the multiplicative order of β_i. Then q divides

the least common multiple of the m_i, so $q|m_i$ for some i. Therefore q divides $|F(\beta_i)^*| := p^d - 1$, so e, the order of p modulo q, divides d. Since K has a unique subfield of order $p^e - 1$, it follows that $F(\beta_i) \supseteq L$, whence $K = k(\beta_i)$. But then $E_i = K$, a contradiction. (When $e = 6$, one can modify this argument slightly by taking $q = 9$, thereby avoiding the reference to [W].)

1.13 **Theorem** (Zsigmondy). *Let p be a prime and e a positive integer. Then there is a prime q such that p has order e modulo q, unless either* (i) *p is a Mersenne prime and $e = 2$, or* (ii) *$p = 2$ and $e = 6$.*

The following theorem summarizes the main results of this section.

1.14. **Theorem.** *Let K/k be a finite Galois extension with Galois group G, and let $\mathbf{I}(G) \cap \mathbb{Z} = (n)$, $n \geq 0$.*

(a) *If $n = 0$, and k is not algebraic over a finite field, then $K^*/\Theta(K/k)$ has elements of infinite order.*

(b) *If $n = 1$, then $K^* = \Theta(K/k)$.*

(c) *If $n \neq 0, 1$ and k is an algebraic number field or a function field, then $K^*/\Theta(K/k)$ is a nonfinitely generated torsion group.*

(d) *If $n \neq 0$, there are examples showing that K^* can equal $\Theta(K/k)$.*

(e) *If $K \neq k$ and k is an algebraic extension of a finite field, then $K^*/\Theta(K, k)$ is a nontrivial torsion group.*

Of course, the proof of (d) depends on the fact, to be proved in §3, that n is either 0 or a prime power.

2. Frobenius complements

As in §1, we suppose K/k is a finite Galois extension. We will always assume that k is not an algebraic extension of a finite field. Then $K^*/\Theta(K/k)$ is a torsion group if and only if $\mathbf{I}(G) \cap \mathbb{Z} \neq 0$. We will show in (2.3) that this holds if and only if G is *not* a Frobenius complement. We refer the reader to Passman's book [P] for a thorough discussion and classification of Frobenius complements, but we will summarize the properties we will need.

Let G be a finite group acting transitively on a set Ω with at least two points. Assume that $G_a \neq 1$ for $a \in \Omega$, but $G_{a,b} = 1$ for $a \neq b$. (Only the identity fixes two points.) Any group isomorphic to a group G_a arising in this way is called a *Frobenius complement.* For our purposes, a different description will be more useful. Recall that an action of a group H on a set S is *semiregular* provided $G_b = 1$ for every $b \in S$. (Thus, in the definition of Frobenius complements, the condition $G_{a,b} = 1$ for $a \neq b$ says that G_a acts semiregularly on $\Omega - \{a\}$.) In the following proposition, most of which is proved in [P], $\overline{\mathbb{Q}}$ denotes the algebraic closure of the field of rational numbers.

2.1. **Proposition.** *Let H be a finite group. The following are equivalent:*

(a) *H is a Frobenius complement.*

(b) *H has a $\overline{\mathbb{Q}}$-representation σ such that for all $h \in H - \{1\}$ the matrix $\sigma(h)$ has no eigenvalue equal to 1.*

(c) *There exist a prime p and a finite, elementary abelian p-group E such that H acts semiregularly on $E - \{0\}$ (via automorphisms of E).*

(d) *For any prime p not dividing $|H|$, there exists such an E.*

Proof. (a) $\Rightarrow$ (b) by Theorem 18.1 of [P], and (d) $\Rightarrow$ (c) trivially. We will

show that (b) $\Rightarrow$ (d) and (c) $\Rightarrow$ (a). Assuming (b) holds, let K be an algebraic number field containing a primitive $|H|$th root of unity as well as all entries of all the matrices $\sigma(h)$, $h \in H$. Then H acts semiregularly on $V - \{0\}$, where V is a vector space over K. Let D be the ring of integers of K, fix a nonzero vector $v \in V$ and let $L = DHv$, a projective D-module of finite rank. For any prime p not dividing $|H|$, let $\mathfrak{p}$ be a prime ideal of D lying over (p), and let $q = p^e = |D/\mathfrak{p}|$. Put $E = L/\mathfrak{p}L$, and let $\overline{\sigma}$ be the induced $GF(q)$-representation of H as automorphisms of E. The eigenvalues of $\overline{\sigma}(h)$ are the images of those of $\sigma(h)$ under the canonical map $\pi : D \to D/\mathfrak{p}$. Since π is a bijection on $|H|$th roots of unity, $\overline{\sigma}(h)$ cannot have 1 as an eigenvalue unless $h = 1$. Therefore H acts semiregularly on $E - \{0\}$.

If (c) holds, let G be the semidirect product of E and H. Let Ω be the set of left cosets of H in G, with the usual G-action. Then H is the stabilizer of the coset H; and H acts semiregularly on $\Omega - \{H\}$, since H acts on $\Omega - \{H\}$ exactly as it does on $E - \{0\}$. Therefore H is a Frobenius complement.

2.2. **Theorem.** *Let G be a finite group. Then $\mathbf{I}(G) \cap \mathbb{Z} = 0$ if and only if G is a Frobenius complement.*

Proof. Let $\mathbf{I} = \mathbf{I}(G)$. If $\mathbf{I} \cap \mathbb{Z} = 0$, then $\overline{\mathbb{Q}}G/\mathbf{I}\overline{\mathbb{Q}}G$ is a nonzero $\overline{\mathbb{Q}}$-algebra, so there is a nontrivial $\overline{\mathbb{Q}}$-algebra homomorphism $\rho : \overline{\mathbb{Q}}G \to M_n(\overline{\mathbb{Q}})$ such that $\sigma(\mathbf{I}) = 0$. If $g \in G$ has order $m > 1$, then $1 + g + \cdots + g^{m-1} \in \mathbf{I}$. Therefore, if $v \in \overline{\mathbb{Q}}^{(n)}$ and $gv = v$, we have $mv = \sigma(1 + g + \cdots + g^{m-1})v = 0$, whence $v = 0$. This shows that G satisfies (2.1, b).

Conversely, suppose G is a Frobenius complement. If $\mathbf{I} \cap \mathbb{Z}$ contains a nonzero integer n, choose any prime $p \nmid n|G|$, and let E be an elementary abelian p-group such that G acts semiregularly on $E - \{0\}$. Suppose $g \in G$ is an element of prime order q. View E as a $\mathbb{Z}G$-module, and note that multiplication by $1 - g$ is an automorphism of E. It follows that $1 + g + \cdots + g^{(q-1)}$ kills E. Since $\mathbf{I}$ is generated by elements of the form $1 + g + \cdots + g^{(q-1)}$, $\mathbf{I}E = 0$. In particular, $nE = 0$, contradiction.

2.3. **Corollary.** *Let K/k be a Galois extension with Galois group G. Then $K^*/\Theta(K/k)$ is a torsion group if and only if either k is an algebraic extension of a finite field or G is not a Frobenius complement.*

The rest of this section is pure group theory and concerns the relationship between Frobenius complements and groups G satisfying the following condition (encountered in (1.6)):

(2.4) If p and q are primes, every subgroup of G of order p^2 or pq is cyclic.

Notice that if L is a group of even order satisfying (2.4), then L has a unique element of order 2 (so in particular $Z(L) \neq \langle 1 \rangle$). For, if x and y are distinct elements of order 2 and xy has order n, then $\langle x, y \rangle$ is a dihedral group of order $2n$, and it has a subgroup violating (2.4).

By [P, 18.1], every Frobenius complement satisfies (2.4). (Of course, this follows also from (2.2) and (1.6).) The converse is false, $SL_2(17)$ being the smallest counterexample. (See [P] or (2.10).) Every *solvable* group satisfying (2.4) is a Frobenius complement, as is pointed out at the end of §18 of [P].

