J. Austral. Math. Soc. (*Series A*) **29** (1980), 462–468

MAXIMAL SUBFIELDS OF ALGEBRAICALLY CLOSED FIELDS

ROBERT M. GURALNICK and MICHAEL D. MILLER

(Received 4 October 1978; revised 30 April 1979)

Communicated by D. E. Taylor

Abstract

Let K be an algebraically closed field of characteristic zero, and S a nonempty subset of K such that $S \cap Q = \varnothing$ and $\operatorname{card} S < \operatorname{card} K$, where Q is the field of rational numbers. By Zorn's Lemma, there exist subfields F of K which are maximal with respect to the property of being disjoint from S. This paper examines such subfields and investigates the Galois group $\operatorname{Gal} K/F$ along with the lattice of intermediate subfields.

1980 Mathematics subject classification (*Amer. Math. Soc.*): 12 F 05.

1.

Let K be an algebraically closed field of characteristic 0, and S a nonempty subset of K such that $S \cap Q = \varnothing$ and $\operatorname{card} S < \operatorname{card} K$, where Q is the field of rational numbers. A straightforward application of Zorn's Lemma shows that there exist subfields F of K which are maximal with respect to the property of being disjoint from S. In fact, we can even insist that F also contain any subset V of K as long as $S \cap Q(V) = \varnothing$. It is the purpose of this paper to study such subfields F, and to investigate the Galois group $\operatorname{Gal} K/F$ along with the lattice of intermediate subfields. In so doing, we generalize and simplify (in the characteristic 0 case) results of Quigley (1962) and McCarthy (1967), and obtain corrected versions of theorems appearing in Gordon and Straus (1965) and Krakowski (1976).

LEMMA 1. $\operatorname{card} F = \operatorname{card} K$.

PROOF. Clearly $\operatorname{card} F \leqslant \operatorname{card} K$, so assume $\operatorname{card} F < \operatorname{card} K$. If $T = \{\tau_\alpha, \alpha \in A\}$ is a transcendence base for K/F, then we must have $\operatorname{card} T = \operatorname{card} K$. The fields

$F(\tau_\alpha)$ intersect pairwise in F and each contains at least one element of S. This is a contradiction since card $S <$ card K, and the result follows.

THEOREM 1. *K is an algebraic extension of F.*

PROOF. Suppose not. Then there exists $x \in K$ such that x is transcendental over F. Consider the subfields $F(x^2+rx)$, $r \in F$. The element x^2+rx is fixed by the automorphism σ_r of $F(x)$ which sends x to $-x-r$. Hence, if $r \neq s$, any element in $F(x^2+rx) \cap F(x^2+sx)$ is fixed both by σ_r and σ_s. Let $f(x)/g(x)$ be any nonzero such element (where f and g are assumed relatively prime). Then we have

$$f(x)/g(x) = f(-x-r)/g(-x-r) = f(-x-s)/g(-x-s).$$

Set $y = -x-r$, so then

$$f(y)/g(y) = f(y+c)/g(y+c), \quad \text{where } c = r-s.$$

If f had a zero $\gamma \in K$, then $f(\gamma+nc) = 0$, $n = 0, 1, 2, 3, \ldots$. This forces f to be constant (since char $K = 0$). Similarly, g must be constant. Hence

$$F(x^2+rx) \cap F(x^2+sx) = F \quad \text{for all } r \neq s.$$

Since card F = card K, the result follows as in the proof of Lemma 1.

Since K/F is algebraic, it follows that every intermediate extension contains a minimal extension of F, each of which contains at least one element of S. It is thus no loss of generality to 'normalize' S and assume that there is a 1–1 correspondence $\alpha \rightarrow F(\alpha)$ between the elements $\alpha \in S$ and the minimal extensions $F(\alpha)$ of F.

An interesting question concerns the degree $[K:F]$. We first need two lemmas from group theory.

LEMMA 2. *Let G be a finite group and $\Phi(G)$ its Frattini subgroup. If $G/\Phi(G)$ can be generated by n elements, then so can G.*

PROOF. See Kurosh (1956), p. 217.

LEMMA 3. *If the group G is generated by n elements, then G has at most $(j!)^n$ subgroups of index j.*

PROOF. See Hall (1950).

