Canad. Math. Bull. Vol. **37** (1), 1994 pp. 133–139

THE NORMAL CLOSURES OF CERTAIN KUMMER EXTENSIONS

WILLIAM C. WATERHOUSE

ABSTRACT. Let F be a field containing a primitive p-th root of unity, let K/F be a cyclic extension with group $\langle\sigma\rangle$ of order p^n, and choose a in K. This paper shows how the Galois group of the normal closure of $K(a^{1/p})$ over F can be determined by computations within K. The key is to define a sequence by applying the operation $x \longmapsto \sigma(x)/x$ repeatedly to a. The first appearance of a p-th power determines the degree of the extension and restricts the Galois group to one or two possibilities. A certain expression involving that p-th root and the terms in the sequence up to that point is a p-th root of unity, and the group is finally determined by testing whether that root is 1. When $\sigma(a)/a \in K^p$, the results reduce to a theorem of A. A. Albert on cyclic extensions.

Introduction. Throughout this paper we fix a prime number p, and F will be a field of characteristic $\neq p$. Until the final section, we assume that F contains ζ, a primitive p-th root of unity. We let K be a Galois extension of F with cyclic Galois group $\langle\sigma\rangle$ of order $q = p^n$. Almost 60 years ago, A. A. Albert [2; 3, 206–216] studied the question of finding extensions of K that were cyclic of degree p^{n+1} over F, and his results have become familiar in textbooks [5, V.152; 11, 289]. The presence of ζ implies that any cyclic extension L of degree p over K has the form $K(a^{1/p})$ for some a in K. Albert showed that L is Galois over F iff $\sigma(a)/a = b^p$ for some b in K, and he observed that the norm $N_{K/F}(b)$ is a p-th root of 1. His main result then was that the Galois group of L over F is cyclic if this p-th root of 1 is nontrivial. If it is trivial, on the other hand, the Galois group is the product of cyclic groups of orders q and p.

In this paper, I shall generalize these results to the case where we take an arbitrary extension $K(a^{1/p})$ and form L as its normal closure over F. The goal is to determine the structure of $\mathrm{Gal}(L/K)$ completely from information involving K alone. Our tool is the sequence of elements in K defined by setting $a_0 = a$ and $a_{i+1} = \sigma(a_i)/a_i$. The degree of L over K will be determined by the first s for which a_s is a p-th power. For each possible degree (except the largest), there are exactly two types of Galois groups that can occur; and from our sequence we shall construct a p-th root of unity which is trivial in one case and nontrivial in the other. In the final section, again generalizing Albert's work, we shall see how the results can be extended to the case where the base field does not contain ζ.

Though the explicit results here are new, there has been a good deal of work on related topics since Albert wrote. One main line has been a study of "embedding problems" that

This work was supported in part by the U.S. NSF/NSA, Grant Number DMS9001223.

Received by the editors June 1, 1992.

AMS subject classification: 12F10.

https://doi.org/10.4153/CMB-1994-019-4 Published online by Cambridge University Press

reached a high point in the proof by Shafarevich [16] that every solvable group occurs as a Galois group over the rationals (*cf.* [10]). A related line was the study of "Galois algebras" initiated by Hasse [9] (after one earlier paper by Brauer [6]); an updated version of the relevant parts of this can be found in [14]. Finally, there have been several more specialized studies dealing with 2-power extensions, as in [7; 13; 18; 19]. Just recently, the case $q = 4$ was studied in detail by Vaughan [17], whose paper suggested to me that the general problem here could be solved.

1. **Review of Kummer theory.** The most rudimentary statement of Kummer theory is the following. Let E be a field of characteristic $\neq p$ containing ζ. Then adjoining various p-th roots to E gives a finite Galois extension with abelian Galois group annihilated by p, and conversely every such Galois extension arises in this way.

Making this statement somewhat more precise, we can say that extensions of this type correspond to finite subgroups $N/(E^\times)^p$ of $E^\times/(E^\times)^p$; the p-th roots of elements in N (where we really need only elements generating the quotient) give a field extension $L = E[N^{1/p}]$, and N is recovered from it as $N = \{x \in E^\times \mid x^{1/p} \in L\}$. The group $\mathrm{Gal}(L/E)$ is (noncanonically) isomorphic to $N/(E^\times)^p$.