We will give a proof of this fact here, as a special case of our classification of groups satisfying (2.4). Our classification (2.10), which will be needed in §3, is an extension of the classification of Frobenius complements found in [P], and we will use several steps of Passman's argument here.

2.5. **Lemma.** *Let G be a finite p-group in which every subgroup of order p^2 is cyclic. Then either G is cyclic, or else $p = 2$ and G is a generalized quaternion group.*

Proof. This follows easily from [P, 9.4 and 9.5].

2.6. **Lemma.** *Let G_1 and G_2 be groups of relatively prime orders. Then* $\mathbf{I}(G_1 \times G_2) \cap \mathbb{Z} = (\mathbf{I}(G_1) \cap \mathbb{Z}) + (\mathbf{I}(G_2) \cap \mathbb{Z})$.

Proof. Every minimal subgroup of $G_1 \times G_2$ is contained in either $G_1 \times \langle 1 \rangle$ or $\langle 1 \rangle \times G_2$.

Let $\Omega(G)$ be the subgroup of G generated by the elements of prime order. Since the minimal subgroups of G are contained in $\Omega(G)$, and since $\mathbb{Z}G$ is a free $\mathbb{Z}(\Omega(G))$-module, we have

$$\mathbf{I}(G) \cap \mathbb{Z} = \mathbf{I}(\Omega(G)) \cap \mathbb{Z}. \tag{2.7}$$

In particular, a finite group G is a Frobenius complement if and only if $\Omega(G)$ is a Frobenius complement. Also, it is clear that G satisfies (2.4) if and only if $\Omega(G)$ satisfies (2.4). Therefore, in our classification theorem, we may harmlessly assume that $G = \Omega(G)$.

2.8. **Lemma.** *Let G be a finite group satisfying* (2.4)*, and suppose $G = \Omega(G)$. Then $G = N \times C$, where N has no nontrivial normal subgroups of odd prime power order, and C is a cyclic group of square-free order prime to $|N|$. If, further, G has cyclic Sylow 2-subgroups, then G itself is cyclic.*

Proof. Let q be any prime divisor of $|G|$ for which the Sylow q-subgroups of G are cyclic. (All odd primes qualify, by (2.5).) Let Q be a minimal normal q-subgroup of G. Then Q is cyclic, and its unique subgroup $\langle x \rangle$ of order q is also normal in G. By minimality, $Q = \langle x \rangle$. Condition (2.4) implies that x commutes with every element of prime order $p \neq q$. Also, since Q is contained in every Sylow q-subgroup of G, Q is the only subgroup of order q in G. Thus x commutes with every element of prime order, whence $x \in Z(G)$. Let $R \supseteq Q$ be any Sylow q-subgroup of G. Since R is cyclic, any automorphism of R fixing Q has order a power of q; hence $N_G(R)/C_G(R)$ is a q-group, that is, $N_G(R) = C_G(R)$. By Burnside's theorem [As2, 39.1] G has a normal q-complement N; then $G = NR$ and $N \cap R = 1$. But $N \times Q$ contains every element of prime order, whence $N \times Q = G$. All hypotheses on G are inherited by N, so we repeat the process on N, continuing until every qualifying prime has been used. This proves the first statement.

If the Sylow 2-subgroups of G are cyclic, then N has no normal p-subgroups for any prime p. On the other hand, the fact that all the Sylow subgroups of N are cyclic implies, by [P, 12.8 and 12.9], that the commutator subgroup $[N, N]$ is cyclic. Then the p-component of $[N, N]$ is normal in G, hence trivial, for each prime p. Therefore $[N, N] = 1$, and hence $N = 1$.

2.9. **Proposition.** *The following conditions are equivalent, for a finite solvable group $G = \Omega(G)$:*

(i) *G is a Frobenius complement.*

(ii) *G satisfies condition* (2.4).

(iii) *G is either cyclic (necessarily of square-free order) or isomorphic to $SL_2(3) \times C$, where C is a cyclic group of (necessarily square-free) order prime to 6.*

Proof. The parenthetical remarks in (iii) come from the observation that $\Omega(C)$ always has square-free order, for a cyclic group C. We already know that (i) $\Rightarrow$ (ii). One checks directly that $SL_2(3)$ is a Frobenius complement, so (iii) $\Rightarrow$ (i) by (1.7), (2.2), and (2.6). Assuming (ii), write $G = N \times C$ as in (2.8). If G has cyclic Sylow 2-subgroups, then G is cyclic, and (iii) holds. If G has generalized quaternion Sylow 2-subgroups, the center of N is a 2-group, and we appeal to [P, 18.4]. (Although N is supposed to be a Frobenius complement in order to apply [P, 18.4], the proof of [P, 18.4] depends only on the weaker hypothesis (2.4).) Of the four possible conclusions in [P, 18.4], one quickly rules out I, II, and IV; hence $N \cong SL_2(3)$.

2.10. **Theorem.** *Let G be a finite group with $G = \Omega(G)$. Then G satisfies* (2.4) *if and only if either G is cyclic or $G \cong SL_2(p) \times C$, for some Fermat prime p and a cyclic group C of (square-free) order prime to $p(p+1)$. Also, G is a Frobenius complement if and only if G is as above and $p = 3$ or 5.*

Proof. The last statement follows from (2.9) and the structure theory of non-solvable Frobenius complements in [P]. To prove the "if" statement, let $G = SL_2(p)$, where p is a Fermat prime. It will suffice to prove that G satisfies (2.4). Now $|G| = (p-1)p(p+1)$, and $p-1$ is a power of 2. We refer the reader to [DA, 38.1] for other relevant properties of G. In particular, G has an element b of order $p+1$, so the odd Sylow subgroups are cyclic. The Sylow 2-subgroups of G are generalized quaternion groups, [P, 13.5], so the subgroups of order 4 are cyclic. Since G has a unique involution, subgroups of order $2q$ are cyclic for each odd prime. There are no nonabelian groups of order pq if $q|(p+1)/2$, so we are reduced to consideration of subgroups of order qr, where $q < r$ are odd primes dividing $p+1$. We may assume the generator y of order r is a power of b. If x is an element of order q normalizing $\langle y \rangle$ then y^x is either y or y^{-1} (Step 1 of the proof of [DA, 38.1]), and y^{-1} is ruled out because $(-1)^r$ is not congruent to 1 modulo q. Thus $y^x = y$, that is, $\langle x, y \rangle$ is cyclic.

For the converse we may assume by (2.9) that G is not solvable, and by (2.8) that $O_q(G) = 1$ for every odd prime q. (O_q = largest normal q-subgroup.) Therefore $F(G)$, the Fitting subgroup, is a 2-group, so by (2.5) it is either cyclic or generalized quaternion. Suppose first that $F(G) = F^*(G)$, the generalized Fitting subgroup, [Su, Chapter 6, 6.10]. (Recall that $F^*(G)$ is generated by $F(G)$ and the components of G.) Then $C_G(F(G)) = Z(F(G))$, since this equality always holds for $F^*(G)$, [As2, (31.13)]. If $F(G)$ is cyclic or of order ≥ 16, then $\mathrm{Aut}(F(G))$ is a 2-group, [P, 9.10], and it follows that G itself is a 2-group, contradiction. Therefore $F(G)$ is the quaternion group of order 8, so $Z(F(G))$ has order 2 and $\mathrm{Aut}(F(G)) \cong S_4$, [P, 9.9]. But then $|G|$ divides 48, contradiction.

