

# Pacific Journal of Mathematics

**JÓNSSON  $\omega_0$ -GENERATED ALGEBRAIC FIELD EXTENSIONS**

ROBERT WILLIAM GILMER, JR. AND WILLIAM JAMES HEINZER

## JÓNSSON $\omega_0$ -GENERATED ALGEBRAIC FIELD EXTENSIONS

ROBERT GILMER AND WILLIAM HEINZER

A field  $K$  algebraic over its subfield  $F$  is said to be a  $J$ -extension (for Jónsson  $\omega_0$ -generated extension) of  $F$  if  $K/F$  is not finitely generated, but  $E/F$  is finitely generated for each proper intermediate field  $E$ . We seek to determine the structure of a given  $J$ -extension and to determine the class of fields that admit a  $J$ -extension. Consideration of Galois  $J$ -extensions plays a special role in each of these problems. In §2, we show that a Galois extension  $K/F$  is a  $J$ -extension if and only if  $\text{Gal}(K/F) \simeq \varprojlim Z/p^n Z$  for some prime  $p$ . In §3, we show that  $F$  admits a  $J$ -extension if the algebraic closure of  $F$  is infinite over  $F$ —that is,  $F$  is neither algebraically closed nor real closed.

**1. Introduction.** Assume that  $\alpha$  is an infinite cardinal. In universal algebra, an algebra  $A$  is said to be a *Jónsson  $\alpha$ -algebra* if  $|A| = \alpha$  while  $|B| < \alpha$  for each proper subalgebra  $B$  of  $A$  [CK, p. 469]. This terminology has been extended in [GH] to generating sets, as follows. The algebra  $A$  is said to be a *Jónsson  $\alpha$ -generated algebra* if  $A$  has a generating set of cardinality  $\alpha$ , no generating set of smaller cardinality, and each proper subalgebra  $B$  of  $A$  has a generating set of cardinality less than  $\alpha$ . In considering these concepts, special attention has been given to the cases where  $\alpha = \omega_0$ , the first infinite cardinal, and where  $\alpha = \omega_1$ , the first uncountable cardinal. For  $\alpha = \omega_0$ , we consider here a problem of this type for field extensions. Specifically, suppose that  $F$  is a subfield of the field  $K$ . Shortening the phrase “ $K$  is a Jónsson  $\omega_0$ -generated  $F$ -algebra”, we say that  $K$  is a  *$J$ -extension of  $F$*  if  $[K:F] = \infty$  while  $[E:F] < \infty$  for each proper intermediate field  $E$ . The condition that  $[E:F] < \infty$  for each proper intermediate field implies that  $K/F$  is countably generated, so in fact,  $[K:F] = \omega_0$  if  $K$  is a  $J$ -extension of  $F$ . We begin by noting three examples of  $J$ -extension; these are labelled below as (E1), (E2), and (E3).

(E1) An absolutely algebraic field  $F$  of characteristic  $p \neq 0$  is uniquely determined, up to isomorphism, by specifying its Steinitz number, a formal product  $N = \prod p_i^{k_i}$  over all primes  $p_i$ , where  $k_i \in \mathbb{Z}_0 \cup \{\infty\}$  for each  $i$  [J, p. 147]. If  $F$  is not algebraically closed, then  $k_t \neq \infty$  for some  $t$ . If  $K$  is the absolutely algebraic extension field of  $F$  with Steinitz number  $\prod p_i^{h_i}$ , where  $h_t = \infty$  and  $h_i = k_i$  for  $i \neq t$ , then  $K$  is a  $J$ -extension of  $F$ ;

the proper intermediate fields, in this case, are the fields corresponding to the Steinitz numbers  $\prod p_i^{v_i}$ , where  $v_i \in \mathbb{Z}_0$ ,  $v_i \geq k_i$ , and  $v_i = k_i$  for  $i \neq t$ .

(E2) If  $F$  is an imperfect field of characteristic  $p \neq 0$  and if  $s \in F \setminus F^p$ , then  $K = F(\{s^{1/p^n}\}_{n=1}^\infty)$  is a  $J$ -extension of  $F$ . The proper intermediate fields are the fields  $F(s^{1/p^n})$ , where  $n \in \mathbb{Z}_0$  (see Lemma 2.8).

(E3) Assume that the field  $E$  is not algebraically closed and let  $K$  be an algebraic closure of  $E$ . Choose  $s \in K \setminus E$  and let  $F$  be an intermediate field maximal with respect to failure to contain  $s$ . If  $[K:F] = \infty$ , then  $K$  is a  $J$ -extension of  $F$ ; the set of proper intermediate fields forms a chain  $F = F_0 < F_1 < F_2 < \cdots$ , where  $[F_n:F] = q^n$ , with  $q$  prime, for each  $n \in \mathbb{Z}^+ [Q]$ .

In each of the examples above, the set of fields between  $F$  and  $K$  is linearly ordered, and given adjacent intermediate fields  $E_1 < E_2$ ,  $[E_2:E_1]$  is a prime integer independent of  $E_1$  and  $E_2$ . While examples of this type are the easiest to produce, we subsequently show (Examples 2.11, 2.18) that there are other examples of  $J$ -extensions with neither of the properties cited. On the other hand, Theorem 2.5 shows that if  $K/F$  is Galois, then the two conditions are satisfied. There are two primary emphases of this paper, as follows: (1) to determine possible structures of a  $J$ -extension (§2), and (2) to determine the class of fields that admit a  $J$ -extension or a Galois  $J$ -extension (§3). The structure of a Galois  $J$ -extension is completely determined in Theorem 2.5, but subsequent examples in §2 show that a variety of structures are possible in the non-Galois case.

Suppose  $F$  is a field that is neither algebraically closed nor real closed. In §3, we initially investigate the question of whether  $F$  admits a Galois  $J$ -extension if  $F$  admits a nontrivial cyclic extension. We observe that the answer is negative in general for a cyclic extension of degree two, but in many other cases we obtain an affirmative answer. We subsequently show (Theorem 3.9) that  $F$  admits a  $J$ -extension if  $F$  is neither algebraically closed nor real closed. If  $F$  is the quotient field of a non-trivial valuation domain with principal maximal ideal, we present in Theorem 3.11 a concrete construction of a  $J$ -extension of  $F$ .

In §4, we show that each subfield of  $A$ , the abelian closure of  $Q$ , admits a Galois  $J$ -extension. The final section of the paper contains comments on two open questions that merit, in our opinion, further consideration.

**2. Structure of  $J$ -extensions.** Suppose  $K$  is a  $J$ -extension of  $F$ . In this section we focus on the lattice  $\mathcal{S}$  of intermediate fields. In particular, we consider two questions concerning  $\mathcal{S}$  that have been mentioned in the introduction: (1) Is  $\mathcal{S}$  linearly ordered under inclusion? (2) What possibil-

ities exist for the set  $\{[E_2:E_1]\}$  as  $E_1 < E_2$  ranges over all adjacent elements of  $\mathcal{S}$ ? Theorem 2.5 shows that if  $K/F$  is Galois, then (1) has an affirmative answer, and in (2),  $[E_2:E_1]$  is a prime integer independent of  $E_1$  and  $E_2$ . We begin the section with a general result concerning  $J$ -extensions; the proof of Proposition 2.1 is routine, and hence is omitted.

**PROPOSITION 2.1.** *Assume that  $F$  is a subfield of the field  $K$ .*

(1) *If  $K$  is a  $J$ -extension of  $F$ , then  $K$  is the union of a strictly ascending sequence of intermediate fields. In fact, if  $\{K_i\}_{i=1}^\infty$  is any strictly ascending sequence of intermediate fields, then  $K = \bigcup_{i=1}^\infty K_i$ .*

(2) *Suppose  $K$  is expressed as the union of a strictly ascending sequence  $\{K_i\}_{i=1}^\infty$  of intermediate fields, where  $[K_i:F] < \infty$  for each  $i$ . The following conditions are equivalent.*

- (a)  *$K$  is a  $J$ -extension of  $F$ .*
- (b) *Each proper intermediate field is contained in some  $K_i$ .*
- (c) *If  $x_i \in K \setminus K_i$  for each  $i$ , then  $K = F(\{x_i\}_{i=1}^\infty)$ .*

**COROLLARY 2.2.** *Assume that  $K$  is an extension field of the field  $F$  and that  $K$  is expressed as the union of a strictly ascending sequence  $\{K_i\}_{i=1}^\infty$  of intermediate fields, where  $[K_i:F] < \infty$  for each  $i$ . If for each  $i$  the set of subfields of  $K_i$  containing  $F$  is linearly ordered under inclusion, then  $K$  is a  $J$ -extension of  $F$ .*

**COROLLARY 2.3.** *Assume that  $F$  is a field of characteristic  $p \neq 0$ . Let  $M$  be an extension field of  $F$  and let  $K, L$  be intermediate fields with  $K/F$  purely inseparable and  $L/F$  a separable  $J$ -extension. Then  $KL$  is a  $J$ -extension of  $K$ .*

*Proof.* According to Proposition 2.1, there exists an ascending sequence  $F = L_0 < L_1 < \dots < L = \bigcup_{i=0}^\infty L_i$  of finite extensions of  $F$  with the property that if  $x_i \in L \setminus L_i$  for each  $i$ , then  $L = F(\{x_i\}_0^\infty)$ . We show that the sequence  $\{KL\}_{i=0}^\infty$  of fields between  $K$  and  $KL$  has the same properties; this suffices to show that  $KL$  is a  $J$ -extension of  $K$ . Since  $K$  and  $L_i$  are linearly disjoint over  $F$ , we have  $[KL_i:K] = [L_i:F] < \infty$ . Hence  $K = KL_0 < KL_1 < \dots < KL = \bigcup_0^\infty KL_i$ . Take  $y_i \in KL \setminus KL_i$  for each  $i$ . There exists a finite extension  $E_i$  of  $F$  in  $K$  so that  $y_i \in E_i L$ , and if  $E_i$  has exponent  $e_i$  over  $F$ , then  $y_i^{p^{e_i}} \in FL = L$ . Since  $KL$  is separable over  $K \subseteq KL_i$ , it is also true that  $y_i^{p^{e_i}} \notin KL_i$ , and hence  $y_i^{p^{e_i}} \notin L_i$ . By hypothesis we have  $F(\{y_i^{p^{e_i}}\}) = L$ , so  $K(\{y_i\}_i^\infty) \supseteq K(\{y_i^{p^{e_i}}\}) \supseteq L$ , and hence  $K(\{y_i\}) = KL$ .

Can the roles of “separable” and “purely inseparable” be interchanged in Corollary 2.3? We have been unable to answer this question. If  $K/F$  is separable and  $L/F$  is a *standard* purely inseparable  $J$ -extension, as defined in the paragraph preceding the statement of Proposition 2.19, then it is easily seen that  $KL/K$  is a standard purely inseparable  $J$ -extension.

Suppose  $K$  is a Galois extension of the field  $F$ . Our determination of equivalent conditions for  $K$  to be a  $J$ -extension of  $F$  uses properties of the group  $\varprojlim Z/p^n Z$ , where  $p \in Z^+$  is prime. We denote this group by  $W_p$ . Much is known about the structure of  $W_p$ ; we list below some of the properties of  $W_p$  that we use.<sup>1</sup>

(W1)  $W_p$  is isomorphic to the additive group of the ring  $Q_p$  of  $p$ -adic integers [F, p. 62]; also  $W_p \simeq \text{End } Z(p^\infty)$ , the endomorphism group of the  $p$ -quasicyclic group  $Z(p^\infty)$  [F, p. 181].

(W2)  $W_p$  is  $q$ -divisible for each prime  $q \neq p$  [Wn, p. 174]; hence  $\{nW_p \mid n \in Z^+\} = \{p^k W_p\}_{k=0}^\infty$ .

(W3)  $W_p/p^k W_p \simeq Z/p^k Z$  for each  $k$  [F, p. 19]. Hence  $\{p^i W_p\}_{i=0}^k$  is the set of subgroups of  $W_p$  containing  $p^k W_p$ .

(W4)  $W_p$  is torsion-free [Wn, p. 174], so  $W_p \simeq p^k W_p$  for each  $k \in Z^+$ .

(W5) If  $H$  is a subgroup of  $W_p$  of finite index, then  $H \simeq W_p$ ; this follows from (W2), (W3), and (W4).

(W6) Considering  $W_p$  as the additive group of  $Q_p$ , each endomorphism of  $W_p$  is multiplication by a fixed element of  $Q_p$  [F, p. 181]. Each automorphism of  $W_p$  is multiplication by a unit of  $Q_p$ .

The proof of Theorem 2.5 uses one new result concerning the group  $W_p$ ; this result is established in Theorem 2.4. We are indebted to Murad Özaydın for the proof of Theorem 2.4.

**THEOREM 2.4.** *Assume that  $G$  is a torsion-free group containing  $W_p$  as a subgroup of finite index. Then  $G \simeq W_p$ .*

*Proof.* Because  $G$  is not assumed to be abelian, we write the group operation in  $G$  as multiplication. However, we consider  $W_p$  as the additive group of  $Q_p$ , and hence we write the group operation within  $W_p$  as addition. It turns out that no confusion results from this dichotomy of notation.

<sup>1</sup>Fuchs [F] and Weinsten [Wn] denote this group by  $J_p$ . In class field theory, the notation  $Z_p$  is frequently used, and a Galois extension of  $K$  with Galois group  $Z_p$  is called a  $Z_p$ -extension of  $K$  [I], [Wa].

Since  $[G:W_p] = s$  is finite,  $W_p$  contains a normal subgroup  $H$  of  $G$  with  $[G:H]$  finite. (W5) shows that  $H \simeq W_p$ , so we assume without loss of generality that  $W_p$  is normal in  $G$ . Thus, if  $g \in G$ , then conjugation by  $g$  induces an automorphism  $\varphi_g$  of  $W_p$ ; (W6) shows that  $\varphi_g$  is multiplication by a unit  $u$  of the ring  $Q_p$ —that is,  $\varphi_g(x) = ux$  for each  $x \in W_p$ . Since  $[G:W_p] = s < \infty$ , then  $g^s \in W_p$ , so  $ug^s = \varphi_g(g^s) = gg^s g^{-1} = g^s$ . Since  $G$  is torsion-free,  $g^s \neq 0$  and we conclude that  $u = 1$ . Therefore  $\varphi_g = 1$  and  $g$  commutes with each element of  $W_p$ . We conclude that  $W_p$  is contained in the center of  $G$ ; this implies that the transfer  $\tau: G \rightarrow W_p$  is a group homomorphism that is the  $s$ th power map:  $\tau(g) = g^s$  for each  $g \in G$  [Ro, p. 155]. Because  $G$  is torsion-free,  $\tau$  is injective and  $W_p \supseteq \tau(G) \supseteq sW_p$ . From (W2), (W3) and (W4), it then follows that  $G \simeq \tau(G) \simeq W_p$ . This completes the proof.

**THEOREM 2.5.** *Assume that  $K$  is an algebraic extension of the field  $F$  and that  $K/F$  is Galois.*

- (1) *If  $K$  is a J-extension of  $F$ , then  $\text{Gal}(K/F) = W_p$  for some prime  $p$ .*
- (2) *Conversely, assume that  $\text{Gal}(K/F) \simeq W_p$ . Then for each  $n \in \mathbb{Z}_0$  there exist a unique intermediate field  $K_n$  with  $[K_n:F] = p^n$ ;  $\{K_n\}_{n=0}^\infty$  is the set of proper intermediate fields.  $K_n/F$  is cyclic and  $K_n \subseteq K_{n+1}$  for each  $n$ . In particular,  $K$  is a J-extension of  $F$ .*

*Proof.* (1): Set  $G = \text{Gal}(K/F)$ . Choose  $x \in K \setminus F$  and let  $E$  be an intermediate field maximal with respect to failure to contain  $x$ . Let  $L$  be any proper finite extension of  $E$  in  $K$  and let  $M$  be the normal closure in  $K$  of  $L/E$ . Because  $E(x)$  is the unique minimal proper extension of  $E$  in  $M$ , the Galois group  $H$  of  $M/E$  has a unique maximal subgroup. Consequently,  $H$  is cyclic of prime-power order  $p^n$  for some prime  $p$ . Because each subgroup of  $G$  is normal in  $G$ , each field between  $E$  and  $M$  is normal over  $E$ . In particular,  $L$  is normal over  $E$  and  $L = M$ . If  $L_1$  and  $L_2$  are distinct finite proper extensions of  $E$  in  $K$  of degrees  $p_1^a$  and  $p_2^b$ , respectively, over  $E$ , then  $p_1 = p_2$  since  $[L_1 L_2 : E]$  is also a prime power. We denote by  $p$  this prime integer associated with  $E$ . Since  $K$  is the union of a chain of extension fields  $E_n$  of  $E$  such that  $E_n$  is cyclic over  $E$  of degree  $p^n$  for each  $n \in \mathbb{Z}^+$ , it follows that the Galois group of  $K$  over  $E$  is isomorphic to  $\varprojlim \mathbb{Z}/p^n \mathbb{Z} = W_p$  [Bol, Prop. 8, p. V. 61], [L, p. 351]. Because  $[E:F] < \infty$ , the index of  $W_p$  in  $G$  is at most  $[E:F]$  [H, Lemma 2.8, p. 247]. Moreover,  $G$  is torsion-free since no proper intermediate field has finite codimension in  $K$  [H, Lemma 2.10, p. 249]. Therefore Theorem 2.4 shows that  $G \simeq W_p$ .