Making the connection still more precise, we let μ_p denote the group of p-th roots of unity in E. Consider an element n in N and an automorphism ϕ in $\mathrm{Gal}(L/E)$. Let y be a p-th root of n, so y lies in L. We have $\phi(y)^p = \phi(n) = n = y^p$, so $\phi(y)/y$ is in μ_p. As ζ is in E, this quotient does not depend on our choice of p-th root. It is easy to see that the function $(n,\phi) \longmapsto \phi(y)/y$ gives a bi-multiplicative pairing

$$N/(E^\times)^p \times \mathrm{Gal}(L/E) \longrightarrow \mu_p;$$

and if we interpret these groups as vector spaces over $\mathbf{Z}/p\mathbf{Z}$, the theorem is that this pairing is nondegenerate. In other words, $\mathrm{Gal}(L/E)$ is naturally isomorphic to the dual of $N/(E^\times)^p$. These results are standard [12, 494–496; 4, 59–64; 5, V.84–86].

Relative versions of Kummer theory are not so familiar but are equally straightforward. (One possible reference is [14].) Suppose that our field E is a finite Galois extension of some field B. Obviously, a Kummer extension L of E will be Galois over B iff the B-conjugates of elements in N are again in N. That is, $\mathrm{Gal}(E/B)$ acts on $E^\times/(E^\times)^p$, and the Kummer extensions Galois over B are those that come from groups $N/(E^\times)^p$ which are invariant under this action. In that case, the elementary abelian group $\mathrm{Gal}(L/E)$ is a normal subgroup of $\mathrm{Gal}(L/B)$, and hence $\mathrm{Gal}(E/B)$ acts on $\mathrm{Gal}(L/E)$ by the conjugation in $\mathrm{Gal}(L/B)$. We have not assumed that ζ is in B, and thus there may be a group action also on μ_p. The one nontrivial thing to observe is that the Kummer pairing is consistent with the actions of $\mathrm{Gal}(E/B)$ on the three groups involved. To see this, let σ be an element of $\mathrm{Gal}(E/B)$, and let σ_1 be an extension of it in $\mathrm{Gal}(L/B)$. In the notation above, we then

https://doi.org/10.4153/CMB-1994-019-4 Published online by Cambridge University Press

have $\sigma_1(y)^p = \sigma(n)$, and

$$(\sigma_1\phi\sigma_1^{-1})\big(\sigma_1(y)\big)/\sigma_1(y) = \sigma_1\phi(y)/\sigma_1(y) = \sigma\big(\phi(y)/y\big).$$

2. **The degree of the extension.**

THEOREM 1. *Let ζ be in F, and let K/F be Galois with group $\langle\sigma\rangle$ of order $q = p^n$.*

(1) For any a in K, define a sequence of elements by setting $a_0 = a$ and $a_{i+1} = \sigma(a_i)/a_i$. Then a_q is always a p-th power.

(2) Let a_s be the first element in the sequence that is a p-th power. Then the normal closure L of $K(a^{1/p})$ over F has degree p^s over K and is given by $L = K(a_0^{1/p}, \ldots, a_{s-1}^{1/p})$.

(3) The only subfields of L containing K and Galois over F are those of the form $K(a_r^{1/p}, \ldots, a_{s-1}^{1/p})$.

PROOF. Curiously, this is almost entirely a theorem of linear algebra. Let S denote the linear mapping given by the action of σ on the vector space $K^\times/(K^\times)^p$. The minimal polynomial of this linear action on any finite-dimensional invariant subspace divides $X^q - 1$, as $\sigma^q = 1$. Since the vector space has characteristic p, we see that $X^q - 1 = (X-1)^q$, and hence the mapping $S - I$ is nilpotent of order at most q. In multiplicative notation, $S - I$ is given by $a \longmapsto \sigma(a)/a$, and thus we have proved (1). Simple linear algebra shows that, if we start with any vector v, then the nonzero elements in the sequence $v, (S-I)v, (S-I)^2v, \ldots$ are independent and span the smallest subspace containing v and invariant under $S - I$. But clearly a subspace is invariant under S iff it is invariant under $S - I$. Translating this information into multiplicative notation (and combining it with Kummer theory), we get (2). Finally, it is also easy to see (and familiar) that the subspace spanned by $v, (S-I)v, (S-I)^2v, \ldots$ has no invariant subspaces except the obvious ones spanned by $(S-I)^r v, (S-I)^{r+1}v, \ldots$; this gives us (3). ■

3. **Possible structures of the Galois group.**

We continue with the hypotheses and notation of Theorem 1.

