MAXIMAL SUBFIELDS OF AN ALGEBRAICALLY CLOSED FIELD NOT CONTAINING A GIVEN ELEMENT

FRANK QUIGLEY

If K is an algebraically closed extension of a field Q, and if $\alpha \in K$, $\alpha \notin Q$, then the set $\mathfrak{S}$ of all subfields of K not containing α is inductive when partially ordered by inclusion. A maximal element M of $\mathfrak{S}$ is by definition a *maximal field without* α. Such fields are thus characterized by the property that all their proper extensions (in K) contain α.

Theorems 1–3 describe the structure of K/M in detail, and Theorems 4–6, in view of this structure, give existence proofs more precise than that trivially given by Zorn's Lemma. The methods throughout are those of classical Galois theory; Lemma 2 (and possibly Lemma 4) are known, but, lacking suitable references, we give proofs of both.

All fields to be considered are subfields of K, and the characteristic of K is $q \geqq 0$.

LEMMA 1. *If M is maximal without α, then K is an algebraic extension of M.*

We observe first that α is algebraic over M; for if $\alpha^2 \notin M$, then $M(\alpha^2) \supset M(\alpha) \supset M(\alpha^2)$, so that α^2 is algebraic over M. Let $\overline{M}$ be the algebraic closure of M in K. If $\exists \eta \notin \overline{M}$, then η is transcendental over M, as is every element of $M(\eta)$ not in M. Since $M(\eta) \neq M$, it follows that $M(\eta) \supset M(\alpha)$; thus, since $\alpha \notin M$, it follows that α is transcendental over M; a contradiction.

THEOREM 1. *If M is maximal without α, then there exists a prime number p such that $[N: M]$ is a power of p for every finite normal extension N of M. Either M is a perfect field, or else K is a purely inseparable extension of M. Furthermore $[M(\alpha): M] = p$, and $M(\alpha)$ is a normal extension of M. All pth roots of unity lie in M, so that there exists $a \notin M(\alpha)$ such that $a^p \in M$ and $M(\alpha) = M(a)$, unless M is perfect and $p = q$.*

The proof is based on the following

LEMMA 2. *Let N be a finite normal separable extension of F and assume that p is a prime number such that $p^r \mid [N: F]$ but $p^{r+1} \nmid [N: F]$. Then there exist subfields L_i of N, $0 \leqq i \leqq r$, such that $L_i \supset L_{i+1} \supset F$, $[L_i: L_{i+1}] = p$, L_i/L_{i+1} is normal, $L_0 = N$, and $p \nmid [L_r: F]$.*

Under the hypotheses of the lemma, the Galois group of N/F has

Received by the editors July 10, 1961.

a Sylow-p^r-subgroup $\mathfrak{H}$, which has a composition series $\{\mathfrak{H}_i, 0 \leqq i \leqq r\}$ where $\mathfrak{H}_r = \mathfrak{H}$. The fixed fields L_i of $\mathfrak{H}_i$, $0 \leqq i \leqq r$, have the required properties.

To prove the theorem, assume that $b^q \in M$ but $b \notin M$; then $M(b) \supset M(\alpha)$ and $[M(b): M] = q$, so that $M(\alpha) = M(b)$, $p = q$, $\alpha^q \in M$, and $M(\alpha)$ is a purely inseparable extension of M. If $c \notin M$, then some power c^{q^t} is separable over M. Thus $c^{q^t} \in M$, for otherwise $M(c^{q^t}) \supset M(\alpha)$ and so is an inseparable extension of M.

Now suppose that M is perfect. Let p be a prime such that $p \mid [M(\alpha): M]$, and let N be a proper finite normal (hence separable) extension of M, so that $N \supset M(\alpha)$ and $p \mid [N: M]$. If p^r is the highest power of p dividing $[N: M]$, then, by the lemma with $M = F$, $\exists L_r \supset M$ with $[N: L_r] = p^r$. Thus $L_r = M$; for otherwise, $L_r \supset M(\alpha)$ and $p \mid [L_r: M]$. Also $\exists L_{r-1}$ such $N \supset L_{r-1} \supset L_r$, so that $[L_{r-1}: M] = p$. Since then $L_{r-1} \supset M(\alpha)$ and since $p \mid [M(\alpha): M]$, it follows that $M(\alpha) = L_{r-1}$, a normal extension of $L_r (= M)$ of degree p.

If $p \neq q$ and e is a primitive pth root of unity, then $[M(e): M] \leqq p-1$. Therefore $M(e) = M$; and since $M(\alpha)$ is a cyclic extension of M of degree p, $\exists a \in M(\alpha)$ such that $a^p \in M$ and $M(\alpha) = M(a)$.

We call the prime number p of Theorem 1 the *exponent* of the maximal field M without α.