Therefore $F(G) < F^*(G)$, and G has a component L (a subnormal subgroup such that $L/Z(L)$ is a nonabelian simple group). Now $[L, F(G)] = \langle 1 \rangle$

by [As2, 31.6], and $[L, M] = \langle 1 \rangle$ if M is any component distinct from L, by [As2, 31.5]. Therefore $Z(L) \leq Z(F^*(G))$, and the latter, being a nilpotent normal subgroup, is a 2-group. Let S be a Sylow 2-subgroup of $F^*(G)$ containing $Z(F^*(G))$. Since $F^*(G)$ is not solvable, S cannot be cyclic, [P, 12.8], and by (2.5) S is a generalized quaternion group. But then $Z := Z(S)$ has order 2, and since $Z(L) \neq \langle 1 \rangle$ (by the comment immediately following (2.4)) we see that $Z(L) = Z(F^*(G)) = Z$. Therefore all the components of G have the same center Z, generated by the unique involution of $F^*(G)$.

Now we will show that $L = F^*(G)$. If M were another component of G, then $[L, M] = \langle 1 \rangle$ so $L \cap M = Z$. But L and M have generalized quaternion Sylow 2-subgroups, so $LM \geq C(2) \times C(2)$, violating (2.4). Similarly, since $F(G)$ is either cyclic or generalized quaternion and since $[L, F(G)] = \langle 1 \rangle$, it follows that $F(G) \leq L$. Thus L is the only component, and it contains $F(G)$, whence $L = F^*(G)$.

Next, we claim that $O(L) = \langle 1 \rangle$, that is, L has no nontrivial normal subgroups of odd order. For, if N is a minimal offender then N is abelian by the Feit-Thompson Theorem, and $O_q(N) \neq \langle 1 \rangle$ for some odd prime q. Then $O_q(L) \neq \langle 1 \rangle$, and since $L = F^*(G)$ is normal in G, we have $O_q(G) \neq \langle 1 \rangle$, contradiction. Now L is a quasisimple group with 2-rank $m(L) = 1$, and with $O(L) = 1$. By a theorem of Gorenstein and Walter, [Su, Chapter 6, 8.17], either $L \cong \mathrm{SL}_2(r)$ for an odd prime power $r = p^e > 3$, or else $L/Z \cong A_7$. The latter is impossible since $A_7 \geq C(3) \times C(3)$. Therefore $L \cong \mathrm{SL}_2(p)$, since the Sylow p-subgroups of $\mathrm{SL}_2(p^e)$ are not cyclic if $e > 1$. To see that p is a Fermat prime, let $\alpha \in GF(p)^*$ have odd prime order q. Then $\mathrm{Diag}(\alpha, \alpha^{-1})$ and the elementary matrix $1 + e_{12}$ generate a nonabelian group of order pq, contradicting (2.4).

It remains to be shown that $L = G$. Since $L = F^*(G)$, we have $Z = Z(L) = C_G(L)$, [Su, Chapter 6, 6.11]. Therefore $G/Z \leq \mathrm{Aut}(L) = \mathrm{PGL}_2(p)$. Then $|G| \leq 2|\mathrm{PGL}_2(p)| = 2|L|$, so $[G : L] \leq 2$. Therefore L contains every element of odd order in G. Since G has generalized quaternion Sylow 2-subgroups, any order-2 subgroup of G is a conjugate of Z and hence is in L. Since $G = \Omega(G)$, $L = G$.

3. $\mathbf{I}(G) \cap \mathbb{Z}$ IS A PRIME POWER

Let K/k be a finite Galois extension, and assume k is not algebraic over a finite field. We know, by (2.3), that $K^*/\Theta(K/k)$ is a torsion group if and only if the Galois group is not a Frobenius complement. Moreover, (1.4) tells us that in this case $K^*/\Theta(K/k)$ is a bounded group. In this section we will show that if the group $K^*/\Theta(K, k)$ is nontrivial and bounded, then its exponent is either p or p^2, for some prime p. The argument is purely group-theoretical: We will show, given any finite group G, that $\mathbf{I}(G) \cap \mathbb{Z}$ is either 0 or (p^e) for a prime p and an integer $e \leq 2$. We do not know whether it every happens that $\mathbf{I}(G) \cap \mathbb{Z} = (p^2)$. The only groups that would have to be checked are the groups $\mathrm{SL}_2(p)$ for Fermat primes $p > 5$.

3.1. **Theorem.** *Let G be a finite group such that $\mathbf{I}(G) \cap \mathbb{Z}$ is neither (0) nor (1). Then $\mathbf{I}(G) \cap \mathbb{Z} = (p)$ or (p^2) for some prime p.*

Proof. By (1.6) we may assume that G satisfies condition (2.4). Then, using

(2.2), (2.6), (2.7), and (2.10) we reduce to the case $G = \mathrm{SL}_2(p)$ where p is a Fermat prime greater than 5. Put $\mathbf{I} = \mathbf{I}(G)$. We will show first that

(3.1.1) $\qquad \mathbf{I}\mathbb{Z}_pG \neq \mathbb{Z}_pG$, but $\mathbf{I}\mathbb{Z}_qG = \mathbb{Z}_qG$ for every prime $q \neq p$.

3.2. **Lemma.** *Let G be any finite group, and let p be a prime. Then $\mathbf{I}\mathbb{Z}_pG = \mathbb{Z}_pG$ if and only if for every irreducible (equivalently, every absolutely irreducible) representation $\phi : G \to \mathrm{GL}(V)$ in characteristic p, there is an element $x \in G$ of prime order, say q, such that either*

(i) *$p \neq q$ and $\phi(x)$ fixes a nonzero vector in V, or*

(ii) *$p = q$ and $\phi(x)$ has a Jordan block of size p.*

Proof. Suppose $\mathbf{I}\mathbb{Z}_pG = \mathbb{Z}_pG$, and let V be any nonzero G-module in characteristic p. Since $\mathbf{I}$ is generated by elements of the form $1 + x + \cdots + x^{q-1}$, for elements x of prime order q, there must be such an x such that $T := \phi(x)$ does *not* satisfy $1 + T + \cdots + T^{q-1} = 0$. If $p \neq q$, then T has 1 as an eigenvalue since $1 - T^q = 0$. If $p = q$ then $1 + T + \cdots + T^{q-1} = (1 - T)^{p-1}$, and T must have a Jordan block of size p.

If $\mathbf{I}\mathbb{Z}_pG \neq \mathbb{Z}_pG$, choose a maximal left ideal $\mathfrak{m}$ containing $\mathbf{I}$. Then $p \in \mathfrak{m}$; hence $V := \mathbb{Z}_pG/\mathfrak{m}$ is an irreducible G-module in characteristic p, and $\mathbf{I}V = 0$. We may assume V is absolutely irreducible, by passing to a splitting field and choosing one of the composition factors of the extension of V. If $x \in G$ has prime order q, then $T := \phi(x)$ satisfies $1 + T + \cdots + T^{q-1} = 0$, making (i) and (ii) impossible.

We will also need the following result on transition from characteristic zero to characteristic p.

3.3. **Lemma.** *Let G be a finite group, and let R be a discrete valuation ring of characteristic zero with quotient field F and residue field k. If every irreducible FG-module is of dimension at most m, the same bound holds for the irreducible kG-modules.*

Proof. We may assume R is complete. Since FG is semisimple, one can find an RG-lattice $L = L_1 \oplus \cdots \oplus L_t$ such that $F \otimes L$ is free of rank one over FG and each $F \otimes L_i$ is irreducible. If M is the free RG-module of rank one, then $F \otimes M \cong F \otimes L$, and by Brauer's Theorem [DB, 48.7], $k \otimes M$ and $k \otimes L$ have the same composition factors. Since every irreducible kG-module occurs as a composition factor of $k \otimes M$, hence of some $k \otimes L_i$, the result follows.

Now let $G = \mathrm{SL}_2(p)$, p a Fermat prime greater than 5, and return to the proof of (3.1). Using (3.2) and the natural representation $G \to \mathrm{GL}_2(p)$, we see that $\mathbf{I}\mathbb{Z}_pG \neq \mathbb{Z}_pG$. Let q be a prime distinct from p, and let V be an absolutely irreducible G-module in characteristic q. We will show that G contains an element x as in (3.2), thereby proving (3.1.1).