THEOREM 2. *If S is finite, then either $[K:F] = 2$ or $[K:F] = \aleph_0$.*

PROOF. If $[K:F]$ is finite, then by the Artin–Schreier Theorem, $[K:F] = 2$. So assume that $[K:F]$ is infinite. It clearly suffices to show that F has only finitely many extensions of any given finite degree. Let L be any finite normal extension of F with $L \supseteq F(S)$, and set $\mathscr{G} = \operatorname{Gal} L/F$. Since $F(S)$ is the join of the minimal extensions of F, it corresponds (under the Galois correspondence) to the Frattini subgroup $\Phi(\mathscr{G})$, and $\mathscr{G}/\Phi(\mathscr{G}) \cong \operatorname{Gal} F(S)/F$. This latter group is finite, and hence can be generated by say n elements. By Lemmas 2 and 3, we conclude that $\mathscr{G}$ has at most $(j!)^n$ subgroups of index j for all j. Since L is arbitrary and every finite extension of F is contained in such an L, it follows by the Galois Correspondence Theorem that F has at most $(j!)^n$ extensions of degree j.

More generally, in the case when S is infinite, we can ask whether

$$[K:F] = \operatorname{card} S.$$

We do not know the answer even for the case $\operatorname{card} S = \aleph_0$.

For a given set S, we are interested in describing the lattice of subfields between F and K, and their respective Galois groups over F. In general, this problem is quite difficult—we shall solve it completely only in the case when $\operatorname{card} S \leqslant 2$, or when the degrees (over F) of the minimal extensions of F are distinct. We begin with a group-theoretical lemma.

LEMMA 4. *Let G be a finite group whose maximal subgroups have distinct indices $p_1, p_2, \ldots, p_k$. Then each p_i is prime and G is cyclic of order $p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, $e_i \geqslant 1$.*

PROOF. The proof is straightforward and follows immediately from results in Takeuchi (1968).

Suppose now that $S = \{\alpha\}$, so that $F(\alpha)$ is the unique minimal extension of F. Let $L \neq F$ be any finite normal extension of F. Then $F(\alpha) \subseteq L$, and $F(\alpha)$ corresponds to the unique maximal subgroup of $\mathscr{G} = \operatorname{Gal} L/F$. By Lemma 4, $\mathscr{G}$ is cyclic of order p^e, where $p = [F(\alpha):F]$ is prime. Moreover, for each integer f with $0 \leqslant f \leqslant e$, there exists a unique intermediate field E with $[E:F] = p^f$, whose Galois group $\operatorname{Gal} E/F$ is necessarily cyclic of order p^f. Since any finite extension of F is contained in such an L, it follows that every such extension is cyclic of degree p^d over F, and that there is at most one for each positive integer d.

Since the pth roots of 1 satisfy a polynomial of degree $p-1$ over F, it follows that F contains all such roots. Hence we can assume that $\alpha^p \in F$ (see Kaplansky (1969), Theorem 34). Using Theorem 51 in Kaplansky, we see that if p is odd and n is a positive integer, then $x^{p^n} - \alpha^p$ is irreducible over F and hence that $F(\alpha^{1/p^{n-1}})$ is the unique extension of F of degree p^n. Moreover, $\operatorname{Gal} K/F \cong \hat{Z}_p$ (the inverse limit of all cyclic p-groups). If $p = 2$ and $i \in F$, then $-4\alpha^2 = (2i\alpha)^2$ is not a fourth power in F and thus (by Theorem 51) results hold as in the case in which p is odd. If $i \notin F$, so that $F(\alpha) = F(i)$, then $i\alpha \in F$ and one of $\pm 2i\alpha$ is a square in F. Thus

$-4\alpha^2$ is a fourth power in F, so again by Theorem 51, $x^4-\alpha^2$ is not irreducible over F, so that $F(\alpha)=F(\sqrt{\alpha})$. If F is real closed, then $\operatorname{Gal} K/F \cong Z_2$. Otherwise, there is an element $\beta \notin F(i)$ with $\beta^2 \in F(i)$ such that $F(\beta^{1/2^{n-2}})$ is the unique extension of F of degree 2^n, $n \geqslant 2$.

The determination of $\operatorname{Gal} K/F$ even in the case $\operatorname{card} S=2$ is more difficult and requires the following discussion of Galois groups of algebraically closed fields.

2.

A group G is called *full* if it is the Galois group of some algebraically closed field K over a subfield F with K/F algebraic. Our objective is to classify full abelian groups, and thus obtain the corrected version of the last corollary in Krakowski (1976).