(2): We assume that  $\text{Gal}(K/F) \simeq W_p$ . Then  $K$  is not a finite extension of  $F$ . Let  $P$  be any finite extension of  $F$  in  $K$  and let  $H = \text{Gal}(K/P)$ . Since  $G$  is Abelian,  $H$  is normal in  $G$ , so  $P$  is normal over  $F$ . The group  $G/H \simeq \text{Gal}(P/F)$  is finite so  $H \supseteq p^k G$  for some  $k$  and  $G/H$  is a homomorphic image of  $G/p^k G \simeq Z/p^k Z$ . Therefore  $G/H$  is cyclic, and we have proved that  $P/F$  is cyclic of degree  $p^m$  for some  $m \in Z_0$ . Because  $K/F$  is not finite-dimensional, the set of degrees of finite extensions of  $F$  in  $K$  is unbounded, and hence for arbitrarily large integers  $n \in Z^+$ , there exists an intermediate field  $K_n$  of degree  $p^n$  over  $F$ . Moreover, since  $K_n/F$  is cyclic, there exists an intermediate field  $K_i$  of degree  $p^i$  over  $F$  for  $0 \leq i \leq n$ . Thus, there exists an intermediate field  $K_n$  of degree  $p^n$  over  $F$  for each  $n \in Z^+$ . If  $E$  is an intermediate field of degree  $p^n$  over  $F$ , then  $EK_n$  is cyclic over  $F$  of degree  $p^r$  for some  $r \geq n$ ; since  $\text{Gal}(EK_n/F)$  admits a unique subgroup of index  $p^n$ , it follows that  $E = K_n$ . To complete the proof, we show that  $K = \bigcup_{n=0}^{\infty} K_n$  and that  $K$  is the only intermediate field distinct from each  $K_n$ . Thus, if  $y \in K$ , then  $[F(y):F] = p^r$  for some  $r$ , so  $F(y) = K_r$  and  $y \in \bigcup_0^{\infty} K_n$ . This proves that  $K = \bigcup_0^{\infty} K_n$ . If  $E \neq K_n$  for  $n \in Z^+$ , then choose  $y_n \in E \setminus K_n$ . We have  $E \supseteq F(y_n) \supseteq K_n$ . Therefore if  $E \notin \{K_n\}_0^{\infty}$ , then  $E \supseteq \bigcup_0^{\infty} K_n = K$  so  $E = K$  and this completes the proof of (2).

**COROLLARY 2.6.** *Assume that  $K$  and  $L$  are subfields of a field  $M$ , that  $F$  is a subfield of  $K \cap L$ , and that  $K$  is a Galois  $J$ -extension of  $F$ . If  $L \not\subseteq K$ , then  $LK$  is a Galois  $J$ -extension of  $L$ .*

*Proof.* The proof of Theorem 2.5 shows that  $K$  is expressible as the union of a strictly ascending sequence  $\{K_i\}_{i=1}^{\infty}$  of intermediate fields such that  $K_i/F$  is cyclic of degree  $p^i$  for each  $i$ , where  $p$  is a fixed prime depending only upon  $K$  and  $F$ . We have  $L \cap K = L \cap (\bigcup K_i) = \bigcup_{i=1}^{\infty} (L \cap K_i) < K$ . Hence  $L \cap K = K_j$  for some  $j$ . Consider the ascending sequence  $L \subseteq LK_{j+1} \subseteq LK_{j+2} \subseteq \cdots$  of subfields of  $LK$ . We have  $LK = \bigcup_{i=1}^{\infty} LK_{j+i}$ . Moreover,  $LK_{j+i}/L$  is Galois since  $K_{j+i}/F$  is Galois and

$$\text{Gal}(LK_{j+i}/L) \simeq \text{Gal}(K_{j+i}/(K_{j+i} \cap L)) = \text{Gal}(K_{j+i}/K_j)$$

is cyclic of order  $p^i$  for each  $i$ . Therefore, the subfields of  $LK_{j+i}$  containing  $L$  are linearly ordered, and  $LK$ ,  $L$  and  $\{LK_{j+i}\}_{i=1}^{\infty}$  satisfy the hypothesis of Corollary 2.2. Consequently,  $LK$  is a Galois  $J$ -extension of  $L$ .

We remark that Corollary 2.6 does not extend to the case where  $K/P$  is a separable  $J$ -extension; an example showing this is noted after the presentation of Example 2.15.

Suppose the field  $F$  admits a Galois  $J$ -extension. Corollary 2.6 implies that if  $L$  is an extension field of  $F$  such that the algebraic closure  $E$  of  $F$  in  $L$  is finite-dimensional over  $F$ , then  $L$  also admits a Galois  $J$ -extension. We investigate more thoroughly in §3 the problem of determining the class of fields that admit Galois  $J$ -extensions, but for the present we merely review a concrete construction of  $J$ -extensions of the field  $Q$  and certain related fields (see [I, §2] or [Wa, §§7.2, 7.3]).

**EXAMPLE 2.7.** Let  $p \in Z^+$  be prime and for each  $r \in Z^+$ , let  $\zeta_r$  be a primitive complex  $p^r$ th root of unity. If  $p$  is odd, the field  $Q(\zeta_r)$  is cyclic over  $Q$  of degree  $p^{r-1}(p-1)$  [J, p. 113]; hence  $Q(\zeta_r)$  is cyclic over  $Q(\zeta_1)$  of degree  $p^{r-1}$ , so Corollary 2.2 implies that  $K = \bigcup_{r=1}^{\infty} Q(\zeta_r)$  is a  $J$ -extension of  $Q(\zeta_1)$ . However, since  $[Q(\zeta_1) : E]$  is not divisible by  $p$  for each proper subfield  $E$  of  $Q(\zeta_1)$ , it follows that  $K$  is not a  $J$ -extension of  $E$  for any such  $E$ . In particular,  $K$  is not a  $J$ -extension of  $Q$ . On the other hand, the field  $Q(\zeta_r)$  contains a unique subfield  $L_r$  of degree  $p^{r-1}$  over  $Q$ ,  $L_r/Q$  is cyclic, and  $L_r \supseteq L_{r-1}$  for  $r \geq 2$ . Therefore  $L = \bigcup_{r=1}^{\infty} L_r$  is a  $J$ -extension of  $Q$  contained in  $K$ .

If  $p = 2$  and  $r \geq 3$ , then  $\text{Gal}(Q(\zeta_r)/Q)$  is the direct product of a cyclic group of order  $2^{r-2}$  and a group of order 2. The real subfield of  $Q(\zeta_r)$  is the field  $F_r = Q(\zeta_r + \zeta_r^{-1}) = Q(\cos(2\pi/2^r))$ ; it is cyclic over  $Q$  of degree  $2^{r-2}$ , and  $F_r \supseteq F_{r-1}$  for  $r \geq 4$ . Consequently,  $F = \bigcup_{r=3}^{\infty} F_r$  is a  $J$ -extension of  $Q$ . As in the case where  $p$  is odd, the field  $\bigcup_{r=3}^{\infty} Q(\zeta_r)$  is a Galois  $J$ -extension of  $Q(\zeta_2) = Q(i)$ .

Some aspects of Example 2.7 seem worthy of comment. First, Theorem 2.5 shows that any Galois  $J$ -extension of  $Q$  is abelian, and hence is contained in the abelian closure of  $Q$ . We observe that if  $F$  is a subfield of the real field  $\mathbf{R}$  and if  $K$  is a Galois  $J$ -extension of  $F$ , then  $K$  is also contained in  $\mathbf{R}$ , for if not, then complex conjugation induces an automorphism  $\mu$  of  $K$  with fixed subfield  $E$  of codimension 2 in  $K$ , a contradiction to the assumption that  $K/F$  is a  $J$ -extension. In particular, any Galois  $J$ -extension of  $Q$  is real. This means, for example, that no nonreal cyclic extension of  $Q$  of prime degree (for example,  $Q(\sqrt{-2})$ ) can be extended to a Galois  $J$ -extension of  $Q$ . It follows from the proof of Theorem 3.11, however, that certain fields of this type (for example,  $Q(\sqrt{-2})$ ) can be extended to a  $J$ -extension of  $Q$ .

What can be said about the structure of a  $J$ -extension  $K/F$  in the case where  $K/F$  is not Galois? This question can be partially reduced to the case where  $K/F$  is either separable or purely inseparable as follows. If  $K/F$  is not separable, then the separable part  $K_s$  of  $K/F$  is a finite extension of  $F$  and  $K/K_s$  is a purely inseparable  $J$ -extension. The reduction is partial because for fields  $F \subseteq E \subseteq K$  with  $E/F$  finite separable and  $K/E$  a purely inseparable  $J$ -extension, it need not follow that  $K/F$  is a  $J$ -extension. For example, let  $F = F_0(X^3)$ , where  $\text{char } F_0 = 2$ , let  $E = F_0(X)$ , and let  $K = F_0(\{X^{1/2^n}\}_{n=1}^\infty)$ ;  $F_0(\{X^{3/2^n}\}_{n=1}^\infty)$  is a proper intermediate field that is not finite-dimensional over  $F$ . One question that naturally arises is whether a  $J$ -extension must, in fact, be either separable or purely inseparable. If  $K/F$  is a normal  $J$ -extension, this question has an affirmative answer, for in that case  $K$  is the composite of  $K_s$  and  $K_i$ , the separable and purely inseparable parts of  $K/F$ , respectively [Ba, p. 88]. Hence  $K_s/F$  or  $K_i/F$  is not finite-dimensional, which implies that  $K = K_s$  or  $K = K_i$ . In general, however, Example 2.11 shows that this question has a negative answer. The presentation of Example 2.11 uses two auxiliary results. The first of these, Lemma 2.8, must be known, but we haven't located an appropriate reference. The statement of Lemma 2.10 uses the following terminology from [Re]. An extension field  $K$  of  $F$  is an *exceptional extension* of  $F$  if  $K/F$  is algebraic, not separable, and  $F$  is the purely inseparable part of  $K/F$ .

**LEMMA 2.8.** *Assume that  $\text{char } F = p \neq 0$  and consider a simple purely inseparable extension  $F(\theta)$  of  $F$ , where  $\theta$  has exponent  $e > 1$  over  $F$ .*

- (1) *For  $1 \leq i \leq e$ ,  $F(\theta^{p^{e-i}}) = \{x \in F(\theta) \mid x^{p^i} \in F\}$ .*
- (2) *If  $\alpha \in F(\theta^{p^{e-i}}) \setminus F(\theta^{p^{e-i+1}})$ , then  $F(\alpha) = F(\theta^{p^{e-i}})$ .*
- (3)  *$\{F(\theta^{p^j})\}_{j=0}^e$  is the set of intermediate fields.*

*Proof.* In (1), we use induction on  $e$ . The case where  $e = 1$  is obvious. At the inductive step, suppose  $\theta$  has exponent  $e + 1$  over  $F$  and the result is known for exponent  $e$ . Let  $E = \{x \in F(\theta) \mid x^{p^e} \in F\}$ . The inclusions  $F(\theta^p) \subseteq E$  and  $E < F(\theta)$  are clear. Since  $[F(\theta) : F(\theta^p)] = p$ , we conclude that  $E = F(\theta^p)$ , where  $\theta^p$  has exponent  $e$  over  $F$ . The equality  $F(\theta^{p^{e+1-i}}) = \{x \in F(\theta) \mid x^{p^i} \in F\}$  is obvious for  $i = e + 1$ . If  $1 \leq i \leq e$  and if  $x^{p^i} \in F$ , then  $x^{p^e} \in F$  and  $x \in F(\theta^p)$ . Thus, the induction hypothesis implies that  $x \in F((\theta^p)^{p^{e-i}}) = F(\theta^{p^{e+1-i}})$ .

(2) If  $\alpha \in F(\theta^{p^{e-i}}) \setminus F(\theta^{p^{e-i+1}})$ , then (1) shows that  $\alpha$  has exponent  $i$  over  $F$ . Therefore  $[F(\alpha) : F] = p^i = [F(\theta^{p^{e-i}}) : F]$ , and consequently,  $F(\alpha) = F(\theta^{p^{e-i}})$ .

(3) follows immediately from (2).

**COROLLARY 2.9.** *Assume that  $\text{char } F = p \neq 0$  and  $F(t)/F$  is a simple inseparable extension of exponent  $e > 1$ . Then  $F(t)/F$  is exceptional if and only if  $F(t^{p^{e-1}})/F$  is exceptional.*

*Proof.* Clearly  $F(t^{p^{e-1}})/F$  is exceptional if  $F(t)/F$  is exceptional. For the converse, we show that if  $x \in F(t)$  is such that  $x^p \in F$ , then  $x \in F$ . This statement follows from Lemma 2.8:  $F(t)/F(t^{p^e})$  is of exponent  $e$ , so Lemma 2.8 implies that  $x \in F(t^{p^{e-1}})$ , and hence  $x \in F$  since  $F(t^{p^{e-1}})/F$  is exceptional.

**LEMMA 2.10.** *Assume that  $F$  is a field of characteristic  $p \neq 0$  and let  $K$  be an algebraic extension of  $F$  containing elements  $a, b, s$  with the following properties:  $a^p, b^p \in F$ ,  $[F(a, b):F] = p^2$ , and  $F(s)/F$  is a nontrivial Galois extension. Let  $t = a + bs$  and let  $L = F(t)$ . Then  $F(t)/F$  is an exceptional extension,  $F(s)$  is the separable part of  $F(t)/F$ , and if  $\alpha \in F(t) \setminus F(s)$ , then  $F(s) = F(\alpha^p)$ .*

*Proof.* We have  $t^p = a^p + b^p s^p$  so  $F(t^p) = F(s^p) = F(s)$ . The inclusion  $F(s) \subseteq F(t)$  is proper, for if not, then  $F(s, b) \supseteq F(s, b, a + bs) = F(s, b, a)$ , so that  $F(s, b) = F(s, b, a)$ . This is a contradiction since  $[F(s, b):F]_i = p$  while  $[F(s, b, a):F]_i = p^2$ . Therefore  $F(s) < F(t)$ ,  $F(s)$  is the separable part of  $F(t)/F$ , and  $[F(t):F]_i = p$ . We next show that  $t$  is the unique conjugate in  $F(t)$  of  $t$  over  $F$ . To do so, let  $K$  be a normal closure of  $F(t)/F$ . If  $t$  is not the only conjugate of  $t$  in  $F(t)$ , then there exists an  $F$ -automorphism  $\sigma$  of  $K$  such that  $\sigma(t) \in F(t)$ ,  $\sigma(t) \neq t$ . Since  $t = a + bs$  with  $a, b$  purely inseparable over  $F$ , then  $\sigma(t) = a + bu$ , where  $u = \sigma(s)$ . We have  $F(t) = F(\sigma(t))$ , and by the argument given above,  $F(s) = F(u)$  is the separable part of  $F(t)/F$ . Moreover,  $t \neq \sigma(t)$  implies that  $s \neq u$ . Thus,  $b(u - s) = a + bu - t \in F(t)$  so  $b \in F(t)$  and  $a = t - bs \in F(t)$ , contrary to the fact that  $[F(t):F]_i < [F(s, a, b):F]_i$ . We conclude that  $F(s)$  is the unique proper subfield of  $F(t)$  containing  $F$  over which  $F(t)$  is normal. In particular,  $F(t)/F$  is exceptional, for if not, then  $F(t)$  is the composite of  $F(s)$  and the purely inseparable part of  $F(t)$  over  $F$ , and hence is normal over  $F$ , a contradiction. Finally, we show that  $F(s) = F(\alpha^p)$  for each  $\alpha \in F(t) \setminus F(s)$ . The inclusion  $F(\alpha^p) \subseteq F(s)$  holds since  $F(t)/F(s)$  is purely inseparable of exponent 1. Note, however, that  $F(t)$  is the composite of  $F(s)$  and the purely inseparable part of  $F(t)/F(\alpha^p)$ , implying that  $F(t)/F(\alpha^p)$  is normal. We conclude that  $F(\alpha^p) = F(s)$ , and this completes the proof of Lemma 2.10.

EXAMPLE 2.11. Let the notation and hypothesis be as in the statement of Lemma 2.10. If  $E = \bigcup_{n=1}^{\infty} F(t^{1/p^n})$ , then  $E$  is an exceptional  $J$ -extension of  $F$ . Moreover, if  $\alpha \in E \setminus F(s)$ , then  $F(s) \subseteq F(\alpha)$ , so each subfield of  $E$  containing  $F$  compares with  $F(s)$  under inclusion.

