MAXIMAL FIELDS DISJOINT FROM CERTAIN SETS

P. J. MCCARTHY[1]

Suppose that C is an algebraically closed field and that Q is a subfield of C. If S is a nonempty subset of C disjoint from Q, it follows from an application of Zorn's lemma that there is a subfield k of C which is maximal with respect to the properties that $Q \subseteq k$ and k and S are disjoint. The problem is to describe the field extension C/k. When S consists of a single element this has been done by Quigley [**4**, Theorems 1, 2 and 3]. In this note we shall give several theorems which describe C/k when S consists of exactly two elements. When S contains more than two elements, some of the arguments used in the proof of Theorem 2 fail.

The first theorem holds when S is any finite (nonempty) subset of C disjoint from Q. It generalizes one of Quigley's results [**4**, Lemma 1].

THEOREM 1. *If S is a finite set then the extension C/k is algebraic.*

PROOF. If C/k is transcendental, and if t is an element of C which is transcendental over k, then $k(t)$ contains some element of S, say a_1. Then a_1 is transcendental over k, so $a_1 \notin k(a_1^2)$ and $k \neq k(a_1^2)$. Hence, $k(a_1^2)$ contains some element of S, say a_2, and $a_2 \neq a_1$. Then a_2 is transcendental over k, so $a_2 \notin k(a_2^2)$ and $k \neq k(a_2^2)$. Also, $a_1 \notin k(a_2^2)$ since $k(a_2^2) \subseteq k(a_1^2)$. We repeat this argument until S is exhausted. If a_n is the final element of S we have $k \neq k(a_n^2) \subseteq \cdots \subseteq k(a_2^2) \subseteq k(a_1^2)$ and $a_i \notin k(a_n^2)$ for $i = 1, \cdots, n$. This contradicts the defining property of k. Hence, C/k must be algebraic.

Henceforth, we assume that S consists of two distinct elements, a and b, of C. A finite extension K of k will be called *cyclic* if it is normal over k and if $G(K/k)$, the group of automorphisms of K which leave each element of k fixed, is cyclic. We do not require that K be separable over k.

THEOREM 2. *There are primes p and q (which may be equal) such that every finite extension of k in C is cyclic of degree $p^r q^s$ over k, for some integers r and s.*

We consider two cases. In the first case, we suppose that either $a \in k(b)$ or $b \in k(a)$: to be definite, assume the latter. If K is a proper extension of k in C then either $a \in K$ or $b \in K$, and so we always have

Received by the editors September 17, 1965.

[1] Research supported by NSF Grant GP1738.

$b \in K$. In Quigley's terminology, k is a maximal field without b. Thus, in this case, C/k is described by Quigley's results, and the result of the theorem holds.

From now on we shall assume that $a \notin k(b)$ and $b \notin k(a)$. We continue the proof of Theorem 2 with a series of lemmas, the first of which is given in [**4**].

LEMMA 1. *Let N be a finite normal separable extension of a field F. Let p be a prime divisor of $[N: F]$. Then there is a sequence of extensions $F \subseteq L_r \subset L_{r-1} \subset \cdots \subset L_0 = N$ such that for $i = 1, \cdots, r$, L_{i-1}/L_i is normal of degree p, and p does not divide $[L_r: F]$.*

LEMMA 2. *There are primes p and q such that $k(a)/k$ is normal of degree p and $k(b)/k$ is normal of degree q.*