THEOREM 2. *Let M be a maximal field without α of exponent p. For each positive integer r there is at most one extension M_r of M such that $[M_r: M] = p^r$. Such an M_r is generated over M by $\{\gamma: [M(\gamma): M] \leqq p^r\}$, and is a normal extension of M, cyclic if M is perfect and purely inseparable otherwise. Furthermore every extension $L \neq K$ of M equals some M_r.*

Assume first that M is perfect.

Let $[N_1: M] = [N_2: M] = p^r$, and let N be a finite normal extension of M containing N_1 and N_2. If $r = 1$, then $N_1 = M(\alpha) = N_2$. If $r > 1$, then the Galois group $\mathfrak{G}$ of N/M has order p^s, $s > 1$. Since $M(\alpha)$ is the only field between N and M of degree p, it follows that the p-group $\mathfrak{G}$ has only one subgroup of order p^{s-1}. Hence $\mathfrak{G}$ is cyclic [4, p. 119], and has precisely one subgroup of order p^r, $0 \leqq r \leqq s$. Thus N has only one subextension of degree p^r over M, and $N_1 = N_2$. Similarly, this unique (if it exists) extension M_r of degree p^r is a cyclic extension of M. Thus if $[M(\gamma): M] \leqq p^r$, then $\gamma \in M_r$, so that M_r is generated over M by $\{\gamma \ni: [M(\gamma): M] \leqq p^r\}$. Finally, let $L \neq K$ be any extension of M. Evidently $M_r \subset M_{r+1}$, and since K is algebraic over M, we have $K = \cup M_r$. If for every r, $\exists \gamma \in L \ni: [M(\gamma): M] \geqq p^r$, then $L \supset M_r$, for all r, and $L = K$; otherwise $L = M_r$, for some r.

Secondly assume that K/M is purely inseparable, so that $p=q$. Evidently $M_r=M^{q^{-r}}$, we prove that $M^{q^{-r}}=M(\alpha^{q^{1-r}})$, inductively. If $c^q\in M$, then either $c\in M$ or $M(c)=M(\alpha)$, and $M_1=M(\alpha)$. If $M_r=M(\alpha^{q^{1-r}})$ and $c^{q^{r+1}}\in M$, then $c^q\in M_r$, and so $c\in M_1(\alpha^{q^{-r}})=M_{r+1}$, Since $K=\cup M^{q^{-r}}$, each extension $L\neq K$ of M equals an M_r.

The preceding paragraph also establishes the following theorem in the case that K/M is purely inseparable.

THEOREM 3. *Let M be maximal without α, and, for each integer $r\geqq 1$, let M_r be generated over M by $\{\gamma\ni: [M(\gamma): M]\leqq p^r\}$. Then, either $\{M_r\}$ is a strictly increasing tower of proper subfields of K, or else $p=2$, $q=0$, and $M_1=M(-1^{1/2})=K$, so that M is a maximal orderable subfield of K. In the case that $M_1\neq K$, there exists $b\in M_1$ such that $M_r=M(b^{p^{1-r}})$ for all r, unless M is perfect and $p=q$.*

For the proof when M is perfect, we need the following

LEMMA 3. *Let M be maximal without α, and of exponent $p\neq q$. If $M(\alpha)=M(a)$ where $a^p\in M$, and if $a^{p^{-1}}\in M(a)$, then $M(a)=M(\epsilon)$, where ϵ is a primitive p^2-root of unity.*

Since, under the hypotheses, $M(a^{p^{-1}})=M(a)$, it follows that $a^{p^{-1}}$ is a zero of an irreducible polynomial $f(X)\in M[X]$ of degree p. It is also a zero of the polynomial $X^{p^2}-a^p\in M[X]$, a polynomial whose roots have the form $\epsilon a^{p^{-1}}$ where ϵ is a p^2-root of unity. Since $f(X)\mid X^{p^2}-a^p$, the roots of $f(X)$ have the form $\epsilon_i a^{p^{-1}}$, $1\leqq i\leqq p$, where $\epsilon_i^{p^2}=1$; hence $\epsilon_1\cdot\cdot\cdot\epsilon_p a\in M$, because the constant term of $f(X)$ is in M. Thus $a=\epsilon b$, where $b\in M$ and $\epsilon^{p^2}=1$. It follows that $M(a)=M(\epsilon b)=M(\epsilon)$.

Returning to Theorem 3, we observe by Theorem 2 that unless $[K: M]<\infty$, the tower $\{M_r\}$ is strictly increasing. If $[K: M]<\infty$, then by a theorem of Artin and Schreier [1; or 3, pp. 48–49], $p=2$, $K=M(-1^{1/2})$ etc. Now assume that $[K: M]=\infty$, $p\neq q$, and that $M(\alpha)=M(a)$, where $a^p\in M$, by Theorem 1. There are two cases.