*Proof.* To prove that  $E$  is a  $J$ -extension of  $F$ , we choose  $x_n \in E \setminus F(t^{1/p^n})$  for each  $n$  and we show that  $E = F(\{x_i\}_{i=1}^{\infty})$ . Thus, for a fixed  $n$ , choose  $m$  so that  $x_n \in F(t^{1/p^m}) \setminus F(t^{1/p^{m-1}})$ ; note that  $m > n$ . Considering  $F(t^{1/p^m})$  as an extension of  $F(t^p) = F(s)$ , Lemma 2.8 shows that  $x_n^{p^m} \in F(t) \setminus F(s)$ . Therefore  $F(x_n^{p^m}) = F(t)$  by Lemma 2.10 so that  $F(x_n) = F(t)(x_n) = F(t^{1/p^m}) \supseteq F(t^{1/p^n})$ . We conclude that  $E$  is a  $J$ -extension of  $F$ . Moreover, the preceding proof, together with Lemma 2.10, shows that  $F(\alpha) \supseteq F(s)$  for each  $\alpha \in E \setminus F(s)$ . Clearly  $E/F$  is not separable; to show that  $E/F$  is exceptional, it suffices to show that  $F(t^{1/p^n})/F$  is exceptional for each  $n$ . This last assertion follows at once from Lemma 2.10 and Corollary 2.9.

One example of fields  $F$  and  $K$  as in the statement of Lemma 2.10 can be obtained by taking  $F = L(a^p, b^p)$  and  $K = L(s, a, b)$ , where  $L$  is a field of characteristic  $p \neq 0$ ,  $a$  and  $b$  are indeterminates over  $L$ , and  $L(s)/L$  is Galois. The presentation of Example 2.11 shows that the lattice of fields between  $F$  and  $E = \bigcup_{n=1}^{\infty} F(t^{1/p^n})$  consists of an isomorphic copy of the lattice of fields between  $L$  and  $L(s)$ , topped by a well-ordered countably infinite chain. Since the lattice of fields between  $L$  and  $L(s)$  is as arbitrary as the lattice of subgroups of a finite group under  $\supseteq$ , it follows that at least at the “bottom”, little can be said about the lattice of subfields of an inseparable  $J$ -extension.

We turn to the problem of examining the structure of a separable  $J$ -extension  $K/F$ . While it seems reasonable to think that  $K/F$  might share properties in common with Galois  $J$ -extensions, as recorded in Theorem 2.5, this turns out to not be the case. One reason that the usual procedure for passing from Galois to separable extensions fails in this case is that no proper extension  $L$  of  $K$  is a  $J$ -extension of  $F$ ; in particular, the normal closure  $L$  of  $K/F$  is not a  $J$ -extension of  $F$  if  $L \neq K$ . We present two constructions of separable  $J$ -extensions  $K/F$ . In the first (Example 2.15), the set  $\{K_i\}_0^{\infty}$  of intermediate fields forms a chain  $F = K_0 < K_1 < \cdots$ , but the degrees  $[K_{i+1} : K_i]$  need not be prime and the set  $\{[K_{i+1} : K_i]\}_{i=0}^{\infty}$  may be infinite. Each example of a  $J$ -extension  $K/F$  considered thus far in the paper has been such that there exists a proper intermediate field  $E$  such that the fields between  $E$  and  $K$  form a

chain. In Example 2.18, we give an example of a separable  $J$ -extension that fails to satisfy this condition. In both Example 2.15 and 2.18, we use results of Fried and MacRae from [FM]. For sake of reference, we record the results used from [FM] as Theorem 2.12; it is a composite of Proposition 3.4 and Theorem 3.6 of [FM].

**THEOREM 2.12 (Fried-MacRae).** *Let  $K$  be a field and let  $f(X) \in K[X] \setminus K$  be such that  $\text{char } K$  does not divide the degree of  $f(X)$ . Each field between  $K(X)$  and  $K(f(X))$  is of the form  $K(g(X))$ , where  $g(X) \in K[X]$  is such that  $f(X) \in K[g(X)]$ . If  $M_1$  and  $M_2$  are intermediate fields of degrees  $d_1$  and  $d_2$ , respectively, over  $K(f(X))$ , then  $[M_1 \cap M_2 : K(f(X))] = \gcd\{d_1, d_2\}$  and  $[M_1 M_2 : K(f(X))] = \text{lcm}\{d_1, d_2\}$ . In particular,  $M_1 \subseteq M_2$  if and only if  $d_1 \mid d_2$ .*

We use two lemmas in presenting Example 2.15.

**LEMMA 2.13.** *Assume that  $r > 1$  is an integer not divisible by the characteristic of the field  $F$ . If  $g = X^r + X^{r-1}$ , then there exists no intermediate field properly between  $F(g)$  and  $F(X)$ .*

*Proof.* By Theorem 2.12, it suffices to show that if  $f \in F[X]$  is such that  $g = h(f)$  for some  $h \in F[X]$ , then either  $\deg f = 1$  or  $\deg f = r$ . Without loss of generality we assume that  $f(0) = 0$ . Then considering  $f, g$ , and  $h$  as elements of  $F[[X]]$ , we have  $\text{ord } g = r - 1 = \text{ord } h \cdot \text{ord } f$ , where  $\text{ord}$  denotes the order function. Moreover,  $\deg g = r = \deg h \cdot \deg f$ . These equations are impossible for  $\text{ord } h < \deg h$  and  $\text{ord } f < \deg f$ . Hence either  $\text{ord } h = \deg h$  or  $\text{ord } f = \deg f$ ; in the first case,  $\deg h = 1$  and  $\deg f = r$ , while the second implies  $\deg f = 1$ . This completes the proof.

**LEMMA 2.14.** *Assume that  $F$  is a field and  $f(X) \in F[X]$  is such that  $\text{char } F$  does not divide  $\deg f$ . Assume that there exists a sequence  $\{F_i\}_{i=0}^n$  of subfields of  $F(X)$  such that  $F(f) = F_0 < F_1 < \dots < F_n = F(X)$  and the following conditions are satisfied for  $0 \leq i \leq n - 1$ .*

- (1) *There are no fields properly between  $F_i$  and  $F_{i+1}$ ,*
- (2) *Each prime divisor of  $[F_i : F_0]$  divides  $[F_{i+1} : F_i]$ .*

*Then  $\{F_i\}_{i=0}^n$  is the set of subfields of  $F_n$  containing  $F_0$ .*

*Proof.* We use induction on  $n$ , the case  $n = 1$  being obvious. Assume the result for  $n - 1$ . Let the prime factorization of  $[F_{n-1} : F_0]$  be  $p_1^{e_1} \dots p_k^{e_k}$  and let  $[F_n : F_0] = (p_1^{h_1} \dots p_k^{h_k})b$ , where no  $p_i$  divides  $b$  and  $e_j < h_j$  for

each  $j$ . Let  $K$  be a subfield of  $F_n$  containing  $F_0$ . If  $K \subseteq F_{n-1}$ , then  $K \in \{F_i\}_{i=0}^{n-1}$  by the induction hypothesis. Otherwise, let  $[K:F_0] = p^{u_1} \cdots p_k^{u_k} c$ , where  $c$  is divisible by no  $p_i$ . Since  $F_{n-1} < KF_{n-1}$ , (1) implies that  $KF_{n-1} = F_n$ , and Theorem 2.12 shows that  $[F_n:F_0] = (p_1^{h_1} \cdots p_k^{h_k})b = \text{lcm}\{p_1^{u_1} \cdots p_k^{u_k} c, p_1^{e_1} \cdots p_k^{e_k}\}$ . Since  $e_i < h_i$  for each  $i$ , this implies that  $c = b$  and  $u_i = h_i$  for each  $i$ , and hence  $F_n = K$ .

**EXAMPLE 2.15.** Let  $F$  be a field and let  $\{k_i\}_{i=1}$  be a sequence of integers,  $k_i > 1$ , such that (i)  $\text{char } F$  does not divide  $k_i$  for each  $i$ , and (ii) each prime divisor of  $k_1 k_2 \cdots k_n$  divides  $k_{n+1}$  for each  $n$ . We prove existence of a separable  $J$ -extension  $K$  of  $F(X)$  with the following properties: (a) the set of proper intermediate fields forms a chain  $F(X) = F_0 < F_1 < F_2 < \cdots$ , and (b)  $[F_i:F_{i-1}] = k_i$  for each  $i$ . Thus, let  $y_1$  be a root of  $Y^{k_1} + Y^{k_1-1} - X$  in an extension field of  $F(X)$  and let  $F_1 = F(y_1)$ . The element  $y_1$  is transcendental over  $F$  and  $X = y_1^{k_1} + y_1^{k_1-1}$ . Therefore Lemma 2.13 implies that there exist no proper intermediate field between  $F_0$  and  $F_1$  and  $[F_1:F_0] = k_1$ . Let  $y_2$  be a root of  $Y^{k_2} + Y^{k_2-1} - y_1$  in an extension field of  $F_1$ . As above, if  $F_2 = F(y_2)$ , then  $[F_2:F_1] = k_2$  and there exists no proper intermediate field between  $F_1$  and  $F_2$ . Now  $X$  is a polynomial in  $y_2$  of degree  $k_1 k_2$ , so Lemma 2.14 shows that  $\{F_0, F_1, F_2\}$  is the set of subfields of  $F_2$  containing  $F_0$ . We inductively continue this process, obtaining a strictly ascending sequence  $\{F_i\}_{i=0}^\infty$  such that  $\{F_i\}_{i=0}^n$  is the set of subfields of  $F_n$  containing  $F_0$  for each  $n$  and  $[F_n:F_{n-1}] = k_n$  for each  $n$ . Corollary 2.2 shows that  $K$  is a  $J$ -extension of  $F(X)$ , and  $K/F(X)$  is separable since  $\text{char } F$  does not divide  $[F_n:F(X)] = k_1 k_2 \cdots k_n$  for each  $n$ .

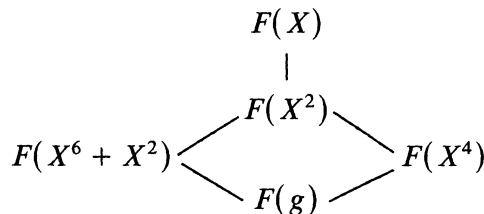
Corollary 2.6 states that if  $K/F$  is a Galois  $J$ -extension, if  $F \subseteq L$ , and if  $K \not\subseteq L$ , then  $LK/L$  is also a  $J$ -extension. Lemma 2.14 can be used, as in Example 2.15, to show that this result does not extend to the case where  $K/F$  is a separable  $J$ -extension. To see this, let  $C$  be the field of complex numbers, let  $F = C(X)$ , and let  $K = F(y_1, y_2, \dots)$ , where  $y_1^7 + y_1^6 - X = 0$ ,  $y_2^7 + y_2^6 - y_1 = 0$ ,  $\dots$ . Lemma 2.14 implies that  $K/F$  is a separable  $J$ -extension. Let  $L = C((X))$ , the quotient field of the formal power series ring  $C[[X]]$ . For  $n \in \mathbb{Z}^+$ , it is known that  $C((X^{1/n})) = L(X^{1/n})$  is the unique algebraic extension of  $L$  of degree  $n$  [Co, Cor. 5.339, p. 418], and  $\bigcup_{n=1}^\infty L(X^{1/n})$  is the algebraic closure of  $L$ . We note that  $X = y_1^7 + y_1^6 = y_1^6(1 + y_1)$  and  $1 + y_1$  has a sixth root  $b$  in  $C[[y_1]] = C[[y_1^6 + y_1^7]][y_1] = C[[X]][y_1] \subseteq L(y_1)$ ; here the equality  $C[[y_1^6 + y_1^7]][y_1] = C[[y_1]]$  follows, for example, from [Bo2, p. 309]. It follows that  $X = (by_1)^6$ , and hence  $L(y_1) = L(X^{1/6})$ . Similarly,  $L(y_1, \dots, y_n)$  has degree

$6^n$  over  $L$ , so  $L(y_1, \dots, y_n) = L(X^{1/6^n})$  for each  $n \in \mathbb{Z}^+$ . Because  $L$  contains the  $6^n$ th roots of unity, it follows that  $LK = L(y_1, y_2, \dots) = \bigcup_{n=1}^{\infty} L(X^{1/6^n})$  is a Galois extension of  $L$ . Since  $L(X^{1/6})$  is an intermediate field of degree 6 over  $L$ , Theorem 2.5 implies that  $LK/L$  is not a  $J$ -extension; more directly,  $\bigcup_{n=1}^{\infty} L(X^{1/2^n})$  is a proper intermediate field that is not finitely generated over  $L$ .

By passing from  $K/F$  to  $K(T)/F(T)$ , where  $T$  is a transcendence basis for  $L = C((X))$  over  $F = C(X)$ , one sees in the above example that a  $J$ -extension need not lift under a separable algebraic field extension, even in the case where the intermediate fields of the  $J$ -extension are linearly ordered and the degree of any adjacent pair of intermediate fields is a fixed prime (in this case 7). Here we are making use of the fact that if  $K/F$  is a separable algebraic field extension and  $T$  is a family of indeterminates over  $K$ , then the lattice of fields between  $F$  and  $K$  is isomorphic to the lattice of fields between  $F(T)$  and  $K(T)$ . To see this fact, one may reduce to the case where  $E/F$  is a finite separable algebraic field extension and use Galois theory. If  $M/F$  is the normal closure of  $E/F$ , then  $M(T)/F(T)$  is the normal closure of  $E(T)/F(T)$ , the Galois groups are isomorphic, and any field between  $F(T)$  and  $E(T)$  is generated over  $F(T)$  by an element of  $E$ .

In comparison to Example 2.15, Example 2.18 is more specific in nature. Also, while Example 2.15 is designed to produce a linearly ordered set of intermediate extensions in a separable  $J$ -extension, the main point of Example 2.18 is to show that branching may occur infinitely often in such an extension. Again we require two lemmas in Example 2.18.

LEMMA 2.16. *Let  $F$  be a field of characteristic distinct from 2 and 3 and let  $g = (X^4 + 1)^2 X^4 \in F[X]$ . The lattice of fields between  $F(X)$  and  $F(g)$  is as follows.*



*Proof.* We have  $g = (X^6 + X^2)^2$ , and clearly  $g$  is a polynomial in both  $X^2$  and  $X^4$ , so there exist distinct intermediate fields as indicated in the diagram. Theorem 2.12 shows that for each divisor  $d$  of 12, there

exists at most one intermediate field of degree  $d$  over  $F(g)$ . Hence, to complete the proof, it suffices to show that there exists no intermediate field of degree 4 over  $F(g)$ . Equivalently, we need to show that  $g \notin F[f(X)]$  for each cubic polynomial  $f(X) \in F[X]$ . Assume, to the contrary, that  $g = f^4 + af^3 + bf^2 + cf + d$  where, without loss of generality, we assume that  $f$  is monic with constant term 0. As a power series in  $X$ ,  $g$  has order 4, so  $c = d = 0$  and  $g = (X^4 + 1)^2 X^4 = f^2(f^2 + af + b)$ . The polynomials  $(X^4 + 1)^2$  and  $X^4$  are relatively prime; if  $b \neq 0$ , then  $f^2$  and  $f^2 + af + b$  are relatively prime, and in this case  $(X^4 + 1)^2$  divides either  $f^2$  or  $f^2 + af + b$ , an impossibility by a degree argument. Hence  $b = 0$  and  $g = f^3(f + a)$ . Now  $a = 0$  is impossible because  $g$  is not a fourth power in  $F[X]$ . But if  $a \neq 0$ , then  $f^3$  and  $f + a$  are relatively prime and we conclude that  $f^3$  is an associate of either  $(X^4 + 1)^2$  or  $X^4$ , neither of which is possible by a degree argument. We conclude that there exists no intermediate field of degree 4 over  $F(g)$ .

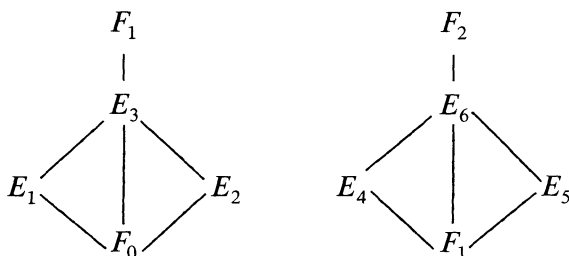
LEMMA 2.17. *Assume that  $F$  is a field of characteristic distinct from 2 and 3. The lattice of fields between  $F(X)$  and  $F((X + 1)^4 X^2)$  is as follows.*

$$\begin{array}{c} F(X) \\ | \\ F((X + 1)^2 X) \\ | \\ F((X + 1)^4 X^2) \end{array}$$

*Proof.* As in Lemma 2.16, we need only show that  $(X + 1)^4 X^2 \notin F[f(X)]$  for each quadratic  $f \in F[X]$ . Because of its similarity to the proof of Lemma 2.16, we omit the proof of this statement.