LEMMA 5. *Let R be a real field with unique ordering, and F a subfield such that R/F is normal algebraic. Then $F=R$.*

PROOF. Let σ be a nonidentity element of $\operatorname{Gal} R/F$. Choose $\alpha \in F$ such that $\sigma(\alpha)<\alpha$. By uniqueness of ordering, σ must preserve order, hence $\sigma^r(\alpha)<\alpha$ for all r. But as α is algebraic over F, it follows that $\sigma^n(\alpha)=\alpha$ for some $n>0$, a contradiction. Thus $\operatorname{Gal} R/F$ is trivial and $R=F$.

COROLLARY. *If a full group $G=\operatorname{Gal} \bar{F}/F$ contains a nontrivial torsion normal subgroup H, then $G \cong Z_2$.*

PROOF. By the Galois Correspondence and Artin–Schreier Theorems, it follows that $H \cong Z_2$. Since $H \trianglelefteq G$, its fixed field is a real closed normal extension of F. Since any real closed field has a unique ordering, this fixed field must be F. Hence $H=G$, and the result follows.

Since a real closed field R is of codimension 2 in its algebraic closure $\bar{R}$, it follows that $\operatorname{Gal} \bar{R}/R \cong Z_2$, so that indeed Z_2 does occur as a full group. In Krakowski (1976), it is stated that if G is full, then so is $G \times \prod_{\alpha \in A} \hat{Z}_{p_\alpha}$ for any index set A and corresponding primes p_α. We see in fact by the above corollary that this is false for $G=Z_2$. A closer examination of his proof reveals that what is actually shown is:

THEOREM 3. *If G is a full group, then there exists a full group H isomorphic to some semidirect product $\prod_{\alpha \in A} \hat{Z}_{p_\alpha} \times_s G$. This product can be taken to be direct if G is a full group over a field containing the cyclotomic field.*

Using this and completing the argument along the lines of that of Krakowski, we obtain the following classification of full abelian groups.

THEOREM 4. *An abelian group G is full if and only if either*

$$G \cong Z_2 \quad or \quad G \cong \prod_{\alpha\in A} \hat{Z}_{p_\alpha}$$

for some set of (not necessarily distinct) primes p_α and index set A.

We define the *degree set* of a field F to be the set of all degrees $[L:F]$ of finite extensions of F. In Gordon and Straus (1965), Theorem 13, it is stated that for any odd prime p, there exists a field F all of whose finite extensions are cyclic and whose degree set is $\{p^e, 2p^e: e = 0, 1, 2, \ldots\}$. This is incorrect, for otherwise $\operatorname{Gal} \bar{F}/F \cong Z_2 \times \hat{Z}_p$, contradicting Theorem 4. However, applying the construction in Krakowski (1976) used to prove our Theorem 3 with $G = Z_2$, we can show that if P is any set of primes, then there exists a field F with

$$\operatorname{Gal} \bar{F}/F \cong \prod_{p_\alpha\in P} \hat{Z}_{p_\alpha} x_s Z_2$$

(where the Z_2 factor acts on the direct product by inversion). It follows that the corresponding degree set is $\{2^\varepsilon p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k},\ \varepsilon = 0, 1;\ p_i \in P\}$. Clearly though, not every finite extension of F can be cyclic.

3.

If the subfield F of K is maximal with respect to the property of being disjoint from a subset $S \subseteq K$, it is in general quite difficult to determine the Galois group of K/F. In the special cases where card S is small, or the minimal extensions of F have distinct degrees over F, we can however make this determination.

THEOREM 5. *Suppose that distinct elements of S have distinct degrees over F. Then:*

(i) *Every finite extension of F is cyclic, and there is at most one of any given degree over F.*

(ii) *The minimal extensions of F all have prime degree over F.*

(iii) *Either* $\operatorname{Gal} K/F \cong Z_2$ *or* $\operatorname{Gal} K/F \cong \prod \hat{Z}_{p_\alpha}$, *where p_α runs through the degrees of the minimal extensions of F.*

PROOF. To prove (i), it suffices (as in the discussion following Lemma 4) to show that every finite normal extension L of F is cyclic. The minimal extensions $M_1, M_2, \ldots, M_k$ of F which are contained in such an L correspond to the maximal subgroups of $\mathscr{G} = \operatorname{Gal} L/F$. By Lemma 4, it follows that $\mathscr{G}$ is cyclic of order $p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, where $p_i = [M_i : F]$. Now (i) and (ii) follow. To prove (iii), we use

Theorem 4 and observe that Gal K/F is abelian since it is the inverse limit of the cyclic groups Gal L/F, where L runs through the finite normal extensions of F.