Let $x = 1 + e_{12}$, an elementary matrix of order p. If x fixes a nonzero vector of V we are done, so assume it does not. Since x is conjugate to x^{m^2} for $1 \leq m \leq (p-1)/2$, it follows that the number of distinct eigenvalues of x is a multiple of $(p-1)/2$. Further, by considering the dimensions of the eigenspaces, we see that $\dim V$ is a multiple of $(p-1)/2$. However, (3.3) implies that $\dim V \leq p + 1$, since this holds in characteristic zero, [DA, 38.1].

Therefore

$$\dim V = (p-1)/2 \text{ or } p-1. \tag{3.1.2}$$

Let $b \in G$ be the element of order $p+1$ considered in the proof of (2.10), and let $y = b^m$ be an element of order 3. (Note $3|p+1$ as p is a Fermat prime.) If χ is an irreducible character of G in characteristic zero, then $\chi(y) \geq -2$. (See [DA, 38.1].) Since $p > 5$ it follows that y must have 1 as an eigenvalue in characteristic zero. The same then holds in characteristic q if $q \nmid |G|$, by [P, 15.11].

Consider the case $q = 2$ (actually, this argument will work as long as $q \neq 3$). Let K be a splitting field for G containing all $p(p+1)$st roots of unity, and let R be its ring of algebraic integers. Let $\mathfrak{m}$ be a maximal ideal of R containing q. By (the proof of) Lemma 3.3, we see that V is a composition factor of $L/\mathfrak{m}L$ for some RG-lattice L with $W := K \otimes L$ irreducible. Every nontrivial G-module has dimension at least $(p-1)/2$, since an element of order p must have at least that many nontrivial eigenvalues. It follows that $L/\mathfrak{m}L$ has composition factors consisting of at most two trivial factors and V, unless $\dim W = (p-1)/2$ and the rank of L is at least $p-1$. So exclude that case for the moment. If y has no fixed points on V, then (since both eigenvalues of order 3 occur with the same multiplicity) $\chi(y) \leq 2 - (1/2)(\dim V)$, where χ is the character of W. Since $p \geq 17$, this contradicts the fact that $\chi(y) \geq -2$.

In the excluded case, let σ be the automorphism of K that generates the automorphism group on pth roots of unity and fixes $(p+1)$st roots of unity. Then σ acts on R, K, and $R/\mathfrak{m}$, and so for any G-module M over one of those rings we can define M^σ in the obvious way. Then W and W^σ are isomorphic, since the character is invariant under σ for any character of degree at least $p-1$. However V and V^σ are not isomorphic, since the eigenvalues of the element of order p will be different. Thus by Brauer's theorem, V and V^σ are both composition factors of $L/\mathfrak{m}L$. In particular, y has no fixed points on either V or V^σ, so 1 has multiplicity at most 2 as an eigenvalue for y on W. We now obtain a contradiction as above.

Finally, suppose q is an odd prime dividing $p+1$, and let b^s generate a Sylow q-subgroup S of G. Since the centralizer of every nontrivial subgroup of S is $\langle b \rangle$ (by Step 1 of the proof of [DA, 38.1]), it follows that $S \cap T = \langle 1 \rangle$ for every Sylow q-subgroup T distinct from S. Letting $N = N_G(S)$, we have, by the Green Correspondence [Al, p. 71, Theorem 1],

$$V_N = U \oplus W, \tag{3.1.3}$$

where U is an indecomposable N-module and W is a projective N-module. If $W \neq 0$ then W is a nonzero projective S-module. But then any element of order q in S acts on W with Jordan blocks of size q. Therefore we assume $W = 0$, that is, V is indecomposable as an N-module. Recall from Step 1 of the proof of [DA, 38.1] that $\langle b \rangle$ has index 2 in N, and if $g \in N - \langle b \rangle$ we have $b^g = b^{-1}$. It follows that $g^2 \in Z(G)$. Therefore, any absolutely irreducible representation of N is at most two-dimensional. (If v is an eigenvector for b, then $\langle v, gv \rangle$ is an N-invariant subspace.) It follows that V is a direct sum of at most 2 indecomposable S-modules, whence $\dim V \leq 2|S|$. (See the discussion on pp. 34, 35, 42, 43 of [A1]. The main point is that V is uniserial as an N module.) Since $2|S|$ divides $p+1$, it follows from (3.1.2)

that $\dim V = (p-1)/2$ and $|S| = (p+1)/2$. But $3|p+1$, so $q = 3$. It follows from (1.13) or directly that the only solution to $2 \cdot 3^e = p+1$ (p Fermat) is $e = 2$, $p = 17$; and so $\dim V = 8$. Then $|N/S| = 4$, and it follows that V is indecomposable as an S-module. Therefore, an element of order 3 in S acting on V has two Jordan blocks of size 3.

We have now verified (3.1.1), and it follows that $\mathbf{I} \cap \mathbb{Z} = (p^e)$ for some $e \geq 1$. Let D be the ring of p-adic integers, let $K \supseteq D$ be a splitting field for G, and let R be the integral closure of D in K. To prove that $p^2 \in \mathbf{I}$, it will suffice to show that $p^2 \in \mathbf{I}(RG)$.

Note that R is local (as D is complete); let (π) be its maximal ideal. Let $\Gamma \supseteq RG$ be a maximal order in KG. Then $\Gamma = \bigoplus_i \Gamma_i$, where $\Gamma_i = \mathrm{End}_{RG}(L_i)$ and each L_i is an RG-lattice with KL_i irreducible. We have already seen, using the character table of G, that the element y of order 3 has 1 as an eigenvalue for each irreducible representation (in characteristic zero). Since y has a nonzero fixed point on L_i, it also has a nonzero fixed point on $L_i/\pi L_i$. Therefore $1 + y + y^2$ acts nontrivially on $L_i/\pi L_i$ (since $p \neq 3$). Then $\pi L_i \not\supseteq (1 + y + y^2)L_i$, and it follows that $\Gamma \mathbf{I} \Gamma = \Gamma$. Since $RG \supseteq |G|\Gamma = p\Gamma$, we have $\mathbf{I}(RG) = (RG)\mathbf{I}(RG) \supseteq (p\Gamma)\mathbf{I}(p\Gamma) = p^2 \Gamma \mathbf{I} \Gamma = p^2 \Gamma$.

If we do not require $\mathscr{H}$ to contain all the minimal subgroups of G, there are easy examples to show that $L(\mathscr{H}) \cap \mathbb{Z}$ need not be a prime power.

3.4. **Example.** Let n be any positive integer, and let $G = C(n) \times C(n) = \langle x \rangle \times \langle y \rangle$. Let $A_i = \langle xy^i \rangle$, $0 \leq i < n$, and for each prime divisor p of n, let $B_p = \langle y^{n/p} \rangle$. If $\mathscr{H} = \{A_i\} \cup \{B_p\}$, a slight modification of the proof of (1.6) shows that $n \in L(\mathscr{H})$. To see that $L(\mathscr{H}) \cap \mathbb{Z} = (n)$, let ζ be a primitive nth root of unity, and map $\mathbb{Z}G$ onto $\mathbb{Z}[\zeta]$ by $x \mapsto 1$, $y \mapsto \zeta$. Then $\sum A_0 \mapsto n$, while the other $\sum A_i$ and all the $\sum B_p$ map to 0 in $\mathbb{Z}[\zeta]$.

4. The groups with $\mathbf{I}(G) \neq \mathbb{Z}G$

We begin by classifying the groups that are "almost" Frobenius complements. For a prime p, we let $\Omega_{p'}(G)$ be the subgroup of G generated by elements of prime order $\neq p$. Recall that $O_p(G)$ is the largest normal subgroup of G, and $O(G)$ is the largest normal subgroup of odd order.