EXAMPLE 2.18. Let  $F$  be a field of characteristic distinct from 2 and 3. To obtain a separable  $J$ -extension with infinite branching, we iterate infinitely many times the extension suggested by Lemma 2.16. To wit, let  $F_0 = F(X)$  and let  $F_1 = F_0(y_1)$ , where  $y_1$  is a root of  $(Y^4 + 1)^2 Y^4 - X$  in an extension field of  $F_0$ , let  $F_2 = F_1(y_2)$ , where  $(y_2^4 + 1)^2 y_2^4 - y_1 = 0$ , and so forth. We take  $K = \bigcup_{i=1}^{\infty} F_i$  and intend to show that  $K/F_0$  is a separable  $J$ -extension. That  $K/F_0$  is separable is clear. The key result in showing that  $K/F_0$  is a  $J$ -extension is a proof that each subfield of  $F_n$  containing  $F_0$  lies between  $F_i$  and  $F_{i-1}$  for some  $i \in \{1, 2, \dots, n\}$ . The proof is by induction on  $n$ , and the case  $n = 2$  is crucial in the process.

Thus, label the lattice of fields between  $F_0$  and  $F_1$  and between  $F_1$  and  $F_2$  as follows.



Letting  $t = y_2^4$ , we examine the following piece of the joined lattice.

$$\begin{array}{rcl}
 & & E_5 = F(y_2^4) = F(t) \\
 & \swarrow & \\
 F_1 & = & F((t+1)^2 t) \\
 & | & \\
 & & E_3 = F((t+1)^4 t^2)
 \end{array}$$

According to Lemma 2.17, no subfield of  $E_5$  containing  $E_3$  has degree 3 over  $E_3$ . Since  $X$  is a polynomial in  $y_2$  of degree 144, Theorem 2.12 implies that there exists no intermediate field  $E$ ,  $F_0 \subseteq E \subseteq F_2$ , with  $[E:F_0] = 18$ , for since  $6|18$  and  $18|36$ , such a field  $E$  would lie between  $E_3$ , of degree 6 over  $F_0$ , and  $E_5$ , of degree 36 over  $F_0$ , and would have degree 3 over  $E_3$ , an impossibility. Now let  $S = \{d \mid d = [E:F_0] \text{ for some field } E \text{ with } F_0 \subseteq E \subseteq F_2\}$ . The set  $S$  contains  $T = \{1, 2, 3, 6, 12, 24, 36, 72, 144\}$ , it is closed under taking greatest common divisors and least common multiples, and we know that  $4, 18, 48 \notin S$ . It is then straightforward to show that  $S = T$ , and hence the assertion holds for  $n = 2$ . Assume by induction that each subfield of  $F_n$  containing  $F_0$  lies between  $F_{i-1}$  and  $F_i$  for some  $i$  between 1 and  $n$ . Since the map  $y_n \rightarrow y_{n+1}$  determines an  $F$ -isomorphism of  $F_n$  onto  $F_{n+1}$  that maps  $F_0$  to  $F_1$ , we know also that each subfield of  $F_{n+1}$  containing  $F_1$  lies between  $F_{i-1}$  and  $F_i$  for some  $i$  between 2 and  $n+1$ . Let  $E$  be a subfield of  $F_{n+1}$  containing  $F_0$  and let  $h = [E:F_0]$ . If  $12|h$  or if  $[F_n:F] = 2^{2n}3^n|h$ , then  $E$  lies between some  $F_{i-1}$  and  $F_i$ . Otherwise,  $EF_n > F_n$  and  $[EF_n:F_0] = \text{lcm}\{h, 2^{2n}3^n\}$  is a proper multiple of  $2^{2n}3^n$ . Therefore either (i)  $2^{2n+1}|h$  and  $3 \nmid h$  or (ii)  $3^{n+1}|h$ . If (i) is true, we obtain the contradiction that  $E \cap F_1$  has degree 4 over  $F_0$ . Suppose (ii) holds. If  $2 \nmid h$ , we obtain the contradiction that  $E \cap E_5$  has degree 9 over  $F_0$ , and if  $2|h$ , then  $[E \cap E_5:F_0] = 18$  yields a contradiction. Hence  $E$  lies between some  $F_{i-1}$  and  $F_i$ .

Finally we conclude that  $K/F_0$  is a  $J$ -extension, for if  $x_n \in K \setminus F_n$  for each  $n$ , then the above result shows that  $F_0(x_n) \supseteq F_n$ , so  $F_0(\{x_n\}_{n=1}^\infty) = K$ . Also, the fields between  $E$  and  $K$  are not linearly ordered for any proper intermediate field  $E$ , for any such  $E$  is contained in some  $F_n$ .

We remark that Example 2.18 has the following group-theoretic implication. If  $E$  is an intermediate field of  $K/F_0$  such that  $E$  is maximal with respect to failure to contain  $a \in K \setminus F_0$ , the  $E(a)$  is the unique minimal proper extension of  $E$  in  $K$ . If  $K_s$  is the separable closure of  $K/E$ ,  $G = \text{Gal}(K_s/E)$  and  $H = \text{Gal}(K_s/K)$ , then  $H$  is contained in a unique maximal subgroup of  $G$ . Since the fields between  $E$  and  $K$  are not linearly ordered, neither are the subgroups of  $G$  containing  $H$  linearly ordered. By taking finite extensions of  $E$  in  $K$ , examples similar to the above can be obtained, where  $G$  is a finite group. On the other hand, it is easy to see that if  $H$  is a normal subgroup of  $G$  contained in a unique maximal subgroup of  $G$ , then the subgroups of  $G$  containing  $H$  are linearly ordered.

We conclude this section with some remarks concerning the structure of purely inseparable  $J$ -extensions. For sake of reference, we call a purely inseparable  $J$ -extension constructed as in example (E2) of the introduction *standard*. Nonstandard examples are not easy to construct, but they do exist. Deveney in [De] constructs, in fact, a purely inseparable  $J$ -extension  $U/V$ , where  $\text{char } V = p$ , so that if  $U_i = \{x \in U \mid x^{p^i} \in V\}$ , then  $[U_i:V] = p^{2^i}$  for each  $i$ ; the set of intermediate fields is not linearly ordered, nor is there a proper intermediate field  $W$  such that the set of subfields of  $U$  containing  $W$  is linearly ordered. If  $x \in U \setminus V$  and if  $W$  is an intermediate field maximal with respect to failure to contain  $x$ , then  $U/W$  provides an example of a nonstandard  $J$ -extension such that  $\{u \in U \mid u^p \in W\}$  has degree  $p$  over  $W$ . Proposition 2.19 contains some positive information concerning purely inseparable  $J$ -extensions.

**PROPOSITION 2.19.** *Assume  $F$  is a field of characteristic  $p \neq 0$  and let  $K$  be a purely inseparable  $J$ -extension of  $F$ . For  $n \in \mathbb{Z}_0$ , let  $K_n = \{x \in K \mid x^{p^n} \in F\} = F^{1/p^n} \cap K$ .*

(1) *The sequence  $\{K_n\}_{n=1}^\infty$  is strictly ascending—that is,  $K$  does not have finite exponent over  $F$ .*

(2)  *$K/F$  is standard if and only if there exists  $s \in F \setminus F^p$  such that  $s^{1/p^n} \in K$  for each  $n \in \mathbb{Z}^+$ .*

*Proof.* (1): Suppose  $K = K_n$  for some  $n$ . Clearly  $n > 0$ . We assume that  $n$  is minimal so that  $K = K_n$ . Then  $K/K_{n-1}$  is a  $J$ -extension of exponent 1. This is impossible, for if  $B$  is a  $p$ -basis for  $K/K_{n-1}$  and if

$b \in B$ , then  $K_{n-1}(B \setminus \{b\})$  is an infinite-dimensional extension of  $K_{n-1}$  properly contained in  $K$ . Therefore  $K_n < K$  for each  $n$ .

(2) If  $K/F$  is standard, then the stated condition is satisfied by definition. Conversely, if  $K$  contains  $\{s^{1/p^n}\}_{n=1}^\infty$  for some  $s \in F \setminus F^p$ , then  $F(\{s^{1/p^n}\}_1^\infty)$  is an infinite-dimensional extension of  $F$  in  $K$ , and hence is equal to  $K$ .

While a standard purely inseparable  $J$ -extension is such that the set of intermediate fields is linearly ordered, a purely inseparable  $J$ -extension  $L/E$  with linearly ordered intermediate fields need not be standard. For example, we can take

$$E = M(\{X_i\}_{i=1}^\infty), \quad \text{where } \text{char } M = p \neq 0, \quad \text{and}$$

$$L = E(\{X_1^{1/p^n} + X_2^{1/p^{n-1}} + \dots + X_n^{1/p}\}_{n=1}^\infty).$$

**3. Fields that admit a  $J$ -extension.** We consider in this section the problem of determining those fields that admit a  $J$ -extension or a Galois  $J$ -extension. We begin with a consideration of the Galois case. Theorem 2.5 answers the question in one sense:  $F$  admits a Galois  $J$ -extension if and only if  $W_p$  can be realized as a Galois group over  $F$  for some prime  $p$ . This criterion, however, is elusive, and we seek to give it more substance. If  $W_p$  can be realized as a Galois group over  $F$ , then  $F$  admits a cyclic extension of degree  $p$ . The converse fails (for example, let  $F$  be the real field and let  $p = 2$ ), but we are able to establish the converse in enough cases to provide a large class of fields that admit Galois  $J$ -extensions. In fact, there are three related questions here for a field  $F$ . We list these as Q(1), Q(2), and Q(3); their answers depend upon the fields  $F$  and  $K$ . Q(1) is most clearly related to the problem at hand.

Q(1) If  $F$  admits a cyclic extension of prime degree, does  $F$  admit a Galois  $J$ -extension?

Q(2) If  $K/F$  is cyclic of prime degree  $p$ , can  $W_p$  be realized as a Galois group over  $F$ ?<sup>2</sup>

Q(3) If  $K/F$  is cyclic of prime degree, can  $K$  be extended to a Galois  $J$ -extension of  $F$ ?

We note that an affirmative answer to question Q( $n$ ) implies an affirmative answer to Q( $n - 1$ ); a more general version of Q(3) asks whether  $K$  can be extended to a Galois  $J$ -extension of  $F$  if  $K/F$  is cyclic of prime-power degree.

---

<sup>2</sup>For an odd prime  $p$ , Q(2) has an affirmative answer; see the appendix to this paper.

Cyclic extension fields play a classical role in Galois theory, and papers of Artin and Schreier [AS] and Albert [A1], [A2] are landmarks in the area. In fact, part (1) of Theorem 3.1 listed below comes from [AS], and part (2) comes from [A1]. Theorem 3.1 provides a case in which Q(3) has an affirmative answer.

**THEOREM 3.1** (*Artin-Schreier; Albert*). *Assume that  $F$  is a field of characteristic  $p \neq 0$ .*

(1)  *$F$  admits a cyclic extension of degree  $p$  if and only if  $F \neq \{a^p - a \mid a \in F\}$ .*

(2) *If  $K$  is a cyclic extension of  $F$  of degree  $p^e$ , then  $K$  can be extended to a cyclic extension of degree  $p^{e+1}$ . Consequently,  $K$  can be extended to a Galois  $J$ -extension of  $F$ .*

A second case in which Q(3) has an affirmative answer is provided by Proposition 3.2.

**PROPOSITION 3.2.** *If  $K/F$  is cyclic of prime degree  $p$  and if  $F$  contains the  $p^n$ th roots of unity for all  $n \in \mathbb{Z}^+$ , then  $K$  is contained in a Galois  $J$ -extension of  $F$ .*

*Proof.* If  $\text{char } F = p$ , then the result follows from Theorem 3.1. If  $\text{char } F \neq p$ , then  $K = F(\sqrt[p]{a})$ , where  $a \in F$  [Ba, p. 174]. The Vahlen-Capelli Theorem [K, Theorem 51] then implies that  $X^{p^n} - a$  is irreducible over  $F$  for each  $n \in \mathbb{Z}^+$ , except in the case where  $p = 2$ ,  $\text{char } F \neq 2$ , and  $-4a$  is a fourth power in  $F$ . Since  $F$  contains a primitive fourth root of unity  $i$ , this exceptional case does not occur, for  $-4a = b^4 = -i^2b^4$  implies  $a = (ib^2/2)^2$ , so  $a$  has a square root in  $F$ , a contradiction. Therefore  $X^{p^n} - a$  is irreducible over  $F$  for each  $n$ , and since  $F$  contains the  $p^n$ th roots of unity,  $F(\sqrt[p^n]{a}) = K_n$  is cyclic over  $F$  of degree  $p^n$  for each  $n$  [Ba, p. 175]. Therefore  $E = \bigcup_{n=1}^{\infty} K_n$  is a Galois  $J$ -extension of  $F$  containing  $K$ .

In passing to the case where  $F$  does not contain the  $p^n$ th roots of unity for all  $n$ , some distinction must be made between the cases where  $p = 2$  and where  $p$  is odd. The following lemma, which fails for  $p = 2$  and  $k = 1$ , is at the root of the distinction. The routine proof of Lemma 3.3 is omitted.

**LEMMA 3.3.** *If  $k, r \in \mathbb{Z}^+$ ,  $b \in \mathbb{Z}$ , and  $p$  is prime, then  $(1 + p^k b)^{p^r} \equiv 1 + p^{k+r} b \pmod{p^{k+r+1}}$  if  $p$  is odd. If  $p = 2$ , this congruence is valid for  $k \geq 2$ .*

**PROPOSITION 3.4.** *Assume that  $p$  is prime and that  $F$  is a field that contains the  $p^k$ th roots of unity but not the  $p^{k+1}$ st roots of unity, where  $k \geq 1$  and where  $k \geq 2$  if  $p = 2$ . Let  $\zeta$  be a primitive  $p^k$ th root of unity in  $F$  and for  $r \in \mathbb{Z}^+$ , let  $\zeta_r$  be a root of  $X^{p^r} - \zeta$  in an extension field of  $F$ . Then  $\zeta_r$  is a primitive  $p^{k+r}$ -th root of unity and  $F(\zeta_r)/F$  is cyclic of order  $p^r$ . Therefore  $F(\{\zeta_r\}_{r=1}^\infty)$  is a Galois  $J$ -extension of  $F$  with Galois group  $W_p$ .*

*Proof.* We have  $(\zeta_r)^{p^{k+r}} = (\zeta_r^{p^r})^{p^k} = \zeta^{p^k} = 1$  and  $(\zeta_r)^{p^{k+r-1}} = \zeta^{p^{k-1}} \neq 1$ , so  $\zeta_r$  has order  $p^{k+r}$ . Since  $F$  contains the  $p$ th roots of unity, the equation  $X^p - \zeta$  is either irreducible over  $F$  or it has a root in  $F$  [vdW, p. 180], but the latter condition fails by choice of  $k$ . Hence  $X^p - \zeta$  is irreducible over  $F$ , and as in the proof of Proposition 3.2, the Vahlen-Capelli Theorem implies that  $[F(\zeta_r):F] = p^r$  for each  $r$ . To show that  $F(\zeta_r)/F$  is cyclic, observe that  $(\zeta_r^{1+p^k})^{p^r} = \zeta_r^{p^r} \zeta_r^{p^{k+r}} = \zeta$ . Hence, there exists  $\sigma \in \text{Gal}(F(\zeta_r)/F)$  such that  $\sigma(\zeta_r) = \zeta_r^{1+p^k}$ . The order of  $\sigma$  is the order of  $1 + p^k$  modulo  $p^{k+r}$ , which, according to Lemma 3.3, is  $p^r$ . Thus,  $\sigma$  generates  $\text{Gal}(F(\zeta_r)/F)$ .

Proposition 3.4 may fail for  $p = 2$  and  $k = 1$ ; for example, it fails if  $F = \mathbb{Q}$ . The distinction between the cases  $p = 2$  and  $p > 2$  carries over to the statement of the next result.

**PROPOSITION 3.5.** *Let  $F$  be a field.*

(a) *Assume that  $p$  is an odd prime and that  $F$  does not contain the  $p$ th roots of unity. Let  $\zeta$  be a primitive  $p$ th root of unity in an extension field of  $F$ , and assume that  $F(\zeta)$  does not contain the  $p^n$ th roots of unity for some  $n$ . Then  $F$  admits a Galois  $J$ -extension with Galois group  $W_p$ .*

(b) *If  $p = 2$ , the statement of (a) remains valid if  $F$  does not contain the fourth roots of unity and if  $F(i)$ , where  $i$  is a primitive fourth root of unity in an extension field of  $F$ , does not contain a  $2^n$ th root of unity for some  $n$ .*

*Proof.* The proof is similar to the one used in Example 2.7 to show that  $\mathbb{Q}$  admits Galois  $J$ -extensions, and indeed, Example 2.7 is a special case of Proposition 3.5. To prove (a), assume that  $k \in \mathbb{Z}^+$  is such that  $F(\zeta)$  contains the  $p^k$ th, but not the  $p^{k+1}$ st roots of unity. Fix an algebraic closure  $L$  of  $F(\zeta)$  and for each  $r \in \mathbb{Z}^+$ , let  $\zeta_r$  be a primitive  $p^{k+r}$ th root of unity in  $L$ . Proposition 3.4 shows that  $F(\zeta_r)$  is cyclic over  $F(\zeta)$  of degree  $p^r$ . Hence  $F(\zeta_r)$  is cyclic over  $F$  of degree divisible by  $p^r$ . It follows that  $F(\zeta_r)$  admits a unique subfield  $K_r$  of degree  $p^r$  over  $F$ . Uniqueness also implies that  $K_{r-1} \subseteq K_r$  for  $r \geq 2$ . hence  $K = \bigcup_{r=1}^\infty K_r$  is a Galois  $J$ -extension of  $F$  with Galois group  $W_p$ .