In case $S = \{\alpha\}$, we have already (in **1**) obtained the results of the theorem. Suppose now that $S = \{\alpha, \beta\}$, where S is assumed 'normalized' (see **1**) so that $F(\alpha) \cap F(\beta) = F$. The field $L = F(\alpha, \beta)$ is a normal extension of F (since it is generated by the two minimal extensions of F), and $\mathcal{G} = \mathrm{Gal}\, L/F$ contains exactly two maximal subgroups. It follows (see Takeuchi (1968)) that there exist distinct primes p and q such that $[F(\alpha) : F] = p$, $[F(\beta) : F] = q$, and $\mathcal{G} \cong Z_{pq}$. Using Theorem 5, we conclude that all finite extensions of F are cyclic, and that $\mathrm{Gal}\, K/F \cong \hat{Z}_p \times \hat{Z}_q$. The lattice of intermediate subfields is just the direct product of two countable chains.

To examine the case card $S = 3$, we need to consider finite groups having exactly three maximal subgroups. These have been classified by Takeuchi (1968) and are either cyclic of order $p_1^{e_1} p_2^{e_2} p_3^{e_3}$, where p_1, p_2, p_3 are distinct primes, or are non-cyclic 2-groups generated by two elements. If the three minimal extensions of F have distinct degrees over F, then Theorem 5 applies and we have $\mathrm{Gal}\, K/F \cong \hat{Z}_{p_1} \times \hat{Z}_{p_2} \times \hat{Z}_{p_3}$. Otherwise, each minimal extension has degree 2 over F. If $\mathcal{G} = \mathrm{Gal}\, K/F$ is abelian, then by Theorem 4, $\mathcal{G} \cong \hat{Z}_2 \times \hat{Z}_2$.

To see that Gal K/F can be nonabelian, we need only observe that the semi-direct product $\mathcal{G} = \hat{Z}_2 \, x_s Z_2$ (where the Z_2 factor acts on $\hat{Z}_2$ by inversion) contains exactly three maximal subgroups of finite index, and (as seen earlier) can arise as the Galois group Gal K/F, where (necessarily) F is maximal with respect to the avoidance of some three elements. The subgroup Z_2 of $\mathcal{G}$ corresponds to a real closed subfield R of K; hence F itself contains no nontrivial roots of unity.

There are even examples of subfields F of K with Gal K/F nonabelian such that F contains the cyclotomic field $\mathcal{A}$ and has exactly three minimal extensions. One such is provided by choosing $S = \{\sqrt[4]{2}, \sqrt[4]{3}, \sqrt[4]{6}\}$ and requiring that F contain $\sqrt[4]{3}\sqrt{(1-\sqrt{2})}$ in addition to $\mathcal{A}$.

Finally, it is worthwhile to note that if F is perfect of arbitrary characteristic, the results of this paper are essentially unchanged. Even if F is not perfect, the results of Section 1 remain valid (except for those involving discussion of Galois groups).

Acknowledgement

The authors wish to thank both referees for their helpful comments.

References

B. Gordon and E. G. Straus (1965), 'On the degrees of the finite extensions of a field', *Proc. Sympos. Pure Math.* **8** (Amer. Math. Soc., Providence, R.I.).

M. Hall (1950), 'A topology for free groups and related groups', *Ann. of Math.* **52**, 127–139.
I. Kaplansky (1969), *Fields and rings* (University of Chicago Press, Chicago).
D. Krakowski (1976), 'A note on Galois groups of algebraic closures', *J. Austral. Math. Soc. Ser. A* **21**, 12–15.
A. G. Kurosh (1956), *The theory of groups*, Vol. II (Chelsea Publishing Co., New York).
P. J. McCarthy (1967), 'Maximal fields disjoint from certain sets', *Proc. Amer. Math. Soc.* **18**, 347–351.
F. Quigley (1962), 'Maximal subfields of an algebraically closed field not containing a given element', *Proc. Amer. Math. Soc.* **13**, 562–566.
K. Takeuchi (1968), 'On Frattini subgroups', *TRU Math.* **4**, 10–13.

Department of Mathematics
University of California
Los Angeles, California
U.S.A.

https://doi.org/10.1017/S1446788700021625 Published online by Cambridge University Press