H. Blau has informed us that W. Stewart in unpublished work [St] has obtained a result similar to Proposition 4.1.

4.1. **Proposition.** *Let G be a finite group and p a prime. Assume $O_p(G) = 1$, and put $H = \Omega_{p'}(G)$. These are equivalent:*

(a) *There is a representation $\sigma : G \to \mathrm{GL}(V)$ in characteristic p such that if $x \in G$ has prime order $\neq p$ then $\sigma(x)$ has no nonzero fixed points in V.*

(b) *There is a representation $\sigma : H \to \mathrm{GL}(V)$ in characteristic p such that if $x \in H$ has prime order $\neq p$ then $\sigma(x)$ has no nonzero fixed points in V.*

(c) *$H \cong A \times B$ where B is cyclic of square-free order prime to $p|A|$, and one of the following holds:*

(i) *$A = \langle 1 \rangle$.*

(ii) *$p = 2$; and either $A \cong Sz(2^{2k+1})$, $k \geq 1$, or $A \cong \mathrm{SL}_2(2^m)$, $m \geq 2$, or $A \cong Sz(2^{2k+1}) \times \mathrm{SL}_2(2^m)$, where $k \geq 1$, $m \geq 1$, and $|Sz(2^{2k+1})|$ and $|\mathrm{SL}_2(2^m)|$ have no common odd prime factor.*

(iii) *$p = 3$; and $A \cong \mathrm{SL}_2(q)$ with $q = 5, 7, 17$ or 3^k, $k \geq 2$.*

(iv) *$p > 3$; and $A \cong \mathrm{SL}_2(q)$ with $q = 3, 5$ or p^k, $k \geq 1$.*

Proof. By considering the restriction of σ to H, we see that (a) implies (b). Similarly, if (b) holds, the induced representation σ^G shows that (a) holds. To show that (c) implies (b), we shall exhibit the representation. It suffices to do so for A and B separately, since the tensor product of the individual representations will satisfy (b) for the direct product (since the orders of A and B are relatively prime). For the cyclic group B, we just take a faithful one-dimensional representation (over a splitting field). If $A = \mathrm{SL}_2(q)$ and p divides q, take the natural two-dimensional representation. If $A = \mathrm{SL}_2(5)$ and p is not 2 or 5, take the two-dimensional representation (which occurs in characteristic 0 and hence in every characteristic). If $p > 3$ and $A = \mathrm{SL}_2(3)$, again take the two-dimensional representation. If $p = 3$ and $A = \mathrm{SL}_2(7)$ or $\mathrm{SL}_2(17)$, we can take a faithful representation of dimension 6 or 16, respectively. Finally, assume $p = 2$. If A is a Suzuki group, take the natural 4-dimensional representation. (Recall A is a subgroup of the 4-dimensional symplectic group.) If A is a direct product of a special linear group and a Suzuki group, take the tensor product of the natural 2-dimensional representation and the 4-dimensional representation.

Now assume (b) holds. The following observations are crucial:

(1) If $q \geq r$ are primes distinct from p, then every subgroup of H of order qr is cyclic.

(2) If q is a prime distinct from p, then either the Sylow q-subgroup of H is cyclic, or $q = 2$ and the Sylow q-subgroup of H is generalized quaternion.

To prove (1), suppose D is a noncyclic subgroup of H of order qr. Then, if $h \in D$ has order r, we know that $\sigma(1) + \sigma(h) + \cdots + \sigma(h^{r-1}) = 0$, since any nonzero vector in its image would be an eigenvector for $\sigma(h)$. In particular, this holds for the elements h_i considered in the proof of (1.6). The computations in the proof of (1.6) (done explicitly in the case $q = r$ and left to the reader in the case $q > r$) now show that $q\sigma(1) = 0$, a contradiction, since q is different from the characteristic. This proves (1); and (2) follows, by (2.5).

Since $O_p(H) = \langle 1 \rangle$, it follows, exactly as in the proof of (2.8), that $H = N \times C$, where C is cyclic of square-free order relatively prime to $p|N|$ and $O(N) = \langle 1 \rangle$. (As in the proof of (2.10), the Feit-Thompson Theorem is used to deduce that $O(N) = \langle 1 \rangle$ from the fact that $O_q(N) = \langle 1 \rangle$ for every odd q.) Thus we may assume that $H = N$.

Suppose first that $p = 2$. Since $O(H) = \langle 1 \rangle$ and $O_2(H) = \langle 1 \rangle$, it follows from [As2, 31.7] that $F^*(H) = E(H)$ is a direct product $L_1 \times \cdots \times L_t$ of simple groups. By (2) and [As1, Lemma 3], L_1 is isomorphic to one of the following:

$$
\begin{aligned}
&J_1, \\
&Sz(2^{2k+1}), \qquad k \geq 1, \text{ or} \\
&\mathrm{PSL}_2(r), \qquad r = 2^k,\ k \geq 2, \text{ or } 5 < r \text{ prime}.
\end{aligned}
$$

We rule out the Janko group J_1 because it has a noncyclic subgroup of order 21. If $L_1 \cong \mathrm{PSL}_2(r)$ with $5 < r$ prime, we see by (1) that r is a Fermat prime. Then the argument in the proof of Proposition (3.1), specifically, the case $q = 2$, shows that σ cannot exist.

Thus $L_1 \cong Sz(q_1)$ or $\mathrm{SL}_2(q_1)$ with q_1 a power of 2. We argue similarly for each L_i. Since every odd Sylow subgroup of H is cyclic, $\gcd(|L_i|, |L_j|)$ is a power of 2 for $i \neq j$. But $|Sz(q_i)|$ and $|\mathrm{SL}_2(q_j)|$ are multiples of 5 and 3, respectively, so $t \leq 2$ and we have (ii) of (c).

Now assume $p > 2$. Arguing exactly as in the proof of (2.8), we see that if the Sylow 2-subgroups of N are cyclic, then N is cyclic. Similarly, if N is solvable, the argument given in the proof of (2.9) shows that $N \cong \mathrm{SL}_2(3)$. (This does not happen if $p = 3$, since $|\Omega_{3'}(\mathrm{SL}_2(3))| = 2$.) So we can assume N has generalized quaternion subgroups and is not solvable. It follows as in (2.10) that either $N \cong \mathrm{SL}_2(q)$ with q an odd prime power or $N/Z \cong A_7$, where $|Z| = 2$. Suppose first that $N/Z \cong A_7$. If $p > 3$ this cannot occur since A_7 has noncyclic Sylow 3-subgroups. If $p = 3$, inspection of the 3-modular irreducible characters of $N = H$ shows that no such representation as in (b) can exist.

Therefore $N \cong \mathrm{SL}_2(q)$ with $3 < q$ an odd prime power, and we claim that either $q = 5$, or $p|q$, or $p = 3$ and $q \in \{7, 17\}$. Assume this is not the case. Then $q = r^e > 5$, with r an odd prime distinct from p. Since the Sylow r-subgroup is cyclic, q is prime. As in the proof of (3.1), we can assume that $\dim V = q - 1$ or $(q-1)/2$. We can also assume that G acts faithfully on V.

If p does not divide $q + 1$, then V is a projective G-module (see [F1, Theorem 2.10, p. 276]), and so $V = L/\mathfrak{m}L$ for some RG-lattice L, where R and $\mathfrak{m}$ are as in (3.1) (but now $p \in \mathfrak{m}$). By [DA, 38.1], it follows that any element of order 3 has fixed points on L and so on V. If $p > 3$, this is a contradiction. If $p = 3$, then, as $q \notin \{7, 17\}$, there is a prime $d > 6$ with $d|q^2 - 1$. By [DA, 38.1], an element of order d has fixed points on L and so on V. So $p|q + 1$.