The proof of (b) differs slightly from that of (a). Thus, assume that  $F(i)$  contains the  $2^k$ th but not the  $2^{k+1}$ st roots of unity. If  $\zeta_r$  is a primitive  $2^{k+r}$ th root of unity in a fixed algebraic closure of  $F(i)$ , then  $F(\zeta_r)/F(i)$  is cyclic of degree  $2^r$ . Therefore  $F(\zeta_r)/F$  is a Galois extension of degree  $2^{r+1}$ . The automorphism  $\sigma_r$  of  $F(\zeta_r)/F$  determined by  $\zeta_r \rightarrow \zeta_r^{-1}$  has fixed subfield  $K_r = F(\zeta_r + \zeta_r^{-1})$  of codimension 2 in  $F(\zeta_r)$ . Moreover,  $\sigma_r(i) \neq i$ , so  $F(i) \not\subseteq K_r$ . It follows that  $F(i)$  and  $K_r$  are linearly disjoint subfields of  $F(\zeta_r)$  with composite field  $F(\zeta_r)$ . Therefore  $\text{Gal}(K_r/F) \simeq \text{Gal}(F(\zeta_r)/F(i))$  is cyclic of order  $2^r$ . The definition of  $K_r$  implies that  $K_r \subseteq K_{r+1}$  for each  $r$ ; hence  $\bigcup_{r=1}^{\infty} K_r$  is a Galois  $J$ -extension of  $F$  and  $\text{Gal}(K/F) \simeq W_2$ .

We note that in the notation of part (a) of the proof of Proposition 3.5, the field  $K_r$  does not contain the  $p$ th roots of unity, but  $K_r(\zeta)$  contains the  $p^{r+k}$ th roots of unity; hence  $\zeta \notin K$ , but  $K(\zeta)$  contains the  $p^r$ th roots of unity for all  $r$ . A similar example for the fourth and  $2^r$ th roots of unity can be obtained from the proof of part (b) of Proposition 3.5.

**PROPOSITION 3.6.** *If  $F$  is a field of positive characteristic and if  $F$  admits a cyclic extension of prime degree  $p$ , then  $F$  admits a Galois  $J$ -extension.*

*Proof.* Let  $E$  be the algebraic closure in  $F$  of the prime subfield of  $F$ . If  $F$  contains the  $p^n$ th roots of unity for all  $n$ , then the result follows from Proposition 3.2. Otherwise,  $E$  is a field as described in Example (E1) of the introduction, so  $E$  admits a Galois  $J$ -extension  $L$ . By Corollary 2.6,  $LF$  is a Galois  $J$ -extension of  $F$ .

Suppose the field  $F$  admits a cyclic extension of prime degree  $p$ . The results of this section leave one case in which we have not given an affirmative answer to Q(1); this is the case where  $\text{char } F = 0$ ,  $F$  does not contain a primitive  $p$ th root of unity  $\zeta$ , but  $F(\zeta)$  contains the  $p^n$ th roots of unity for all  $n$ . In this case it may happen that  $F$  is not real closed and yet does not admit a Galois  $J$ -extension. If  $S$  is the solvable closure of  $Q$ , then  $S$  admits no Galois  $J$ -extension since solvability of field extensions is a transitive property [G1, Cor. 3.9]. Since  $S/Q$  is normal and  $S$  is not contained in the field  $\mathbf{R}$  of real numbers,  $F = S \cap \mathbf{R}$  is a subfield of  $S$  such that  $S/F$  is cyclic of degree two. But Corollary 2.6 implies that  $F$  does not admit a Galois  $J$ -extension. It would be interesting to know

whether a field  $F$  that admits a cyclic extension of degree  $p > 2$  necessarily admits a Galois  $J$ -extension (See the appendix.)

Our next result shows that there exists a finite extension of  $S$  that does admit a Galois  $J$ -extension. Proposition 3.7 will also be useful in proving that a field that is neither algebraically closed nor real closed admits a  $J$ -extension.

**PROPOSITION 3.7.** *If the field  $F$  is imperfect, then  $F$  admits a standard purely inseparable  $J$ -extension. If the separable algebraic closure  $F_s$  of  $F$  is such that  $F_s/F$  is infinite, then there exists a finite separable extension  $E$  of  $F$  such that  $E$  admits a Galois  $J$ -extension.*

*Proof.* If  $F$  is imperfect, then as in example (E2) of the introduction.  $F$  admits a standard purely inseparable  $J$ -extension. If there exists a finite separable algebraic extension of  $F$  of degree over  $F$  divisible by an odd prime  $p$ , then the normal closure of this extension is a finite Galois extension  $K/F$  such that  $p$  divides  $|G|$ , where  $G = \text{Gal}(K/F)$ . Let  $H$  be a subgroup of  $G$  of order  $p$ , and let  $E$  be the fixed field of  $H$  acting on  $K$ . If  $E$  contains a primitive  $p$ th root of unity, then  $E$  admits a Galois  $J$ -extension by Propositions 3.2 and 3.4. Otherwise, let  $E_1 = E(\zeta)$ , where  $\zeta$  is a primitive  $p$ th root of unity. We note that  $KE_1/E_1$  is cyclic of order  $p$  since  $[K:E]$  and  $[E_1:E]$  are relatively prime, and hence the previous case implies that  $E_1$  admits a Galois  $J$ -extension.

The remaining case is where each finite separable algebraic extension of  $F$  is of degree over  $F$  a power of 2. The field  $F(i)$ , where  $i$  is a primitive fourth root of unity, has this same property. Since any group of order  $2^k$  contains a subgroup of index 2, it follows that  $F(i)$  admits a cyclic extension of degree 2, and Propositions 3.2 and 3.4 again show that  $F(i)$  admits a Galois  $J$ -extension. This completes the proof of Proposition 3.7.

We move to a consideration of fields that admit a  $J$ -extension. In this connection, it is useful to note that if  $L/K$  is a  $J$ -extension, then the fields between  $K$  and  $L$  satisfy the descending chain condition (d.c.c.). Moreover, if  $L/F$  is a field extension that is not finitely generated but is such that the fields between  $F$  and  $L$  satisfy d.c.c., then there exists a  $J$ -extension of  $F$  contained in  $L$ . For if  $E$  is an intermediate field such that  $E$  is minimal with respect to the property that  $E/F$  is not finitely generated, then  $E/F$  is a  $J$ -extension.

Concerning d.c.c. on intermediate fields, we note the following easy fact.

LEMMA 3.8. *If  $K/F$  is a finite algebraic field extension and  $L/K$  is a field extension such that the intermediate fields satisfy d.c.c., then the fields between  $F$  and  $L$  also satisfy d.c.c.*

*Proof.* Suppose there exists a strictly descending chain of fields  $E_1 > E_2 > \cdots$  between  $F$  and  $L$ . Since the fields between  $K$  and  $L$  satisfy d.c.c., the chain  $E_1K \supseteq E_2K \supseteq \cdots$  stabilizes, so there exists a positive integer  $n$  such that  $E_nK = E_{n+i}K$  for all  $i \geq 0$ . If  $[K:F] = s$ , then  $[E_iK:E_i] \leq s$  for each  $i$ . But  $[E_n:E_{n+s}] > s$  since the chain  $\{E_i\}$  strictly descends. This gives  $E_{n+s} \subseteq E_n \subseteq E_nK = E_{n+s}K$  with  $[E_{n+s}K:E_{n+s}] \leq s$  and  $[E_n:E_{n+s}] > s$ , a contradiction. We conclude that the fields between  $F$  and  $L$  satisfy d.c.c..

Proposition 3.7 and Lemma 3.8 yield the following general result.

THEOREM 3.9. *If the field  $F$  is neither algebraically closed nor real closed, then  $F$  admits a  $J$ -extension. More precisely, if the separable algebraic closure  $F_s$  of  $F$  is such that  $F_s/F$  is infinite, then  $F$  admits a separable  $J$ -extension. If  $F$  is not perfect, then  $F$  admits a standard purely inseparable  $J$ -extension.*

Theorem 3.9 shows that the class of fields that admit a  $J$ -extension properly contains the class of fields that admit a Galois  $J$ -extension. We record this formally in the following corollary.

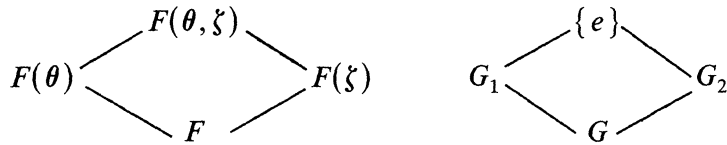
COROLLARY 3.10. *There exist fields  $F$ , such as the solvable closure  $S$  of  $Q$ , that admit a  $J$ -extension but do not admit a Galois  $J$ -extension.*

Theorem 3.9 is genuinely an existence theorem. For a field  $F$  that is the quotient field of a nontrivial valuation domain with principal maximal ideal, we present in Theorem 3.11 a more explicit result and construction.

THEOREM 3.11. *Assume that  $F$  is the quotient field of a nontrivial valuation domain  $V$  with principal maximal ideal  $M = mV$ . Then  $F$  admits a separable  $J$ -extension for which the intermediate fields are linearly ordered with respect to inclusion.*

*Proof.* Choose a prime  $p \neq \text{char}(V/M)$  and a sequence  $\theta_1, \theta_2, \cdots$  of elements in a fixed algebraic closure of  $F$  such that  $\theta_1^p = m$ ,  $\theta_2^p = \theta_1$ ,  $\theta_3^p = \theta_2, \cdots$ . We show that  $K = F(\theta_1, \theta_2, \cdots) = \bigcup_{i=1}^{\infty} F(\theta_i)$  has the desired properties. Separability is no problem; to prove the theorem, it will

suffice to show that the set of subfields of  $F(\theta_n)$  containing  $F$  is linearly ordered for each  $n \in \mathbb{Z}^+$ . Let  $\zeta_n$  be a primitive  $p^n$ th root of unity in an extension field of  $K$ . We show below that (i)  $[F(\theta_n):F] = p^n$ , and (ii)  $F(\theta_n) \cap F(\zeta_n) = F$ . Assuming (i) and (ii) for the moment, we complete the proof of Theorem 3.11. Thus, since  $F(\zeta_n)/F$  is Galois, it follows that  $F(\theta_n)$  and  $F(\zeta_n)$  are linearly disjoint over  $F$ . Write  $\theta$  and  $\zeta$  for  $\theta_n$  and  $\zeta_n$ , and consider the following diagram, where  $G$  denotes the Galois group of  $F(\theta, \zeta)/F$  and  $G_1$  and  $G_2$  are subgroups of  $G$  corresponding to the fields  $F(\theta)$  and  $F(\zeta)$ , respectively.



We have  $|G_2| = p^n = [G:G_1]$ , and  $G = G_1G_2$ , where  $G_2$  is normal in  $G$  and  $G_1 \cap G_2 = \{e\}$ . The subfields of  $F(\theta)$  are in 1-1 order-reversing correspondence with the subgroups of  $G$  containing  $G_1$ , and each such subgroup  $H$  is of the form  $G_1(G_2 \cap H)$ . Since  $G_2$  is cyclic of order  $p^n$ , its subgroups form a chain; hence the subgroups of  $G$  containing  $G_1$  form a chain, and consequently, the subfields of  $F(\theta)$  containing  $F$  are linearly ordered. Since  $[F(\theta_n):F] = p^n$ , where  $\theta_n^{p^n} \in F$ , it follows easily that  $[F(\theta_n^{p^i}):F] = p^{n-i}$  for  $0 \leq i \leq n$ , and hence  $\{F(\theta_n^{p^i})\}_{i=0}^n$  is the set of intermediate fields of  $F(\theta_n)/F$ .

We proceed to establish the equality  $F(\theta) \cap F(\zeta) = F$  in (ii) by showing that  $V$  is totally ramified with respect to  $E$  if  $F \subseteq E \subseteq F(\theta)$ ; in the process, we also prove (i). Let  $v$  be a valuation associated with  $V$  and let  $w_1, \dots, w_g$  be the extensions of  $v$  to  $F(\theta)$ . Let  $e_i$  and  $f_i$ , respectively, denote the reduced ramification index and the relative degree of  $w_i$  with respect to  $v$ . We have  $p^n w_i(\theta) = v(m) > 0$  for each  $i$ , and since  $v(m)$  is the smallest positive element of the value group of  $v$ , it follows that  $\{jw_i(\theta)\}_{j=1}^{p^n}$  is a set of representatives of distinct cosets of the value group of  $v$  in the value group of  $w_i$ . Therefore  $e_i \geq p^n$  for each  $i$ . Since  $\sum_{i=1}^g e_i f_i \leq [F(\theta):F] \leq p^n$  [Ri, p. 228], we conclude that  $g = 1$  and  $e_1 = p^n$ ,  $f_1 = 1$ —that is,  $V$  is totally ramified with respect to  $F(\theta)$  and  $[F(\theta):F] = p^n$ . If  $E$  is a subfield of  $F(\theta)/F$ , then standard techniques and two applications of the inequality cited in the preceding sentences show that  $V$  is totally ramified with respect to  $E$ —that is,  $v$  admits a unique extension  $u$  to  $E$  and the reduced ramification index of  $u$  with respect to  $v$  is  $[E:F]$ . Next we consider the behavior of  $V$  with respect to  $F(\zeta)$ . Since  $p$  is a unit of  $V/M$ , Theorem 10.18 of [N] shows that  $V[\zeta]$  is the integral closure of  $V$  in  $F(\zeta)$ ; thus, each extension of  $V$  to  $F(\zeta)$  is a

quotient ring of the Prüfer domain  $V[\zeta]$ . Then [N, (38.6)] implies that  $V$  is unramified with respect to  $F(\zeta)$ ; this means that for each extension  $(V^*, M^*)$  of  $V$  to  $F(\zeta)$ ,  $V^*/M^*$  is separable over  $V/M$ , and  $V^*$  and  $V$  have the same value group. Since these two properties are obviously inherited by extensions of  $V$  to an intermediate field  $E$ , then  $V$  is unramified with respect to each such field  $E$ . We conclude that  $V$  is both unramified and totally ramified with respect to  $F(\zeta) \cap F(\theta)$ , so  $F(\zeta) \cap F(\theta) = F$  as we wished to prove.

What fields  $F$  are *not* the quotient field of a nontrivial valuation domain  $V$  with principal maximal ideal? A sufficient condition for this to occur is that the equation  $X^n - t = 0$  has a solution in  $F$  for each  $t \in F$  and for infinitely many integers  $n \in \mathbb{Z}^+$ . Thus, if  $\text{char } F = p \neq 0$ , then the hypothesis of Theorem 3.11 implies that  $F$  is imperfect, and hence  $F$  also admits a standard purely inseparable  $J$ -extension. It seems reasonable to ask whether  $F$  is the quotient field of a rank-one discrete valuation domain if  $F$  satisfies the hypothesis of Theorem 3.11. We proceed to show (Example 3.13) that this question has a negative answer. The presentation of Example 3.13 involves the notion of a Henselian domain, defined as follows (see [N, p. 103]). Let  $(D, M)$  be a quasi-local domain with quotient field  $K$ . We say that  $(D, M)$  is *Henselian* and that  $K$  is *Henselian with respect to  $D$*  if the following condition is satisfied. If  $f, g_0, h_0$  are monic polynomials in  $D[X]$  such that  $f \equiv g_0 h_0 \pmod{M[X]}$ , where  $g_0$  and  $h_0$  are relatively prime modulo  $M[X]$ , then there exist monic polynomials  $g, h \in D[X]$  such that  $f = gh$ ,  $g \equiv g_0 \pmod{M[X]}$ , and  $h \equiv h_0 \pmod{M[X]}$ . We use a result (Satz 2.3.11, p. 60) from [BKKN] in Example 3.13. This result, labelled below as Theorem 3.12, is attributed to F. K. Schmidt [S] in [BKKN].