If $a^{p^{-1}}\notin M_1$ $(=M(a))$, then $M_2=M_1(a^{p^{-1}})$. Let ϵ be a primitive p^2-root of unity; then $[M(\epsilon): M]\leqq p$, since $\epsilon^p\in M$ by Theorem 1. Thus $\epsilon\in M_1$. But M_1 is maximal without $a^{p^{-1}}$, and it follows that $a^{p^{-2}}\notin M_2$; for otherwise, by Lemma 3, $M_2=M_1(a^{p^{-1}})=M_1(\epsilon)=M_1$, which is a contradiction. Continuing inductively, we find that in this case we may take $b=a$.

On the other hand, if $a^{p^{-1}}\in M_1$, then, by Lemma 3, $M_1=M(a)=M(\epsilon)$. Now $\exists b\in M(\epsilon)\ni: b^{p^{-1}}\notin M(\epsilon)$, and such an element b is not in M; for otherwise $[M(b^{p^{-1}}): M(b)]=[M(b^{p^{-1}}): M]=p$, and $b^{p^{-1}}\in M(\epsilon)$. Thus $M(a)\supset M(b)\neq M$, and $M(\epsilon)=M(b)$. But M_1 is now maximal without $b^{p^{-1}}$ and $(b^{p^{-1}})^p\in M_1$. If $b^{p^{-1}}\in M_1(b^{p^{-1}})$, then

$M_1(b^{p^{-1}}) = M_1(\epsilon) = M_1$, which is false. Hence $b^{p^{-2}} \notin M_1(b^{p^{-1}})$, and we continue the argument as in the first case.

In the proofs which follow, the "Theorem of natural irrationality" [2, p. 149] is called (TNI), and Q is any subfield of K.

THEOREM 4. *If α is transcendental over Q, and if p is a prime number, then there exists a maximal $M \supset Q$ without α of exponent p. When $p = q$, both perfect and imperfect M exist.*

Let $\{\beta\} \cup \{t_\mu,\ \mu \in I\}$ be a transcendence basis of K/Q, where $\beta = \alpha^p$, or where $\beta = \alpha^q - \alpha$ and $p = q$. Let e be a primitive pth root of unity, and let $L = Q(e, \beta, \{t_\mu\})$. Then $\alpha \notin L$, and L has an extension M which is maximal without α. Also $L(\alpha)$ is a normal extension of L of degree p [1; or 2, p. 177]. Since $\alpha \notin M$, it follows that $L(\alpha) \cap M \neq L(\alpha)$; thus $L(\alpha) \cap M = L$, and, if M is perfect, by (TNI), $[L(\alpha): L] = [M(\alpha): M] = p$. If M is imperfect, so that $p = q$, then $\alpha^p \in M$ but $\alpha \notin M$, and again $[M(\alpha): M] = p$.

THEOREM 5. *Let α be algebraic $\{$separably algebraic$\}$ over Q, and let p be a prime. If there exists a maximal $M \supset Q$ without α of exponent p, then there exists a finite algebraic extension F of Q such that $F(\alpha)$ is a normal $\{$normal separable$\}$ extension of F of degree p. On the other hand, if there exists any field F such that $F(\alpha)/F$ is normal and $p \mid [F(\alpha): F]$, then there exists a maximal M without α of exponent p. If E is the fixed field of the automorphism group of $F(\alpha)/F$, and if $p \mid [F(\alpha): E]$, then a perfect M exists; if $p \mid [E: F]$, then an imperfect M exists.*

If M exists and is imperfect, let $F = Q(\alpha^q)$. If M exists and is perfect, let $\mathfrak{M}$ be the Galois group of $M(\alpha)/M$. Let N be generated over Q by $\{\alpha^\sigma,\ \sigma \in \mathfrak{M}\}$, and let $\mathfrak{G}$ be the automorphism group of N/Q. If E is the fixed field of $\mathfrak{G}$, then $\mathfrak{G}$ is the Galois group of N/E, which is a normal separable extension. Now $N \subset M(\alpha)$, and $M(N) = M(\alpha)$, since $\alpha \in N$. If $F = M \cap N$, then, by (TNI), $[N: F] = [M(\alpha): M] = p$. Finally, $N = F(\alpha)$, since $\alpha \notin F$.

For the second part, suppose $\exists F$ such that $F(\alpha)/F$ is normal and $p^r \mid [F(\alpha): E]$ but $p^{r+1} \nmid [F(\alpha): E]$, where E is the fixed field of the automorphism group of $F(\alpha)/F$. If $E \neq F(\alpha)$, then, by Lemma 2, there exists L_1 such that $F(\alpha) \supset L_1 \supset E$ and $[F(\alpha): L_1] = p$, normal. Since $\alpha \notin L_1$, there exists a maximal M without α containing L_1. But then $M \cap F(\alpha) = L_1$, $M(F(\alpha)) = M(\alpha)$, and $p = [F(\alpha): L_1] = [M(\alpha): M]$. If $p = q$ and $E \neq F$, then α is inseparable over F and $[F(\alpha): F(\alpha^q)] = q$. Imbed $F(\alpha^q)$ in a maximal M without α; then $[M(\alpha): M] = q$, since $\alpha^q \in M$ but $\alpha \notin M$.