If q is not a Fermat prime, let c be an odd prime divisor of $q - 1$. Then there is a noncyclic subgroup of order qc, contradicting (1) above. Also, if $p > 3$, then, arguing exactly as in (3.1) for the case of characteristic 2, we see that every element of order 3 has a fixed point on V. So assume $p = 3$ and q is a Fermat prime. Then V is a composition factor of $L/\mathfrak{m}L$ for some RG-lattice L with $W := K \otimes L$ irreducible. The dimensions of the faithful irreducible KG-modules are $(q-1)/2$, $q - 1$, and $q + 1$. (See [DA, 38.1], noting that $q \equiv 1 \pmod 4$.) If $\dim W = q + 1$, then $L/\mathfrak{m}L$ is projective and irreducible for any RG-lattice L in W (see [Se, Proposition 46, p. 136]). If $\dim W = (q-1)/2$, then $L/\mathfrak{m}L$ is irreducible, since $\mathrm{SL}_2(q)$ has no smaller nontrivial representations in any characteristic different from q. If $3 < b$ is a prime divisor of $q + 1$, we see by the character table that an element of order b has fixed points on L and so on $L/\mathfrak{m}L$. Finally, suppose $\dim W = q - 1$. Since the elements of order p have no fixed points on W, either $L/\mathfrak{m}L$ is irreducible or $L/\mathfrak{m}L$ has two composition factors of dimension $(q-1)/2$. Moreover, these two composition factors are conjugate under the Galois group. (See the argument in the proof of (3.1).) Again, from the character table, we see that an element of order b has fixed points on W, hence on L, and so on all composition factors of $L/\mathfrak{m}L$. This completes the proof.

We can now classify the groups G for which $\mathbf{I}(G) \neq G$. If G is not a Frobenius complement, then there is a unique prime p for which $\mathbf{I}(G)\mathbb{Z}_pG \neq \mathbb{Z}_pG$, by (3.1). Therefore (2.2), (2.10) and the theorem below give the complete classification. Note that condition (1) in (4.2) is identical to (c) of (4.1) except when $p = 3$: This time we cannot rule out the possibility that $A \cong \mathrm{SL}_2(3)$.

4.2. **Theorem.** *Let G be a finite group and let p be a prime. Set $H = \Omega(G)/O_p(\Omega(G))$. Then $\mathbf{I}(G)\mathbb{Z}_pG \neq \mathbb{Z}_pG$ if and only if the following conditions*

(1) *and* (2) *are both satisfied*:

(1) $H \cong A \times B$, *where* B *is cyclic of square-free order prime to* $p|A|$, *and one of the following holds*:

(i) $A = \langle 1 \rangle$.

(ii) $p = 2$; *and either* $A \cong Sz(2^{2k+1})$, $k \geq 1$, *or* $A \cong \mathrm{SL}_2(2^m)$, $m \geq 2$, *or* $A \cong Sz(2^{2k+1}) \times \mathrm{SL}_2(2^m)$, *where* $k \geq 1$, $m \geq 1$, *and* $|Sz(2^{2k+1})|$ *and* $|\mathrm{SL}_2(2^m)|$ *have no common odd prime factor.*

(iii) $p = 3$; *and* $A \cong \mathrm{SL}_2(q)$ *with* $q = 3, 5, 7, 17$ *or* 3^k, $k \geq 2$.

(iv) $p > 3$; *and* $A \cong \mathrm{SL}_2(q)$ *with* $q = 3, 5$ *or* p^k, $k \geq 1$.

(2) *If* $p = 2$, *or if* $p = 3$ *and* $A \cong \mathrm{SL}_2(q)$ *with* $q = 7$ *or* 17, *then every element of order* p *in* G *is in* $O_p(G)$.

Proof. If (1) and (2) are satisfied, one uses the representations described in the proof of (4.1) to conclude that $\mathbf{I}(G)\mathbb{Z}_pG \neq \mathbb{Z}_pG$. For the converse, we may assume as usual that $G = \Omega(G)$. By (3.2), there is an irreducible representation $\sigma : G \to \mathrm{GL}(V)$ in characteristic p, such that

(3.2, i) if $x \in G$ has prime order $q \neq p$, then $\sigma(x)$ does not have 1 as an eigenvalue, and

(3.2, ii) if $x \in G$ has prime order p, then $T := \sigma(x)$ satisfies $1 + T + \cdots + T^{p-1} = 0$.

It follows from (3.2, i) that $\ker\sigma \leq O_p(G)$. Since σ is irreducible, $O_p(G) \leq \ker\sigma$ by [A1, Chapter 1, §3, Corollary 3 and Theorem 4]. Thus $O_p(G) = \ker\sigma$, and we can view σ as a faithful representation of H. By (3.2, i), H satisfies (b), and hence (a) of (4.1), so write $K := \Omega_{p'}(H) = A \times B$ as in (4.1), (c). Note that A and B are both normal in H. We want to show that $H = K$ except in one special case.

Let Δ be the image in H of the set of elements of order p in G. Since $G = \Omega(G)$, $H = \langle K, \Delta \rangle$. If $p = 2$, then $\Delta = \langle 1 \rangle$ by (ii), so $H = K$, and conditions (1) and (2) are satisfied. We assume from now on that $p > 2$. Suppose $y \in \Delta$, respectively, $y \in H$ has prime order $r \neq p$. Then y cannot normalize any abelian p'-subgroup D of H unless y commutes with D. (Otherwise, as D is cyclic and every eigenspace of D is faithful, y must permute the eigenspaces of D in orbits of size p, respectively, r. Then V is a free $\langle y \rangle$-module. This contradicts (3.2, i) if y has order r and (3.2, ii) if $y \in \Delta$.) Thus, exactly as in the proof of (2.8), it follows that if R is a nontrivial normal r-subgroup, $2 \neq r$ prime, then $H = H_0 \times R$ where $r \nmid |H_0|$, and $|R| = r$. Since $O_p(H) = \langle 1 \rangle$, we have $H = N \times C$, where C is cyclic of the square-free order prime to $2p$, and N has no nontrivial normal subgroups of odd order. Then $\langle A, \Delta \rangle \leq N$, and since $H = \langle K, \Delta \rangle$ it follows that $N = \langle A, \Delta \rangle$.

If $y \in \Delta$, we claim y induces an inner automorphism on A. For otherwise p divides $|\mathrm{Out}(A)|$; and since $p > 2$ it follows that $A \cong \mathrm{SL}_2(p^e)$ where $p|e$, and y induces a field automorphism on A. Therefore y normalizes but does not centralize some subgroup of prime order dividing $p^e - 1$, and we have already seen that this is impossible.

Thus, for each $y \in \Delta$, there is an element $b \in A$ such that $yay^{-1} = bab^{-1}$ for all $a \in A$. Then $y = b(b^{-1}y) \in AC_N(A)$, so $\Delta \subseteq AC_N(A) = N$. If $A = \langle 1 \rangle$, then K is cyclic and N/K is a p-group. Thus $N = \langle \Delta \rangle$ is solvable. Argue as in (2.10) to conclude that either $N = \langle 1 \rangle$ or $N \cong \mathrm{SL}_2(3)$ (and so $p = 3$). Since $H = N \times C$, we have the special case $q = 3$ of (iii). If $A \neq \langle 1 \rangle$,

then (since $p > 2$) $|Z(A)| = 2$. Let $C = C_N(A)$ and $Z = Z(A)$. Since $N = CA$, it follows that $N/Z = C/Z \times A/Z$. Since the Sylow 2-subgroup of N is a generalized quaternion group, it follows that C/Z has odd order. Thus $C = ZO(C)$. However, since $O(N) = \langle 1 \rangle$, this implies $O(C) = \langle 1 \rangle$. Thus $C = Z$ is contained in K, whence Δ is as well. Therefore $H = K$, and (1) is proved.

To prove (2), suppose $p = 3$ and $H = \mathrm{SL}_2(q) \times B$ with $q = 7$ or 17. If $y \in H$ has order 3, we see by inspection that $1 + \sigma(y) + \sigma(y^2) \neq 0$. Thus, if $x \in G$ has order 3, x must be trivial in H, whence $x \in O_3(G)$.