PROOF. Assume that k is perfect. We show first that there is a normal extension of k in C which contains one of a and b but not the other. Assume this is not the case, and let N be the smallest normal extension of k in C which contains a. Then $b \in N$ and, in fact, N is the smallest normal extension of k in C which contains b. If we use Lemma 1 and the fact that $a \notin k(b)$ and $b \notin k(a)$, we conclude that $[k(a): k]$ and $[k(b): k]$ are relatively prime. Let p be a prime which divides $[k(a): k]$. Since p divides $[N: k]$ it follows from [**4**, Theorem 6] that there is a maximal subfield K of C without b, having exponent p, with $k \subseteq K$. Suppose $K \neq k$. Then $a \in K$ and so $k(a) \subseteq K$. By [**4**, Theorem 2], $[KN: K]$ is a power of p, and so the same is true of $[N: K \cap N]$ by the TNI (Theorem of Natural Irrationality [**1**, p. 149]). Note that $[N: K \cap N] \neq 1$ since $b \notin K$. If H is the subgroup of $G(N/k)$ having $K \cap N$ as its fixed field, then H is a p-subgroup of $G(N/k)$. Let F be the fixed field of the Sylow-p-subgroup of $G(N/k)$ which contains H. Then $F \subseteq K \cap N$. If $F = k$ then $[N: k]$ is a power of p, so p divides $[k(b): k]$, which is not true. Hence $F \neq k$, and since $b \notin F$ we have $k(a) \subseteq F$. But this cannot happen since p does not divide $[F: k]$. Thus, we are forced to conclude that $K = k$. Then, by [**4**, Theorem 2], $[k(b): k]$ is a power of p, again contrary to fact.

Thus, we may assume that there is a normal extension of k in C which contains a but not b. An application of Lemma 1 shows that $k(a)/k$ is normal of degree p. If $k(b)/k$ is not normal, there is a k-automorphism σ of C such that $k(\sigma(b)) \neq k(b)$. Then $b \notin k(\sigma(b))$ and so $k(a) \subseteq k(\sigma(b))$. If we apply σ^{-1} to $k(\sigma(b))$ and use the fact that $k(a)/k$ is normal, we get $a \in k(b)$, contrary to assumption. Thus, $k(b)/k$ is normal, and we can use Lemma 1 to show that $[k(b): k] = q$ for some prime q.

Now, assume that k is imperfect and let p be the characteristic of C. Let $c\in C$ be such that $c\notin k$ but $c^p\in k$. Then, $k(c)/k$ is purely inseparable of degree p and so contains exactly one of a and b, say a. Thus $k(a)/k$ is normal of degree p. By the argument used in the preceding paragraph we show that $k(b)/k$ is normal. If $k(b)/k$ is separable it follows from Lemma 1 that $[k(b): k]=q$ for some prime q. If $k(b)/k$ is inseparable, then $k(b^p)\neq k(b)$ [**1**, p. 130], and since $a\notin k(b^p)$ we must have $b^p\in k$. Then $k(b)/k$ is purely inseparable of degree p. Actually, this last situation cannot occur. For, if $k(a)/k$ and $k(b)/k$ are both purely inseparable of degree p, then so is $k(a+b)/k$ and so either $a\in k(a+b)$ or $b\in k(a+b)$. In the former case $b\in k(a)$, and in the latter $a\in k(b)$, contrary to assumption. This completes the proof of Lemma 2.

The following lemma is proved easily by induction.

LEMMA 3. *Let G be a group of order p^n, where p is a prime and $n\geqq 2$. If G has more than one subgroup of index p, then it has at least $p+1$ subgroups of index p.*

LEMMA 4. *If k is perfect then $p\neq q$.*

PROOF. Suppose $p=q$. We use Lemma 1, and the fact that $k(a)\neq k(b)$, to show that if N is the smallest normal extension of k in C which contains both a and b, then $[N: k]=p^n$ and $n\geqq 2$. Since $k(a)$ and $k(b)$ are the only subfields of N of degree p over k, $G(N/k)$ has exactly two subgroups of index p, which contradicts Lemma 3. Thus, $p\neq q$.

To complete the proof of Theorem 2 we show that every finite normal separable extension of k in C is cyclic of degree p^rq^s for some integers r and s. It follows from this, that for a given positive integer n, k has at most one separable extension of degree n in C. Hence, by [**2**, Theorem 9], every finite extension of k in C is cyclic. Since every finite extension of k in C has a degree over its separable part equal to some power of the characteristic of C, Theorem 2 will follow.

Let N be a finite normal separable extension of k in C. If k is imperfect we continue to assume a is inseparable over k. Then $a\notin N$, so $b\in N$ and it follows from Lemma 1 that $[N: k]$ is a power of $q=[k(b): k]$. Also, N has exactly one subfield, $k(b)$, of degree q over k. Hence, $G(N/k)$ is cyclic [**3**, Theorem 12.5.3].