THEOREM 6. *If α is algebraic over Q and p is a prime, let N be the*

least normal extension of Q containing α. Then there exists a maximal $M \supset Q$ without α of exponent p if and only if $p \mid [N: Q]$.

This follows at once from Theorem 5 and the following

LEMMA 4. *Let α be algebraic over Q, and let N be the least normal extension of Q containing α. If p is a prime, then there exists a field $F \supset Q$ such that $F(\alpha)/F$ is a normal extension of degree p if and only if $p \mid [N: Q]$.*

If $\exists F \ni : F(\alpha)/F$ is normal and separable of degree p, then, by (TNI), the Galois groups of $N/N \cap F$ and $N(F)/F$ are naturally isomorphic, and $N(F) \supset F(\alpha) \supset F$. Let $\mathfrak{H}$ comprise all automorphisms of $N(F)$ leaving $F(\alpha)$ fixed, and let $\mathfrak{H}'$ be the restriction to N of the automorphisms in $\mathfrak{H}$. The fixed field of $\mathfrak{H}'$ is $(N \cap F)(\alpha)$, and $[(N \cap F)(\alpha): N \cap F] = [F(\alpha): F] = p$. Thus $p \mid [N: Q]$. If $F(\alpha)/F$ is inseparable, then $p = q$ and $\alpha^q \in F$. Since $\alpha \notin F$, it follows that $\alpha \notin Q(\alpha^q) \subset F$; thus $[Q(\alpha): Q(\alpha^q)] = q$ and $q \mid [N: Q]$.

Conversely, assume that $p \mid [N: Q]$, and let $\mathfrak{G}$ be the automorphism group of N/Q. Let E be the fixed field of $\mathfrak{G}$. If $p \nmid [N: E]$, then $p \mid [E: Q]$, $p = q$, and we may take $F = Q(\alpha^q)$. If $p \mid [N: E]$, let $\mathfrak{H}_1, \cdots, \mathfrak{H}_s$ be all the Sylow p-subgroups of $\mathfrak{G}$, and let $\mathfrak{H}$ be the group which they generate. Since the $\mathfrak{H}_i$ are a complete set of conjugate subgroups of any one of them, $\mathfrak{H}$ is a normal subgroup of $\mathfrak{G}$. Let F_0 be the fixed field of $\mathfrak{H}$, and F_i the fixed field of $\mathfrak{H}_i$; then $F_0 = \bigcap_1^s F_i$. We observe that $\alpha \notin F_0$. For otherwise, since F_0/E is normal and $N \supset F_0$, it follows that $F_0 = N$, and $\mathfrak{H}$ contains only the identity, which is false. Thus $\alpha \notin F_{i_0}$ for some $i_0 \geqq 1$. If p^r is the order of $\mathfrak{H}_{i_0}$, then p^{r+1} does not divide the order of $\mathfrak{G}$, since $\mathfrak{H}_{i_0}$ is a Sylow p-group, so that $p^{r+1} \nmid [N: E]$ and $[N: F_{i_0}] = p^r$. Hence $[F_{i_0}(\alpha): F_{i_0}] = p^t$, $1 \leqq t \leqq r$. If G is the subgroup of $\mathfrak{G}$ leaving $F_{i_0}(\alpha)$ fixed, then $G (\subset \mathfrak{H}_{i_0})$ is a p-group, so $\exists G' \ni : G \subset G' \subset \mathfrak{H}_{i_0}$, $(G': G) = p$, and G is a normal subgroup of G'. Let F be the fixed field of G'; then $[F_{i_0}(\alpha): F] = (G': G) = p$, and $F_{i_0}(\alpha)/F$ is normal. Finally $F_{i_0}(\alpha) \supset F(\alpha)$, but $F(\alpha) \neq F$, since $\alpha \notin F$; thus $F_{i_0}(\alpha) = F(\alpha)$.

REFERENCES

1. E. Artin and O. Schreier, *Eine Kennzeichnung der reell abgeschlossenen Körper*, Abh. Math. Sem. Univ. Hamburg **5** (1927), 225–231.

2. N. Bourbaki, *Algèbre*, Ch. 5, Actualités Sci. Ind., no. 1102, Hermann, Paris, 1950.

3. ———, *Algèbre*, Ch. 6, Actualités Sci. Ind., no. 1179, Hermann, Paris, 1952.

4. H. Zassenhaus, *The theory of groups*, Chelsea, New York, 1949.

TULANE UNIVERSITY