Summary. At this point the reader should return to (1.14) to recall the field-theoretic implications of the integer n, where $\mathbf{I}(G) \cap \mathbb{Z} = (n)$. We learned in §3 that either $n = 0$, $n = 1$, $n = p$, or $n = p^2$, where p is prime. Assume, now, that K/k is Galois with Galois group G, and that k has an infinite set, of finite character, consisting of discrete rank-one valuations that split completely in K. (By (1.8) such valuations exist for algebraic number fields and function fields; in particular they exist if k is finitely generated but not algebraic over an arbitrary field.) Combining the field-theoretic results with our classification theorems (2.10) and (4.2), we have the following possibilities:

$n = 0 \Leftrightarrow K^*/\Theta(K/k)$ has elements of infinite order.
$\Leftrightarrow G$ is a Frobenius complement.
$\Leftrightarrow \Omega(G) \cong A \times B$, where B is a cyclic group of (square-free) order relatively prime to $|A|$, and A is either trivial or $\mathrm{SL}_2(3)$ or $\mathrm{SL}_2(5)$.

$n = p$ or $p^2 \Leftrightarrow K^*/\Theta(K/k)$ is an infinite bounded group of exponent p or p^2.
$\Leftrightarrow G$ is not a Frobenius complement and G satisfies (1) and (2) of (4.2).

The only other possibility is $n = 1$, in which case $K^* = \Theta(K/k)$.

Remarks. 1. Let H be a finite group with $O_p(H) = \langle 1 \rangle$ for a fixed prime p. We can find a finite $(\mathbb{Z}/p\mathbb{Z})H$-module M and an element $\alpha \in H^2(H, M)$ such that α restricted to every cyclic subgroup of H is nonzero. Let G be the extension of H by M corresponding to α. Then it follows that $M = O_p(G)$ contains all elements of order p in G (from the fact that the restriction of α is nonzero on every subgroup of order p). Moreover, if $H = \Omega_{p'}(H)$, it follows that $G = \Omega(G)$. Since $\mathrm{SL}_2(3)$ is generated by its elements of order 3, it thus follows that given any H, p as in (4.2) there exists a $G = \Omega(G)$ with $G/O_p(G) \cong H$.

2. Notice that (4.2) implies that $\mathbf{I}(G) = \mathbb{Z}G$ for every nonabelian simple group G. There is, however, a direct proof of this fact: By Glauberman's Z^* Theorem, it follows that G contains an elementary abelian group of order 4. (See the comments after [DA, 19.8].) Therefore $2 \in \mathbf{I}(G)$. By the Baer-Suzuki Theorem, [As2, 39.6], G also contains an odd dihedral group; therefore $\mathbf{I}(G)$ contains an odd prime.

5. The case of a non-Galois extension

Let E_1 and E_2 be subfields of K. Assume K is not an algebraic extension of a finite field, and neither extension K/E_i is purely inseparable. If K has finite degree over $E_1 \cap E_2$, then $K^*/E_1^*E_2^*$ is known to have infinite rank, [W]. In this section we will prove this result under the weaker assumption that K is algebraic over $E_1 \cap E_2$. (See (5.5).) On the other hand, we show, in (5.6), that every field K of infinite transcendence degree over its prime subfield has proper subfields E_1 and E_2 such that $K^* = E_1^*E_2^*$.

We will reprove the result from [W], but in a stronger form (5.3) that explains in a quantitative way why two intermediate fields should behave differently from three. Our proof is much easier than the one in [W] and makes use of the rational group algebra $\mathbb{Q}G$. It also uses a result (5.2) similar to (1.4), in which the top field K is really an intermediate field for a Galois extension. This allows us to study the multiplicative structure of finite-dimensional separable extensions that are not necessarily Galois.

5.1. **Lemma.** *Let M/k be a finite Galois extension with Galois group G, and assume that k is not an algebraic extension of a finite field. Then the $\mathbb{Q}G$-module $\mathbb{Q} \otimes M^*$ has a free $\mathbb{Q}G$-module of infinite rank as a direct summand.*

Proof. We follow the proof of (1.4), with M in place of k. Let $\Psi_i : \mathbb{R} \otimes M^* \to \mathbb{R}G$ be the homomorphisms induced by the maps Φ_i of (1.4.1). For each $d \geq 1$, $(\Psi_1, \ldots, \Psi_d)$ maps $\mathbb{R} \otimes M^*$ onto $(\mathbb{R}G)^{(d)}$, by the approximation theorem. Since $\mathbb{R}G$ and $\mathbb{Q}G$ are semisimple the desired result follows easily.

In fact, Jia Bao-Ping [Ji] has shown that $\mathbb{Q} \otimes M^*$ is a free $\mathbb{Q}G$-module. He has also obtained the next result independently:

5.2. **Proposition.** *Let M, k, and G be as in* (5.1), *and let $K, E_1, \ldots, E_t$ be intermediate fields with $K \supseteq E_i$ for all i. Let $A, B_1, \ldots, B_t$ be the corresponding subgroups of G, and put $D = E_1^* \cdots E_t^*$ $(= \Theta(\{B_1, \ldots, B_t\})$ in the notation of* §1). *Then the following are equivalent:*

(a) *K^*/D is bounded.*
(b) *K^*/D is torsion.*
(c) *K^*/D has finite rank.*
(d) *$L(\{A\})/L(\{B_1, \ldots, B_t\})$ is torsion (hence finite).*

Proof. Clearly (a) $\Rightarrow$ (b) $\Rightarrow$ (c). Assuming (d), put $r = [M : K]$ and $n = |L(\{A\})/L(\{B_1, \ldots, B_t\})|$. If $\alpha \in K^*$, we have $\alpha^r = \alpha^{\sum A}$, and $n(\sum A) \in L(\{B_1, \ldots, B_t\})$. By (1.1), $\alpha^{nr} \in D$; thus (d) $\Rightarrow$ (a). To show that (c) $\Rightarrow$ (d), note that $(\mathbb{Q} \otimes M^*)^{L(\{A\})} = \mathbb{Q} \otimes K^*$ and $(\mathbb{Q} \otimes M^*)^{L(\{B_1, \ldots, B_t\})} = \mathbb{Q} \otimes D$, by (1.1). If (d) fails, the quotient $\mathbb{Q}L(\{A\})/\mathbb{Q}L(\{B_1, \ldots, B_t\})$ is nontrivial, and by (5.1), $(\mathbb{Q} \otimes M^*)^{L(\{A\})}/(\mathbb{Q} \otimes M^*)^{L(\{B_1, \ldots, B_t\})}$ has a direct summand isomorphic to a direct sum of infinitely many copies of this quotient. Thus $\mathbb{Q} \otimes K^*/\mathbf{Q} \otimes D$ is infinite-dimensional, and (c) fails.