**THEOREM 3.12 (Schmidt).** *If  $(D, M)$  is a Henselian integral domain with quotient field  $K$  and if  $V$  is a rank-one discrete valuation domain on  $K$ , then  $D \subseteq V$ .*

**EXAMPLE 3.13.** We exhibit a field  $L$  that is the quotient field of a valuation domain with principal maximal ideal, but not the quotient field of a rank-one discrete valuation domain. Existence follows from Theorem 3.12 once we give an example of a Henselian valuation domain with principal maximal ideal that is not contained in a rank-one discrete valuation domain of its quotient field. It is easy to construct a valuation domain  $V$  such that  $V$  has principal maximal ideal and  $V$  is not contained

in a rank-one discrete valuation domain of its quotient field. For example, if  $X, Y, Z$  are indeterminates over a field  $k$ , we define a rank-one nondiscrete valuation domain  $W$  on the field  $k(X, Y, Z)$  over  $k(X)$  by defining  $W(Y) = 1$  and  $W(Z) = \sqrt{2}$ . Then  $W = k(X) + N$ , where  $N$  is the maximal ideal of  $W$  [G2, Exer. 12, p. 271]. Therefore  $V = k[X]_{(X)} + N$  is a rank-two valuation domain with the required properties. The Henselization  $V^*$  of  $V$  is a localization of the integral closure  $D$  of  $V$  in a appropriate algebraic extension field  $L$  [N, p. 180]; hence  $D$  is a Prüfer domain and  $V^*$  is a Henselian valuation domain with principal maximal ideal  $M^* = MV^*$  [ibid]. The rank-one valuation overring of  $V^*$  is  $D_P$ , where  $P$  is the rank-one prime of  $D$  contained in  $M^* \cap D$ . Hence  $D_P$  is an extension of  $V$  to  $L$ , and since  $V$  is nondiscrete, so is  $D_P$ .

We remark that the sufficient condition given in Theorem 3.11 for  $F$  to admit a separable  $J$ -extension with linearly ordered intermediate fields is not necessary. This is shown, for example, by the fields of example (E1) of the introduction; other examples can be obtained from Proposition 3.7 or by taking  $F = K(\{X^{1/p^n}\}_{n=1}^\infty)$ , where  $K$  has characteristic  $p \neq 0$  and  $K$  admits a Galois  $J$ -extension.

REMARK 3.14. A field  $F$  that is the quotient field of a rank-one discrete valuation domain need not admit a Galois  $J$ -extension. To see this, let  $\mathbf{R}$  denote the field of real numbers, and let  $F = \mathbf{R}((X))$  be the quotient field of the formal power series ring  $\mathbf{R}[[X]]$ . Then  $f$  does not admit an abelian field extension of degree  $n > 4$ , and hence does not admit a Galois  $J$ -extension. For suppose  $F_n/F$  is an abelian field extension of degree  $n > 4$ , and consider the compositum  $K_n = F_n\mathbf{C}$ , where  $\mathbf{C}$  is the field of complex numbers. Since  $\mathbf{C}((X))/F$  is cyclic of degree 2,  $K_n/F$  is an abelian extension and  $[K_n : \mathbf{C}((X))] = m$ , where  $m = n$  or  $m = n/2$ . By Puiseux's Theorem [Co, p. 418],  $K_n = \mathbf{C}((Y))$ , where  $Y^m = X$ . Therefore  $K_n$  contains the subfield  $\mathbf{R}((Y))$ . But  $\mathbf{R}((Y))/F$  is not Galois for  $m > 2$ , which means that  $K_n/F$  cannot be abelian. We conclude that  $F$  does not admit an abelian extension of degree  $n > 4$ , so by Theorem 2.5,  $F$  does not admit a Galois  $J$ -extension.

**4. Abelian extensions of  $Q$ .** Denote by  $A$  the abelian closure of  $Q$ . This section deals with the same general theme as §3, but is more concrete in nature; to wit, the main result of the section is Corollary 4.11, which states that each subfield  $F$  of  $A$  admits a Galois  $J$ -extension.

To begin, we introduce some notation that will be used throughout this section. For  $n \in \mathbf{Z}^+$ , let  $\zeta_n$  be a primitive  $n$ th root of unity over  $Q$ . Let  $\mathbf{P} = \{p_j\}_{j=0}^\infty$  be the sequence of primes, where  $p_0 = 2$ , and for  $p \in \mathbf{P}$ ,

denote by  $\Delta_p$  the Galois  $J$ -extension of  $Q$  with Galois group  $W_p$  exhibited in Example 2.7. Recall that for  $p$  odd,  $\Delta_p = \bigcup_{j=1}^{\infty} \Delta_{p,j}$ , where  $\Delta_{p,j}$  is the unique subfield of  $Q(\zeta_{p^{j+1}})$  of degree  $p^j$  over  $Q$ , while  $\Delta_2 = \bigcup_{j=1}^{\infty} \Delta_{2,j}$ , where  $\Delta_{2,j}$ , the real subfield of  $Q(\zeta_{2^{j+2}})$ , is cyclic over  $Q$  of degree  $2^j$ . We have  $Q(\zeta_{2^{j+2}}) = \Delta_{2,j}(i)$ , while  $Q(\zeta_{p^{j+1}}) = \Delta_{p,j}(\zeta_p)$ . Hence  $A = \Delta(\zeta_4, \zeta_3, \zeta_5, \dots)$ , where  $\Delta$  is the compositum of the family  $\{\Delta_p \mid p \in \mathbf{P}\}$ .

The first three results of the section are used in the proof of Theorem 4.4.

**LEMMA 4.1.** *Assume that  $F(\alpha, \beta)$  is an abelian extension of the field  $F$  and that  $F(\alpha) \cap F(\beta) = F$ . If  $K$  is a subfield of  $F(\alpha)$  containing  $F$ , then  $[F(\alpha, \beta) : K(\beta)] = [F(\alpha) : K]$ .*

*Proof.* Since  $F(\alpha) \cap F(\beta) = F$ , then  $[F(\alpha, \beta) : F(\beta)] = [F(\alpha) : F]$ . Also,  $K \cap F(\beta) = F$  implies  $[K(\beta) : F(\beta)] = [K : F]$ . Therefore

$$\begin{aligned} [F(\alpha, \beta) : K(\beta)] &= [F(\alpha, \beta) : F(\beta)] / [K(\beta) : F(\beta)] \\ &= [F(\alpha) : F] / [K : F] = [F(\alpha) : K]. \end{aligned}$$

If  $r, s \in \mathbf{Z}^+$  have greatest common divisor  $d$  and least common multiple  $m$ , then  $Q(\zeta_r) \cap Q(\zeta_s) = Q(\zeta_d)$  and  $Q(\zeta_r, \zeta_s) = Q(\zeta_m)$  [C, Th. 1], [L, p. 314]. We use this result in the proof of Lemma 4.2.

**LEMMA 4.2.** *Assume that  $k, n \in \mathbf{Z}^+$  with  $k < n$ , and that  $\{e_j\}_{j=0}^n$  is a subset of  $\mathbf{Z}^+$ . Let*

$$\begin{aligned} r &= 2^{e_0+2} \prod_{j=1}^k p_j^{e_j+1}, & s &= \prod_{k+1}^n p_j^{e_j+1}, \\ t &= 4p_1 \cdots p_k, & u &= p_{k+1} \cdots p_n. \end{aligned}$$

Let  $K_1 = \prod_{j=0}^k \Delta_{p_j, e_j}$ ,  $K_2 = \prod_{j=k+1}^n \Delta_{p_j, e_j}$ , where  $\prod$  denotes compositum, and let  $K = K_1 K_2$  be the compositum of  $K_1$  and  $K_2$ . Then  $[K(\zeta_u, \zeta_t)K(\zeta_u)] = [K_1(\zeta_t) : K] = \phi(t) = [Q(\zeta_t)Q]$ .

*Proof.* We note that  $K_1(\zeta_t) = Q(\zeta_r)$  and  $K_2(\zeta_u) = Q(\zeta_s)$ , where  $Q(\zeta_r) \cap Q(\zeta_s) = Q$ . Since  $K(\zeta_u, \zeta_t)$  is the compositum of  $K_1(\zeta_t)$  and  $K_2(\zeta_u)$  and since  $K(\zeta_u)$  is the compositum of  $K_1$  and  $K_2(\zeta_u)$ , it follows that

$$\begin{aligned} [K(\zeta_u, \zeta_t) : K(\zeta_u)] &= [K(\zeta_u, \zeta_t) : Q] / [K(\zeta_u) : Q] \\ &= [K_1(\zeta_t) : Q][K_2(\zeta_u) : Q] / [K_1 : Q][K_2(\zeta_u) : Q] \\ &= [K_1(\zeta_t) : Q] / [K_1 : Q] = [K_1(\zeta_t) : K_1]. \end{aligned}$$

To see that  $K_1(\Delta_t)$  has degree  $\phi(t)$  over  $K_1$ , note that the equality  $\Delta_{p_j, e_j} \cap (\prod\{\Delta_{p_v, e_v} \mid 0 \leq v \leq k, v \neq j\}) = Q$  (which follows since  $\Delta_{p_j, e_j} \subseteq Q(\zeta_{p_j}^{e_j} + 2)$  for each  $j$ ) implies that  $[K_1 : Q] = \prod_{j=0}^k [\Delta_{p_j, e_j} : Q] = \prod_{j=0}^k p_j^{e_j}$ . Therefore

$$\begin{aligned} [K_1(\zeta_t) : K_1] &= [Q(\zeta_r) : K_1] = [Q(\zeta_r) : Q] / [K_1 : Q] \\ &= \phi(r) / [K_1 : Q] = \phi(t) = [Q(\zeta_t) : Q]. \end{aligned}$$

**COROLLARY 4.3.** *Let  $U = \{4\} \cup \{p_j\}_{j=1}^\infty$ .*

(1) *If  $\{u_j\}_{j=1}^n$  is a finite nonempty subset of  $U$ , if  $u = u_1 u_2 \cdots u_n$ , and if  $V = U \setminus \{u_j\}_{j=1}^n$ , then  $\zeta_u$  has degree  $\phi(u)$  over  $\Delta(\{\zeta_v \mid v \in V\})$ ; hence the minimal polynomial for  $\zeta_u$  over  $\Delta(\{\zeta_v \mid v \in V\})$  is the  $u$ th cyclotomic polynomial  $\Phi_u(X)$ .*

(2) *If  $U = V \cup W$  is a partition of  $U$  into nonempty subsets  $V$  and  $W$ , and if  $V^* = \{\zeta_v \mid v \in V\}$ ,  $W^* = \{\zeta_w \mid w \in W\}$ , then  $\Delta(V^*)$  and  $\Delta(W^*)$  are linearly disjoint over  $\Delta$ .*

*Proof.* In (1), assume first that  $4 \in U$ . The minimal polynomial  $f(X)$  for  $\zeta_u$  over  $\Delta(\{\zeta_v \mid v \in V\})$  has coefficients in a finite extension  $E$  of  $\Delta$  in  $\Delta(\zeta_v)$ . There exists a finite subset  $\{v_j\}_{j=1}^m$  of  $V$  and a set  $\{e_j\}_{j=1}^h$  of positive integers such that  $E \subseteq K(\zeta_w)$ , where  $K$  is the compositum of  $\{\Delta_{p_j, e_j}\}_{j=1}^h$  and  $w = v_1 v_2 \cdots v_m$ . Since the degree of  $\zeta_u$  over  $\Delta(\{\zeta_v\})$  is the same as its degree over any subfield of  $\Delta(\{\zeta_v\})$  containing  $E$ , we assume without loss of generality that  $\{p_j\}_{j=1}^h = \{u_j\}_{j=1}^n \cup \{v_j\}_{j=1}^m$ . Then Lemma 4.2 implies that the degree of  $f(X)$ , which is the degree of  $\zeta_u$  over  $K(\zeta_w)$ , is  $\phi(u)$ , and hence  $f(X) = \Phi(X)$ . If  $4 \notin U$ , let  $F = \Delta(\{\zeta_v \mid v \in V, v \neq 4\})$ . By the case just considered,  $F(\zeta_{4u}) = F(\zeta_4, \zeta_u)$  has degree  $\phi(4u) = 2\phi(u)$  over  $F$  and  $\zeta_4$  has degree 2 over  $F(\zeta_u)$ . Therefore  $\zeta_u$  has degree  $\phi(u)$  over  $F(\zeta_4) = \Delta(\{\zeta_v \mid v \in V\})$ , and again this implies that  $\Phi_u(X)$  is the minimal polynomial for  $\zeta_u$  over  $\Delta(\{\zeta_v\})$ .

(2): If  $V$  is finite, the assertion in (2) follows from (1). Otherwise, let  $V = \{v_j\}_{j=1}^\infty$ . Since  $\Delta(V^*) = \bigcup_{j=1}^\infty \Delta(\zeta_{v_1 \cdots v_j})$  and since  $\Delta(\zeta_{v_1 \cdots v_j}) \cap \Delta(W^*) = \Delta$  for each  $j$ , it follows that  $\Delta(V^*) \cap \Delta(W^*) = \Delta$ —that is,  $\Delta(V^*)$  and  $\Delta(W^*)$  are linearly disjoint over  $\Delta$ .

**THEOREM 4.4.** *Let  $F$  be a proper subfield of  $\Delta$  and let  $L$  be the compositum of the set of Galois  $J$ -extensions of  $F$  in  $A$ . Then  $L = \Delta$ .*

*Proof.* Since  $F < \Delta$ , there exists  $p$  such that  $\Delta_p \not\subseteq F$ . Then  $F\Delta_p \subseteq L$ , and hence  $\Delta_p \subseteq L$  for each  $p$  with  $\Delta_p \not\subseteq F$ . Since the inclusion  $\Delta_p \subseteq L$  is clear if  $\Delta_p \subseteq F$ , we conclude that  $\Delta \subseteq L$ . Suppose that the inclusion is

proper, and let  $E \subseteq A$  be a Galois  $J$ -extension of  $F$  that is not contained in  $\Delta$ . Choose  $\theta \in E \setminus \Delta$ . There exists  $k \in \mathbb{Z}^+$  such that  $\theta \in \Delta(\zeta_u)$ , where  $u = 4p_1 p_2 \cdots p_k$ . Let  $M = \Delta(\{\zeta_{p_j}\}_{j=k+1}^\infty)$ ; part (1) of Corollary 4.3 shows that  $B = M(\zeta_u)$  is Galois over  $F$  of degree  $\phi(u)$ . Since  $\theta \notin M$  by part (2) of Corollary 4.3, it follows that there exists an  $M$ -automorphism  $\sigma$  of  $B$  such that  $\sigma(\theta) \neq \theta$ . Since  $F \subseteq M$  and  $E/F$  is Galois,  $\sigma$  induces an  $F$ -automorphism  $\mu$  of  $E$  such that  $\mu$  has finite order. Since  $E/F$  is a  $J$ -extension, it follows that  $\mu = 1$ , contrary to the fact that  $\mu(\theta) \neq \theta$ . Consequently,  $L \subseteq \Delta$ , equality holds, and this completes the proof of Theorem 4.4.

**COROLLARY 4.5 (Iwasawa [I]).** *The field  $\Delta_p$  is the unique Galois  $J$ -extension of  $Q$  with Galois group  $W_p$ .*

*Proof.* If  $E$  is a Galois  $J$ -extension of  $Q$  with Galois group  $W_p$ , then by Theorem 4.4,  $E \subseteq \{\theta \in \Delta \mid [Q(\theta):Q] \text{ is a power of } p\} = \Delta_p$ . Hence  $\Delta_p = E$  since  $\Delta_p/Q$  is a  $J$ -extension.

We have observed in more than one place that Q(3) fails in general, but Corollary 4.5 shows that this failure occurs on a wide scale. To wit, (4.5) implies that for each prime  $p$ , there exists a unique extension  $E_p$  of  $Q$  such that  $E_p/Q$  is cyclic of degree  $p$  and  $E_p$  can be extended to a Galois  $J$ -extension of  $Q$ .

By a result of Brumer [Br], (4.5) is known to extend to a finite totally real<sup>3</sup> abelian extension  $F$  of  $Q$ —that is,  $F\Delta_p$  is the unique Galois  $J$ -extension of  $F$  with Galois group  $W_p$ . Thus, the phrase “in  $A$ ” in the statement of Theorem 4.4 is redundant if  $[F:Q]$  is finite and  $F$  is totally real<sup>4</sup>. On the other hand, if  $Q \subseteq F < \Delta$  and if  $[F:Q]$  is infinite, then  $F$  may admit a Galois  $J$ -extension that is not contained in  $\Delta$ ; for example, slight modifications of the proofs of (4.8) and (4.9) show that  $\Delta_2$  admits a Galois  $J$ -extension  $E$  with Galois group  $W_2$  such that  $E \not\subseteq \Delta$ .<sup>5</sup>

<sup>3</sup>Recall that a finite algebraic extension  $L$  of  $Q$  is *totally real* if each of the conjugate fields of  $L$  over  $Q$  is real; hence if  $L/Q$  is Galois, then  $L$  is totally real if and only if  $L$  is real.

<sup>4</sup>If  $F$  is a finite abelian extension of  $Q$  that is not totally real, then it is known that  $F$  admits infinitely many  $W_p$ -extensions (see [I, p. 253], [Bm, p. 248]).

<sup>5</sup>In fact, using Remark 4.6, it follows that  $E \not\subseteq A$  for any such field  $E$ .