Suppose that k is perfect. If N contains only one of a and b we repeat the above argument to show that N/k is cyclic of degree a power of p or a power of q. Assume N contains both a and b. Then $G=G(N/k)$ has exactly two maximal subgroups, one of index p and the other of index q (and $p \neq q$). These maximal subgroups are normal in G, since $k(a)/k$ and $k(b)/k$ are normal, and so G is nilpotent [**3**, Corollary 10.3.4]. Hence, G is the direct product of its Sylow subgroups [**3**, Theorem 10.3.4]. If G_p and G_q are the Sylow-p-subgroup and Sylow-q-subgroup of G, respectively, we see by Lemma 1 that $G = G_p \times G_q$. The fixed field of G_p contains exactly one subfield, $k(b)$, of degree q over k. Hence, G_q is cyclic. Similarly, G_p is cyclic. Hence, G is cyclic of degree $p^r q^s$ for some integers r and s. This completes the proof of Theorem 2.

Suppose k is perfect. Since $p \neq q$ we may assume $p \neq 2$. It follows from [**2**, Theorem 11] that for each integer $r \geqq 0$ there is an extension of k in C of degree p^r over k. Furthermore, it follows from what we have proved that there is only one such extension. Call it k_r. Then $k = k_0 \subset k_1 = k(a) \subset k_2 \subset \cdots$, and we let k_∞ be the union of the k_r. It follows that k_∞ is a maximal subfield of C without b. We have $k_r = \{c \mid c \in C \text{ and } [k(c)\colon k] = p^t \text{ for some } t \leqq r\}$. The structure of C/k_∞ is given by the first three theorems of [**4**].

Now, suppose that k is imperfect. As above, we take $k(a)/k$ to be purely inseparable and $k(b)/k$ to be separable. For each integer $r \geqq 0$ let $k_r = k(a^{p^{1-r}})$. Then $k = k_0 \subset k_1 = k(a) \subset k_2 \subset \cdots$ and $[k_r\colon k] = p^r$. Furthermore, $k_r = \{c \mid c \in C \text{ and } c^{p^r} \in k\}$. If k_∞ is the union of the k_r, then $k_\infty = k^{p^{-\infty}}$ [1, p. 128] and k_∞ is a maximal subfield of C without b. Again, the structure of C/k_∞ is given by theorems in [**4**].

In both the perfect and imperfect cases we set $K_r = \{c \mid c \in C,\ c \text{ is separable over } k, \text{ and } [k(c)\colon k] = q^t \text{ for some } t \leqq r\}$. Then K_r is a subfield of C and $K_r \subseteq K_{r+1}$ for all r. Let K_∞ be the union of the K_r. It may happen, when C has characteristic zero and $q = 2$, that $K_r = k(b)$ for all $r \geqq 1$. If this is not the case, then $K_r \subset K_{r+1}$ for all $r \geqq 0$.

We can now state the following theorem, which completes our description of C/k.

THEOREM 3. *Let L be an extension of k in C. Then, for some r and s, one or both of which may be infinity, we have $L = k_r K_s$. In this case, $[L\colon k] = p^r q^s$.*

PROOF. If k is perfect we set $E = \{c \mid c \in L \text{ and } [k(c)\colon k] \text{ is a power of } p\}$ and $F = \{c \mid c \in L \text{ and } [k(c)\colon k] \text{ is a power of } q\}$. If k is imperfect we let E be the fixed field of $G(L/k)$ and F be the separable part of L/k. In both cases, $E = k_r$ for some r, $F = K_s$ for some s, and $L = EF$.

Finally, we can use arguments similar to those used in the proofs of the last three theorems of [**4**] to obtain existence theorems for the various cases that have arisen.

References

1. N. Bourbaki, *Algèbre*, Chapters 4 and 5, Actualités Sci. Ind., No. 1102, Hermann, Paris, 1950.

2. Basil Gordon and E. G. Straus, *On the degrees of finite extensions of a field*, Proc. Sympos. Pure Math., Vol. 8, pp. 56–65, Amer. Math. Soc., Providence, R. I., 1965.

3. Marshall Hall, *The theory of groups*, Macmillan, New York, 1959.

4. Frank Quigley, *Maximal subfields of an algebraically closed field not containing a given element*, Proc. Amer. Math. Soc. **13** (1962), 562–566.

The University of Kansas