5.3. **Theorem.** *Let K/k be a finite algebraic extension, and assume k is not an algebraic extension of a finite field. Let $E_1, \ldots, E_t$, $t \geq 2$, be intermediate fields such that $K^*/E_1^* \cdots E_t^*$ has finite rank (equivalently, is bounded). Let $d_i = [K : E_i]_s$ (the separable degree), and let $d = [K : k]_s$. Then*

$$\frac{1}{d_1} + \cdots + \frac{1}{d_t} \geq 1 + \frac{t-1}{d}.$$

Proof. Let L, respectively F_i, be the subfield of elements of K, respectively E_i, separable over k. Then $L^*/F_1^* \cdots F_t^*$ has finite rank and hence is bounded, by (5.2). The parenthetical remark that $K^*/E_1^* \cdots E_t^*$ is bounded follows from the fact that K^*/L^* is bounded. Since $[L : F_i] = d_i$ (by multiplicativity of the separable degree function) and $[L : k] = d$, we may as well change notation and simply assume that K/k is separable. Let M/k be the normal closure of K/k, and let G, A, B_i be as in (5.2). Then $\mathbb{Q}L(\{A\}) = \mathbb{Q}L(\{B_1\}) + \cdots + \mathbb{Q}L(\{B_t\})$ in the group algebra $\mathbb{Q}G$. But, for any subgroup H of G, $\mathbb{Q}L(\{H\})$ has dimension $[G : H]$. Since the subspaces $\mathbb{Q}L(\{B_i\})$ all have the one-dimensional subspace $\mathbb{Q}L(\{G\})$ in their intersection, we have

$$d \leq \frac{d}{d_1} + \cdots + \frac{d}{d_t} - (t-1).$$

If $t = 2$, we see that either $d_1 = 1$ or $d_2 = 1$, that is, K is purely inseparable over E_1 or E_2. If $t = 3$, the only possibilities with $d_i > 1$ are $2, 2, m$, with $m \leq d/2$ (of course!); or $2, 3, m$, with $m \leq 6/(1 + 12/d)$.

The next result will be used to handle algebraic extensions that are not finite-dimensional.

5.4. **Lemma.** *Let L/k be an algebraic field extension, and let $E_1, \ldots, E_t$ be intermediate fields. If N/k is a finite Galois extension, then*

$$((E_1^* \cdots E_t^*) \cap N)/((E_1^* \cap N) \cdots (E_t^* \cap N))$$

is torsion.

Proof. By replacing each E_i by its subfield of elements separable over k, we may assume that each E_i/k is separable. Let $x = y_1 \cdots y_t \in N$, with $y_i \in E_i^*$. Let M be the normal closure over k of $N(y_1, \ldots, y_t)$. Set $G = \mathrm{Gal}(M/k)$, $f = \sum \mathrm{Gal}(M/N)$, and $f_i = \sum \mathrm{Gal}(M/(M \cap E_i))$. (These are sums in $\mathbb{Z}G$ as in §1.) Since N/k is normal, f is central in $\mathbb{Z}G$. Let $n = [M : N]$, let $m_i = [M : M \cap E_i]$, and let m be the least common multiple of the m_i. Now $y_i^{f_i} = y_i^{m_i}$, so $y_i^m = z_i^{f_i}$ for some $z_i \in M \cap E_i$. Then $y_i^{mf} = z_i^{f_i f} = z_i^{f f_i} \in M \cap E_i$, and of course $y_i^{mf} \in N$. Thus $y_i^{mf} \in E_i^* \cap N$, whence $x^{mn} = x^{mf} \in (E_1^* \cap N) \cdots (E_t^* \cap N)$.

5.5. **Theorem.** *Let E_1 and E_2 be subfields of K such that K is algebraic over $k := E_1 \cap E_2$. Assume K is not an algebraic extension of a finite field and neither extension K/E_i is purely inseparable. Then $K^*/E_1^* E_2^*$ has infinite torsion-free rank.*

Proof. As in the proof of (5.3), we may assume K/k is separable. Choose $x \in K - (E_1 \cup E_2)$, and let N be the normal closure of $k(x)$ over k. Using (5.4), we may replace the E_i and K by their intersections with N, and assume that K/k is a finite extension. Now apply the case $t = 2$ of (5.3).

Next we show that the previous result can fail if K is not assumed to be algebraic over k.

5.6. **Theorem.** *Let K be a field of infinite transcendence degree over its prime subfield k, and let E be any subfield such that K/E is algebraic. Then there*

exists a subfield F of K such that K has infinite transcendence degree over F and $K^* = E^*F^*$.

Proof. By hypothesis, the transcendence degree of K/k is equal to $|K|$. Choose a transcendence basis X for E/k, and write X as the disjoint union of sets X_i, $i = 1, 2, 3, \ldots$, each of cardinality $|K|$. Let E_i, respectively, K_i be the algebraic closure of $k(X_1, \ldots, X_i)$ in E, respectively, in K. Then E is the ascending union of the E_i, and K is the ascending union of the K_i. Let r_i be a surjection from X_i to K_{i-1} for each $i > 0$. Set $F_1 = k$, and define F_{i+1} inductively by $F_{i+1} = F_i(\{x \cdot r_i(x) : x \in X_i\})$. It follows that

(i) F_{i+1} is a subfield of K_i, and

(ii) $\{x \cdot r_i(x) : x \in X_i\}$ is algebraically independent over K_{i-1}.

Since F_i is a subfield of K_{i-1}, F_{i+1} is purely transcendental over F_i, whence

(iii) $S := \{x \cdot r_i(x) : x \in X_i, i > 0\}$ is algebraically independent over k.

Now let $F = k(\{x \cdot r_i(x) : x \in X_i, i > 1\})$. By (iii), the transcendence degree of K over F is $|X_1|$. Also, for each $i > 1$ and each $x \in X_i$, we have

(iv) $r_i(x) = x^{-1} \cdot (x \cdot r_i(x)) \in E^*F^*$.

Therefore $E^*F^* \supseteq K_{i-1}$ for every $i > 1$, and it follows that $E^*F^* = K^*$.

One can of course enlarge F to obtain examples in which K/E and K/F are both proper algebraic extensions, yet $K^* = E^*F^*$. At the other extreme, one can modify the construction to get examples in which both extensions K/E and K/F have infinite transcendence degree. We do not know whether or not there are examples with $K^* = E^*F^*$, where E and F are proper subfields of K, and K has finite transcendence degree over $E \cap F$. When K/E and K/F are purely inseparable, it is even conceivable that $K/(E \cap F)$ could be algebraic.

References

[As1] M. Aschbacher, *Thin finite simple groups*, J. Algebra **54** (1978), 50–152.

[As2] ——, *Finite group theory*, Cambridge Univ. Press, Cambridge, 1986.

[Al] J. L. Alperin, *Local representation theory*, Cambridge Univ. Press, Cambridge, 1986.

[B] A. Brandis, *Über die multiplikative Struktur von Körpererweiterungen*, Math. Z. **87** (1965), 71–73.

[DA] L. Dornhoff, *Group representation theory, Part* A, Dekker, New York, 1971.

[DB] ——, *Group representation theory, Part* B, Dekker, New York, 1972.

[DM] E. D. Davis and P. Maroscia, *Affine curves on which every point is a set-theoretic complete intersection*, J. Algebra **87** (1984), 113–135.

[F1] W. Feit, *The representation theory of finite groups*, North-Holland, Amsterdam, 1982.

[F2] ——, *On large Zsigmondy primes*, Proc. Amer. Math. Soc. **102** (1988), 29–36.

[G] R. Guralnick, *A question of Stafford about affine* PI *algebras*, Comm. Algebra **18** (1990), 3055–3057.

[H] W. J. Haboush, *Multiplicative groups of Galois extensions* (preprint).

[Ja] G. Janusz, *Algebraic number fields*, Academic Press, New York, 1973.

[Ji] Jia Bao-Ping, *Splitting of rank-one valuations*, Comm. Algebra **19** (1991), 777–794.

[NNT] M. Nagata, T. Nakayama, and T. Tuzuku, *On an existence lemma in valuation theory*, Nagoya Math. J. **6** (1953), 59–61.

[P] D. Passman, *Permutation groups*, Benjamin, New York, 1968.

[Se] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977.

[St] W. B. Stewart, *Largely fixed point free groups*, (unpublished).

[Su] M. Suzuki, *Group theory* II, Springer-Verlag, New York, 1986.

[W] R. Wiegand, *Picard groups of singular affine curves over a perfect field*, Math. Z. **200** (1989), 301–311.

[Z] K. Zsigmondy, *Zür Theorie der Potenzreste*, Monatsh. Math. **3** (1892), 265–284.

Department of Mathematics, University of Southern California, Los Angeles, California 90089-1113

Department of Mathematics, University of Nebraska, Lincoln, Nebraska 68588-0323