REMARK 4.6. The proof of Theorem 4.4 shows that each element  $\theta \in A \setminus \Delta$  is moved by an automorphism  $\sigma_\theta$  of  $A$  of finite order; any such  $\sigma_\theta$  induces the identity map on  $\Delta$ . Using this fact and an argument similar to that of (4.4), it can be shown that if  $\Delta \subseteq F \subseteq A$ , then  $F$  admits no Galois  $J$ -extension within  $A$ . On the other hand, Corollary 4.11 shows that  $F$  admits a Galois  $J$ -extension.

REMARK 4.7. For each  $n \in \mathbb{Z}^+$ , there exists a unique extension  $\Sigma_n$  of  $Q$  in  $\Delta$  such that  $[\Sigma_n : A] = n$ . Specifically, if  $n > 1$  and  $n = \prod_{j=1}^k p_j^{e_j}$  is the prime factorization of  $n$ , then  $\Sigma_n$  is the composite of the fields  $\Delta_{p_j, e_j}$ , for  $1 \leq j \leq k$ . For the sake of future reference, we note that  $\Sigma_2 = Q(\sqrt{2})$  and  $\Sigma_3 = Q(\zeta_9 + \zeta_9^{-1})$ ; thus,  $\Sigma_3$  is the splitting field over  $Q$  of the polynomial  $X^3 - 3X + 1$ .

We turn to a proof of the result that each subfield of  $A$  admits a Galois  $J$ -extension. The proof is obtained by showing (Corollary 4.10) that  $\Delta$  admits a Galois  $J$ -extension with Galois group  $W_2$ .

THEOREM 4.8. *If there exist  $a \in \Delta$ ,  $|a| < 1$ , such that  $\sqrt{(1 - a^2)} \in \Delta$  and the polynomial  $s_n(X) = X^{2^n} - 2aX^{2^{n-1}} + 1$  is irreducible over  $\Delta$  for each  $n \in \mathbb{Z}^+$ , then  $\Delta$  admits a Galois  $J$ -extension with Galois group  $W_2$ .*

*Proof.* Choose elements  $\beta, \theta_1, \theta_2, \dots$  so that  $\beta = a + i\sqrt{(1 - a^2)}$  is a root of  $s_1(X)$ ,  $\theta_1 = \sqrt{\beta}$ , and  $\theta_{n+1} = \sqrt{\theta_n}$  for each  $n \in \mathbb{Z}^+$ . We show for each  $n$  that (1)  $\Delta(\theta_n) = \Delta(\theta_n, i)$  is Galois over  $\Delta$  with Galois group  $Z_2 \times Z_{2^n}$ , (2)  $\Delta(\theta_n + \theta_n^{-1})$  is a subfield of  $\Delta(\theta_n)$  that is cyclic over  $\Delta$  of degree  $2^n$ , and (3)  $\Delta(\theta_n + \theta_n^{-1}) \subseteq \Delta(\theta_{n+1} + \theta_{n+1}^{-1})$ . Once these statements have been proved, it then follows that  $\bigcup_{n=1}^\infty \Delta(\theta_n + \theta_n^{-1})$  is a Galois  $J$ -extension of  $\Delta$  with Galois group  $W_2$ . The assertion in (3) follows at once from the equality  $\theta_n + \theta_n^{-1} = (\theta_{n+1} + \theta_{n+1}^{-1})^2 - 2$ . To prove (1), fix  $n$  and write  $\theta$  in place of  $\theta_n$ . Since  $\theta$  is a root of  $s_{n+1}(X)$ , it has degree  $2^{n+1}$  over  $\Delta$ . Also,  $\theta^{2^n} = \beta$ , so  $\Delta(\beta) = \Delta(i)$  is a subfield of  $\Delta(\beta)$ , and  $\Delta(i)$  contains the  $2^k$ th roots of unity for all  $k$ ; in particular,  $\Delta(i)$  contains a primitive  $2^n$ th root of unity  $\zeta$ . Since  $\theta$  has degree  $2^n$  over  $\Delta(i)$ , it follows that  $\{\zeta^j \theta\}_{j=0}^{2^n-1}$  is the set of conjugates of  $\theta$  over  $\Delta(i)$ ; hence  $\{\zeta^j \theta\}_{j=0}^{2^n-1}$  is a set of  $2^n$  conjugates of  $\theta$  over  $\Delta$ . What are the other  $2^n$  conjugates of  $\theta$  over  $\Delta$ ? To answer this question, let  $G$  be the galois group of  $s_{n+1}(X)$  over  $\Delta$ . There exists  $\sigma \in G$  such that  $\sigma(i) = -i$ ; thus  $\sigma(\theta^{2^n}) = \sigma(\beta) = \bar{\beta} = [\sigma(\theta)]^{2^n} = \beta^{-1}$ . Since  $(\theta^{-1})^{2^n} = \beta^{-1}$ , it follows that the other  $2^n$  conjugates of  $\theta$  over  $\Delta$  are the elements  $\zeta^j \theta^{-1}$  for  $0 \leq j \leq 2^n - 1$ . Consequently,  $\Delta(\theta)/\Delta$  is normal. An element of  $G$  is completely determined by its

action on  $\theta$ ; hence  $G = \{\sigma_i\}_{i=0}^{2^n-1} \cup \{\tau_j\}_{j=0}^{2^n-1}$ , where  $\sigma_j(\theta) = \zeta^j\theta$  and  $\tau_j(\theta) = \zeta^j\theta^{-1}$ . We note  $\sigma_j(\theta^{2^n}) = (\zeta^j\theta)^{2^n} = \theta^{2^n}$  and  $\tau_j(\theta^{2^n}) = \theta^{-2^n}$ , the complex conjugate of  $\theta^{2^n}$ . It follows that  $\sigma_j$  induces the identity automorphism on  $\Delta(i)$  and  $\tau_j$  restricted to  $\Delta(i)$  is complex conjugation on this field. In particular,  $\sigma_j(\zeta^j) = \zeta^j$  and  $\tau_j(\zeta^j) = \zeta^{-j}$ . It is then straightforward to show that  $\sigma_j^k(\theta) = \zeta^{jk}\theta$  and  $\tau_j^{2^k}(\theta) = \zeta^{-j2^k}\theta$  for each  $k \in \mathbb{Z}^+$  and that  $G$  is abelian. In particular, the order of  $\sigma_j$  and of  $\tau_j$  is the additive order of  $j$  in the group  $\mathbb{Z}/2^n\mathbb{Z}$ . Hence  $G$  contains elements, such as  $\sigma_1$ , of order  $2^n$ , but no element of order  $2^{n+1}$ . It follows that  $G \simeq \mathbb{Z}_{2^n} \times \mathbb{Z}_2$ , and in fact,  $G = \langle \sigma_1 \rangle \times \langle \tau_0 \rangle$ , where  $\tau_0(\theta) = \theta^{-1}$ . This completes the proof of (1).

Continuing the notation of the preceding paragraph, it is clear that  $\Delta(\theta + \theta^{-1})$  is contained in the fixed subfield of  $\tau_0$ . On the other hand,  $\theta$  satisfies the quadratic polynomial  $X^2 - (\theta + \theta^{-1})X + 1$  over  $\Delta(\theta + \theta^{-1})$ , and consequently,  $\Delta(\theta + \theta^{-1})$  is the fixed field of  $\tau_0$ . Therefore, the Galois group of  $\Delta(\theta + \theta^{-1})$  over  $\Delta$  is isomorphic to  $(\langle \sigma_1 \rangle \times \langle \tau_0 \rangle) / \langle \tau_0 \rangle \simeq \langle \sigma_1 \rangle$ —that is,  $\Delta(\theta + \theta^{-1})$  is cyclic over  $\Delta$  of degree  $2^n$ , as asserted in (2).

**PROPOSITION 4.9.** *The polynomial  $t_n(X) = X^{2^n} - (8/5)X^{2^{n-1}} + 1$  is irreducible over the field  $\Delta$  for each  $n \in \mathbb{Z}^+$ .*

*Proof.* The roots of  $t_1(X)$  are  $\beta = (4 + 3i)/5$  and  $\bar{\beta} = \beta^{-1} = (4 - 3i)/5$ . Since  $\Delta$  is a real field, it follows that  $t_1$  is irreducible over  $\Delta$ . Let  $\theta = \sqrt{\beta}$ . The roots of  $t_2(X)$  are  $\pm\theta$  and  $\pm\theta^{-1}$ . We show that  $\theta \notin \Delta(\beta) = \Delta(i)$ ; this will imply that  $\Delta(\theta) = \Delta(i, \theta)$  has degree 4 over  $\Delta$ , and hence  $t_2(X)$  is irreducible over  $\Delta$ . Note that  $(\theta + \theta^{-1})^2 = \theta^2 + 2 + \theta^{-2} = 18/5$ , and hence  $\sqrt{10} \in Q(\theta)$ . Thus, if  $\theta \in \Delta(i)$ , then  $\sqrt{10} \in \Delta(i)$ . On the other hand, Remark 4.7 shows that  $Q(\sqrt{2})$  is the unique quadratic extension of  $Q$  in  $\Delta$ , so  $\sqrt{10} \notin \Delta$  and  $\Delta(i) = \Delta(\sqrt{10})$ ; this is a contradiction, for  $\Delta(\sqrt{10})$  is a real field.

We have shown that  $X^2 - \beta$  is irreducible over  $\Delta(i)$ , and hence the Vahlen-Capelli Theorem implies that  $X^{2^n} - \beta$  is irreducible over  $\Delta(i)$  for each  $n \in \mathbb{Z}^+$ . If  $\theta_n$  is a root of  $X^{2^n} - \beta$ , then  $\theta_n$  is also a root of  $t_{n+1}(X)$  and  $\Delta(\theta_n) = \Delta(i, \theta_n)$  has degree  $2^{n+1}$  over  $\Delta$ , so  $t_{n+1}$  is irreducible, as asserted.

**COROLLARY 4.10.** *The field  $\Delta$  admits a Galois  $J$ -extension with Galois group  $W_2$ .*

*Proof.* Apply (4.8) and (4.9).

**COROLLARY 4.11.** *Each subfield  $F$  of the abelian closure  $A$  of  $Q$  admits a Galois  $J$ -extension.*

*Proof.* If there exists a Galois  $J$ -extension  $K$  of  $Q$  such that  $K \not\subseteq F$ , then  $FK$  is a Galois  $J$ -extension of  $F$ . On the other hand, if  $F$  contains each Galois  $J$ -extension of  $Q$ , then  $\Delta \subseteq F$ . Let  $M$  be a Galois  $J$ -extension of  $\Delta$ ; existence is assured by Corollary 4.10. Remark 4.6 shows that  $M \not\subseteq A$ , and hence  $M \not\subseteq F$  as well. Consequently,  $FM$  is a Galois  $J$ -extension of  $F$ .

Using the description of the unique cubic extension  $\Sigma_3$  of  $Q$  in  $\Delta$  given in Remark 4.7, we have been able to prove that  $W_3$  can be realized as a Galois group over  $\Delta$ . In fact, if  $\beta$  is a root of  $X^2 - (2/7)X + 1$  and if  $\theta_1, \theta_2, \dots$  are chosen so that  $\theta_1 = \beta^{1/3}$ ,  $\theta_2 = \theta_1^{1/3}, \dots$ , then  $\bigcup_{j=1}^{\infty} \Delta(\theta_j + \theta_j^{-1})$  is a Galois  $J$ -extension of  $\Delta$  with Galois group  $W_3$ . For  $p > 3$ , we have been unable to determine whether  $W_p$  can be realized as a Galois group over  $\Delta$ . Since  $\Delta$  does admit a cyclic extension of degree  $p^k$  for each  $k \in \mathbb{Z}^+$ , the field  $F = \Delta$  represents a test case for  $Q(2)$ . (See the appendix.)

**5. Concluding remarks.** We conclude with some remarks concerning two open questions that seem to merit further study. The first question concerns the restriction to the case of algebraic extensions in the definition of a  $J$ -extension. To wit, if  $K$  is an extension field of  $F$ , then consider the following condition ( $\#$ ):  $K$  is not finitely generated as an extension field of  $F$ , but  $E/F$  is finitely generated over  $F$  for each proper intermediate field  $E$ . If  $K/F$  is algebraic, then a ( $\#$ )-extension is the same as a  $J$ -extension, but we have been unable to determine whether a ( $\#$ )-extension is necessarily algebraic. If not, then it is straightforward to show that there exists a ( $\#$ )-extension  $K/F$  of transcendence degree 1 with  $F$  algebraically closed in  $K$ . In this case,  $K/F(t)$  is a  $J$ -extension for each  $t \in K \setminus F$ ; moreover, either (1)  $[K:F(t)]_s = \infty$  for each  $t \in K \setminus F$ , or else (2)  $[K:F(t)]_i = \infty$  for each  $t \in K \setminus F$ . Condition (1) leads to a contradiction in the case where  $\text{char } F \neq 0$ , and (2) is impossible in the case where  $\text{char } F \neq 0$  and  $F$  is perfect. Beyond this, we have no additional information.

The second question is the case of  $Q(2)$ , §3, where  $p$  is odd: if  $F$  admits a cyclic extension of degree  $p$ , can  $W_p$  be realized as a Galois group over  $F$ ? While the corresponding case of  $Q(3)$  has a negative answer, the answer to  $Q(2)$  has been shown to be “yes” except possibly in the case where  $\text{char } F = 0$ ,  $\zeta_p \notin F$ , and  $F(\zeta_p)$  contains the  $p$ ’th roots of

unity for all  $n$ . As mentioned in §4, the case where  $F = \Delta$  and  $p > 3$  is one test case for this second question. (See the appendix.)

## REFERENCES

- [A1] A. A. Albert, *Cyclic fields of degree  $p^n$  over  $F$  of characteristic  $p$* , Bull. Amer. Math. Soc., **40** (1934), 625–631.
- [A2] ———, *On cyclic fields*, Trans. Amer. Math. Soc., **37** (1935), 454–462.
- [A3] ———, *Modern Higher Algebra*, Univ. Chicago Press, Chicago, 1937.
- [AS] E. Artin and O. Schreier, *Eine Kennzeichnung der reell abgeschlossenen Körper*, Abh. Math. Sem. Univ. Hamburg, **5** (1927), 225–231.
- [Ba] J. Bastida, *Field Extensions and Galois Theory*, Encyclopedia of Mathematics and Its Applications, Vol. 22, Addison-Wesley, Reading, Mass., 1984.
- [BKKN] R. Berger, R. Kiehl, E. Kunz, and J.-J. Nastold, *Differentialrechnung In Der Analytischen Geometrie*, Lecture Notes Math., Vol. 38, Springer-Verlag, New York, 1967.
- [Bm] J. Bloom, *On the invariants of some  $Z_p$ -extensions*, J. Number Theory, **11** (1979), 239–256.
- [Bol] N. Bourbaki, *Algèbre*, Chap. V, Corps Commutative, Masson, Paris, 1981.
- [Bo2] ———, *Commutative Algebra*, Addison-Wesley, Reading, Mass., 1972.
- [Br] A. Brumer, *On the units of algebraic number fields*, Mathematika, **14** (1967), 121–124.
- [C] R. Chalkley, *A lattice of cyclotomic fields*, Math. Mag., **48** (1975), 42–44.
- [CK] C. C. Chang and H. J. Keisler, *Model Theory*, North-Holland, Amsterdam, 1973.
- [Co] Ian Connell, *Modern Algebra A Constructive Introduction*, North Holland, New York, 1982.
- [D] R. A. Dean, *A rational polynomial whose group is the quaternions*, Amer. Math. Monthly, **88** (1981), 42–45.
- [De] J. K. Deveney,  *$\omega_0$ -generated field extensions*, Arch. d. Math., (to appear).
- [DD] J. Diller and A. Dress, *Zur Galoisstheorie Pythagorischer Körper*, Arch. Math., **16** (1965), 148–152.
- [FM] M. D. Fried and R. E. MacRae, *On the invariance of chains of fields*, Illinois J. Math., **13** (1969), 165–171.
- [F] L. Fuchs, *Infinite Abelian Groups*, Vol. I, Academic Press, New York, 1970.
- [G1] R. Gilmer, *On solvability by radicals of field extensions*, Math. Ann., **199** (1972), 263–277.
- [G2] ———, *Multiplicative Ideal Theory*, Marcel Dekker, New York, 1972.
- [GH] R. Gilmer and W. Heinzer, *Cardinality of generating sets for modules over a commutative ring*, Math. Scand., **52** (1983), 41–57.
- [H] T. W. Hungerford, *Algebra*, Springer-Verlag, New York, 1980.
- [I] K. Iwasawa, *On  $Z_r$ -extensions of algebraic number fields*, Ann. Math., **98** (1973), 246–326.
- [J] N. Jacobson, *Lectures in Abstract Algebra, Vol. III, Theory of Fields and Galois Theory*, Springer-Verlag, New York, 1981.
- [K] I. Kaplansky, *Fields and Rings*, Univ. Chicago Press, Chicago, 1972.
- [L] S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1984.
- [N] M. Nagata, *Local Rings*, Wiley Interscience, New York, 1962.
- [Q] F. Quigley, *Maximal subfields of an algebraically closed field not containing a given element*, Proc. Amer. Math. Soc., **13** (1962), 562–566.
- [Re] J. D. Reid, *A note on inseparability*, Michigan Math. J., **13** (1966), 219–223.

- [Ri] P. Ribenboim, *Theorie des Valuations*, Presses Univ. Montreal, Montreal, 1965.
- [Ro] J. J. Rotman, *An Introduction to the Theory of Groups*, Third edition, Allyn and Bacon, Boston, 1984.
- [S] F. K. Schmidt, *Mehrfach perfekte Korper*, Math. Ann., **108** (1933), 1–25.
- [vdW] B. L. van der Waerden, *Algebra*, Vol. I, Frederick Ungar, New York, 1970.
- [Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.
- [Wn] M. Weinstein, *Examples of Groups*, Polygonal Publ. House, Passaic, N. J., 1977.
- [ZS] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. I, Springer-Verlag, New York, 1975.

APPENDIX

Professor David Saltman has informed us that  $Q(2)$  has an affirmative answer for an odd prime  $p$ , and this may have been previously known. The argument given below was supplied by him.

**THEOREM 1.** *If  $p$  is an odd prime and if the field  $F$  admits a cyclic extension of degree  $p$ , then  $W_p$  can be realized as a Galois group over  $F$ . If  $F$  admits a cyclic extension of degree 4, then  $W_2$  can be realized as a Galois group over  $F$ .*

*Proof.* We begin with some general comments. Let  $F$  be any field and  $G = \text{Gal}(F_s/F)$  the Galois group of  $F$  in its separable closure. The character group  $\chi(F)$  is the group of continuous homomorphisms  $\text{Hom}_c(G, Q/Z)$ , where  $Q$  is the additive group of the rational field and  $Z$  is the subgroup of integers.  $Q/Z$  is supplied with the discrete topology. Let  $\chi(F)_p$  be the  $p$ -primary component of  $\chi(F)$ . If  $f: G \rightarrow Q/Z$  is in  $\chi(F)$ , then  $f^{-1}(0)$  is open in  $G$ , so  $f(G)$  is finite. But all finite subgroups of  $Q/Z$  are cyclic, so if  $N$  is the kernel of  $f$ , then  $G/N$  is cyclic of order, say,  $n$  and  $f^{-1}(1/n + Z) = \sigma N$  is a generator of  $G/N$ . Conversely, if  $L/F$  is cyclic of degree  $n$  and  $\tau$  generates  $\text{Gal}(L/F)$ , set  $N = \text{Gal}(F_s/L) \subseteq G$ .  $N$  is normal in  $G$  and  $G/N = \text{Gal}(L/F)$ . Viewed in  $G/N$ , let  $\tau$  be  $\sigma N$ . Define  $f: G \rightarrow Q/Z$  by setting  $f(\eta) = i/n + Z$  if  $\eta \in \sigma^i N$ . It is not hard to see that  $f \in \chi(F)$ . In this way we have a bijection between  $\chi(F)$  and pairs  $(L/F, \tau)$ , where  $L/F$  is cyclic and  $\tau$  generates the Galois group of  $L/F$ . Note that in this correspondence, the order of  $f$  is the degree of  $L/F$ . The following lemma is the way we find  $W_p$ -extensions.

**LEMMA.** *Suppose  $f \in \chi(F)_p$  and that  $f$  corresponds to  $(L/F, \tau)$ . Then  $L/F$  embeds in a  $W_p$ -extension if and only if  $f$  is in a divisible subgroup of  $\chi(F)_p$ .*

*Proof.* Let  $f, (L/F, \tau)$  be as above, assume that  $L/F$  has degree  $q$ , and let  $L \subseteq L'$ , where  $L'/F$  is a  $W_p$ -extension. Then there are  $L \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L'$  such that  $L_i/F$  is cyclic of degree  $qp^i$ . Furthermore,  $\text{Gal}(L'/F)$  has a topological generator  $\sigma$  such that  $\sigma$  restricted to  $L$  is  $\tau$ . Let  $\tau_i$  be the restriction of  $\sigma$  to  $L_i$ . Define  $f_i \in \chi(F)_p$  to be the character associated with  $(L_i/F, \tau_i)$ . Then  $p^i f_i = f$  for all  $i$ . That is,  $f$  is in a divisible subgroup of  $\chi(F)_p$ .

Conversely, suppose  $f$  is in a divisible subgroup of  $\chi(F)_p$ . Then there are  $f_i \in \chi(F)_p$  such that  $pf_{i+1} = f_i$  and  $pf_1 = f$ . Then  $L_i \subseteq L_{i+1}$  and the restriction of  $\tau_{i+1}$  to  $L_i$  is  $\tau_i$ . If  $L' = \bigcup L_i$ , then  $L'/F$  is a  $W_p$ -extension. This proves the lemma.

We require one more general observation. Let  $F, G$  be as above and let  $H \subseteq G$  be a subgroup of finite index  $m$ . The restriction map defines a homomorphism  $\text{res}: \text{Hom}_c(G, Q/Z) \rightarrow \text{Hom}_c(H, Q/Z)$ . On the other hand, if we supply  $Q/Z$  with the trivial  $G$ - (and hence  $H$ -) action, then  $\text{Hom}_c(G, Q/Z) = H^1(G, Q/Z)$  and  $\text{Hom}_c(H, Q/Z) = H^1(H, Q/Z)$ . By, for example, [1, p. 82], there is a corestriction homomorphism  $\text{cor}: \text{Hom}_c(H, Q/Z) \rightarrow \text{Hom}_c(G, Q/Z)$  such that the composition  $(\text{cor})(\text{res})$  is just multiplication by  $m$ . Using our definition of  $\chi(F)_p$ , we have that if  $F'/F$  is a separable extension of degree  $m$ , there are maps  $\text{res}: \chi(F')_p \rightarrow \chi(F)_p$  and  $\text{cor}: \chi(F)_p \rightarrow \chi(F')_p$  such that  $(\text{cor})(\text{res})$  is multiplication by  $m$ .

We are ready to prove the theorem. Let  $F$  be a field with a cyclic extension  $L/F$  of degree  $q$ , where  $q = p$  if  $p$  is odd and  $q = 4$  if  $p$  is 2. Assume that  $F$  has no  $W_p$ -extension. Let  $F'$  be the field gotten by adjoining all  $p^s$  roots of one to  $F$ . Let the group  $U$  be cyclic of order  $p - 1$  if  $p$  is odd and cyclic of order 2 if  $p$  is 2. Then  $\text{Gal}(F'/F) \cong U' \oplus B$ , where  $U'$  is a subgroup of  $U$  and  $B$  is either  $(0)$  or  $W_p$ . Since  $F$  has no  $W_p$ -extensions,  $B = (0)$  and  $F'/F$  is finite of degree  $m$ , where  $m$  is prime to  $p$  if  $p$  is odd and  $m$  is 1 or 2 if  $p$  is 2. Over  $F'$ , all cyclic  $p$ -extensions can be embedded in a  $W_p$ -extension. Thus  $\chi(F')_p$  is divisible. If  $p$  is odd, the fact that  $(\text{cor})(\text{res})$  is multiplication by an integer prime to  $p$  implies that  $\text{cor}: \chi(F')_p \rightarrow \chi(F)_p$  is a surjection. Thus  $\chi(F)_p$  is nonzero and divisible. This case is done by the lemma. If  $p$  is 2, let  $f$  be a character associated with  $L/F$ , so  $f \in \chi(F)_2$  has order 4.  $\text{cor}(\text{res}(f)) = f$  or  $2f$ , which are not 0. Thus  $\text{cor}(\chi(F')_p)$  is a nonzero divisible subgroup of  $\chi(F)_p$ , and we are again done by the lemma. Thus the theorem is proved.

[1] K. Brown, *Cohomology of Groups*, Springer-Verlag, New York and Berlin 1982.

Professor David Leep has pointed out to us some consequences of Theorem 1 that we proceed to record below as Theorems 2–4. The first of these theorems is related to Q(3).

**THEOREM 2.** *Assume that  $F$  is a field and  $p$  is prime. Denote by  $\zeta$  either a primitive  $p$ th root of unity, for  $p$  odd, or a primitive fourth root of unity if  $p = 2$ . Assume that  $F(\zeta)$  contains the  $p^n$ th roots of unity for all  $n$ , and that  $K/F$  is cyclic of degree  $p$ .*

- (1) *If  $p$  is odd,  $K$  can be extended to a Galois  $J$ -extension of  $F$ .*
- (2) *If  $p = 2$ , then  $K$  can be extended to a Galois  $J$ -extension of  $F$  if and only if  $K$  can be extended to a cyclic extension of  $F$  of degree 4.*

*Proof.* The proof of Theorem 2 is essentially contained in the proof of Theorem 1. In fact, in the notation of that proof, the hypothesis on  $F$  implies that for  $p$  even or odd,  $B = (0)$ . Thus, (1) follows exactly as in the proof of Theorem 1. In (2), let  $L$  be an extension field of  $K$  such that  $L/F$  is cyclic of degree 4. If  $f$  is the character associated with  $L/F$ , the proof of Theorem 1 shows that either  $f$  or  $2f$  belongs to a nonzero divisible subgroup of  $\chi(F)_p$ , and hence in either case  $2f$ , the character associated with  $K/F$ , belongs to such a subgroup. Hence  $K/F$  can be extended to a Galois  $J$ -extension of  $F$ , as asserted.

Another consequence of Theorem 1 is a result which represents a stronger form of Corollary 4.11.

**THEOREM 3.** *Each subfield  $F$  of  $A$  admits a Galois  $J$ -extension with Galois group  $W_p$  for each prime  $p$ .*

*Proof.* Fix  $p$ . If  $\Delta_p \not\subseteq F$ , then  $F\Delta_p/F$  is Galois with Galois group  $W_p$ . Suppose  $\Delta_p \subseteq F$ . We show first that  $\Delta_p$  admits a Galois  $J$ -extension with Galois group  $W_p$ . To do so, it suffices, in view of Theorem 1, to show that  $\Delta_p$  admits a cyclic extension of degree  $p^2$ . This is easy to do: take  $q$  prime such that  $q \equiv 1 \pmod{p^2}$ . If  $\zeta$  is a primitive  $q$ th root of unity then  $\Delta_p(\zeta)/\Delta_p$  is cyclic of degree  $q - 1$ , and hence  $\Delta_p(\zeta)$  contains a subfield that is cyclic over  $\Delta_p$  of degree  $p^2$ . Let  $K$  be a  $W_p$ -extension of  $\Delta_p$ . Since no element of  $\Delta$  has degree  $p$  over  $\Delta_p$ , it follows that  $K \not\subseteq \Delta$ , and hence  $\Delta K/\Delta$  is also a  $J$ -extension. Remark 4.6 then implies that  $\Delta K \not\subseteq A$ ; hence  $K \not\subseteq A$ ,  $K \not\subseteq F$ , and  $FK$  is a Galois  $J$ -extension of  $F$  with Galois group  $W_p$ .

In relation to part (2) of Theorem 2, we remark that even under the hypothesis of that result, it need not be true that a cyclic extension  $K/F$

of degree 4 can be extended to a Galois  $J$ -extension of  $F$ . (Thus, if  $2f$  belongs to a divisible subgroup of  $\chi(F)_2$ ,  $f$  itself need not belong to such a subgroup.) For example, let  $F = \Delta_2$ . If  $\zeta$  is a primitive fourth root of unity over  $F$ , then  $F(\zeta)$  contains the  $2^n$ th roots of unity for all  $n$ . If  $\mu$  is a primitive fifth root of unity over  $F$ , then  $F(\mu)/F$  is cyclic of degree 4, and the unique subfield  $E = F(\cos 2\pi/5)$  of  $F(\mu)$  of degree 2 over  $F$  is a subfield of the reals. We claim that  $F(\mu)$  cannot be extended to a field  $L$  that is cyclic over  $F$  of degree 8. We argue by contradiction. If such a field  $L$  exists, then  $L/E$  is cyclic of degree 4, and it is known that this implies that the intermediate field  $F(\mu)$  is of the form  $E(\sqrt{t})$ , where  $t$  is the sum of two squares in  $E$  [A3, Exer. 1, p. 208], [D, p. 43]. This leads to the contradiction that  $F(\mu) = E(\sqrt{t})$  is a subfield of the reals. Therefore  $K/F$  cannot be extended to a  $J$ -extension of  $F$ .

Finally, Leep pointed out to us that the following known result (\*) which is included in Satz 1 of [DD], yields a more complete answer to Q(2) than that provided by Theorem 1. In the statement of (\*), recall that a field  $F$  is *Pythagorean* if each sum of squares in  $F$  is a square in  $F$ .

(\*) *If  $F$  admits a cyclic extension of degree 2, then  $F$  fails to admit a cyclic extension of degree 4 if and only if  $\text{char } F \neq 2$  and  $F$  is Pythagorean.*

Theorem 4 follows immediately from Theorem 1 and (\*).

**THEOREM 4.** *If  $F$  admits a cyclic extension of degree 2, then  $W_2$  can be realized as a Galois group over  $F$  unless  $\text{char } F \neq 2$  and  $F$  is Pythagorean.*

*Added in proof.* We have learned that Theorem 2 of the paper *Algebraic extensions of arbitrary fields*, Duke Math. J., **24** (1957), 201–204, by G. Whaples, also answers (Q1) and (Q2). Propositions 3.2, 3.4 and 3.5, as well as Theorems 1, 2 and 4 of the Appendix, can be obtained from Whaples' theorem and its proof.

Received November 6, 1985. The first author's research was supported by NSF Grant DMS-8501003 and the second author by NSF Grant DMS-8320558.

FLORIDA STATE UNIVERSITY  
TALLAHASSEE, FL 32306

AND

PURDUE UNIVERSITY  
W. LAFAYETTE, IN 47907

# PACIFIC JOURNAL OF MATHEMATICS

## EDITORS

V. S. VARADARAJAN  
(Managing Editor)  
University of California  
Los Angeles, CA 90024  
HERBERT CLEMENS  
University of Utah  
Salt Lake City, UT 84112  
R. FINN  
Stanford University  
Stanford, CA 94305

HERMANN FLASCHKA  
University of Arizona  
Tucson, AZ 85721  
RAMESH A. GANGOLLI  
University of Washington  
Seattle, WA 98195  
VAUGHAN F. R. JONES  
University of California  
Berkeley, CA 94720  
ROBION KIRBY  
University of California  
Berkeley, CA 94720

C. C. MOORE  
University of California  
Berkeley, CA 94720  
H. SAMELSON  
Stanford University  
Stanford, CA 94305  
HAROLD STARK  
University of California, San Diego  
La Jolla, CA 92093

## ASSOCIATE EDITORS

R. ARENS      E. F. BECKENBACH      B. H. NEUMANN      F. WOLF      K. YOSHIDA  
(1906–1982)

## SUPPORTING INSTITUTIONS

UNIVERSITY OF ARIZONA  
UNIVERSITY OF BRITISH COLUMBIA  
CALIFORNIA INSTITUTE OF TECHNOLOGY  
UNIVERSITY OF CALIFORNIA  
MONTANA STATE UNIVERSITY  
UNIVERSITY OF NEVADA, RENO  
NEW MEXICO STATE UNIVERSITY  
OREGON STATE UNIVERSITY

UNIVERSITY OF OREGON  
UNIVERSITY OF SOUTHERN CALIFORNIA  
STANFORD UNIVERSITY  
UNIVERSITY OF HAWAII  
UNIVERSITY OF TOKYO  
UNIVERSITY OF UTAH  
WASHINGTON STATE UNIVERSITY  
UNIVERSITY OF WASHINGTON

# Pacific Journal of Mathematics

Vol. 128, No. 1

March, 1987

<b>Anthony Peter Bahri and Peter Gilkey</b> , The eta invariant, $\text{Pin}^c$ bordism, and equivariant $\text{Spin}^c$ bordism for cyclic 2-groups .....	1
<b>Friedrich-Wilhelm Bauer</b> , Extensions of generalized homology theories .....	25
<b>Marilyn Breen</b> , A characterization theorem for compact unions of two starshaped sets in $R^3$ .....	63
<b>Boniface Ihemotuonye Eke</b> , Special generating sets of purely inseparable extension fields of unbounded exponent .....	73
<b>Robert William Gilmer, Jr. and William James Heinzer</b> , Jónsson $\omega_0$ -generated algebraic field extensions .....	81
<b>Guido Lupacciolu</b> , Holomorphic continuation in several complex variables .....	117
<b>Douglas C. McMahon, Jaap C. S. P. van der Woude and Ta-Sun Wu</b> , Connectedness related to almost periodicity of compositions of flow homomorphisms .....	127
<b>Sophocles Mercourakis</b> , Some characterizations of analytic metric spaces .....	149
<b>Peter Frederick Stiller</b> , The Picard numbers of elliptic surfaces with many symmetries .....	157
<b>David J. Winter</b> , Reducible complements of Lie algebra radicals .....	191
<b>Rade Živaljević</b> , On a cohomology theory based on hyperfinite sums of microsimplexes .....	201