THEOREM 2. *Let $G = \mathrm{Gal}(L/F)$. Let $A = \mathrm{Gal}(L/K)$, so $A \simeq (\mathbf{Z}/p\mathbf{Z})^s$ and $G/A \simeq \langle\sigma\rangle$.*

(1) Let τ_i be the basis of A dual to the a_i under the Kummer theory pairing. Then the action of σ fixes τ_0 and sends τ_i to $(\tau_i\tau_{i-2}\cdots)(\tau_{i-1}\tau_{i-3}\cdots)^{-1}$ for $i > 0$.

(2) If $s = q$, there is just one possible isomorphism type for G, namely, the semidirect product of A and $\langle\sigma\rangle$.

(3) If $s < q$, there are exactly two possible isomorphism types for G, the semi-direct product and one other.

PROOF. If we let w_i be a p-th root of a_i, then the dual basis τ_i is defined by $\tau_i(w_i) = \zeta w_i$ and $\tau_i(w_j) = w_j$ for $j \neq i$. We know from Section 1 that the action of $\langle\sigma\rangle$ on the dual basis is the transpose inverse of the action on the original basis, and thus (1) is true.

The rest of the argument is actually a computation in group cohomology, but (except at one point) nothing is gained by stating it that way. Let σ_1 in G be some element mapping

https://doi.org/10.4153/CMB-1994-019-4 Published online by Cambridge University Press

onto σ, so that the action of σ on A is given by conjugation with σ_1. Clearly all elements in G can be written uniquely in the form $\tau\sigma_1^i$ for some τ in A and $0 \leq i < q$, and (1) tells us the relation between $\sigma_1\tau$ and $\tau\sigma_1$. The group then will be determined by the value of σ_1^q. This element obviously lies in the kernel, A. Equally obviously, it is fixed by the σ-action. Hence it must be some power of τ_0. If it is the identity, then $\langle\sigma_1\rangle \simeq \langle\sigma\rangle$, and G is the semidirect product of A and $\langle\sigma\rangle$.

If we temporarily write A additively, we see that conjugation by σ_1 is a linear transformation S on A with $S\tau_0 = \tau_0$ and $S\tau_i = \tau_i - \tau_{i-1} + \cdots$. Now we can change our choice of σ_1 to any $\tau\sigma_1$ with τ in A. A simple computation in characteristic p shows that

$$(\tau\sigma_1)^q = \big((I + S + \cdots + S^{q-1})\tau\big)\sigma_1^q = \big((S - I)^{q-1}\tau\big)\sigma_1^q.$$

If $s = q$, we see that we can take τ to be a power of τ_{q-1} and thereby change σ_1^q by a power of τ_0. Hence in this case we can always find a choice making σ_1^q the identity, and we always have the semidirect product. Thus (2) is true.

If however $s < q$, then we see that all choices of σ_1 have the same q-th power. If that power happens to be the identity, then of course we again have the semi-direct product; but the power might also be some nontrivial τ_0^k. The exponent k is determined by the action of τ_0 on $a_0^{1/p}$, without reference to the other a_i (which involve σ in their definition). Thus if we go back and replace our generator σ by some σ^e (with e relatively prime to p), we will replace τ_0^k by τ_0^{ek}. Thus all cases with σ_1^q nontrivial give isomorphic groups G.

Next, we observe (for $s < q$) that the two different G we have described are indeed nonisomorphic; for the semi-direct product contains only elements of order at most $q = p^n$, while the other type contains an element σ_1 of order p^{n+1}.

Finally, though direct verification is not hard, we may as well refer to the general theory of group extensions (or group cohomology) for the fact that the equations we have given for the multiplication in our second type of group (with σ_1^q nontrivial) do indeed define such a group. See, for instance, [15, 121; 8, 225]. All finite groups of course occur as Galois groups of suitable field extensions, and thus we have proved (3). ∎

For $s < q$, we shall see in the next section that the elements a that yield semidirect products are the "special" ones, as they satisfy an extra condition. Indeed, the semidirect products are overlooked in [17] because of an oversight in group-theoretic analysis.

4. Determination of the Galois group.

We continue with the hypotheses and notations of Theorems 1 and 2.

THEOREM 3. *Suppose* $1 \leq s < q$. *Write* $a_{q-1} = d^p$ *with* d *in* K. *Set* $e(k) = \binom{q}{k}/p$, *and let*

$$c = \Big(\prod_{k=1}^{q-1} a_k^{e(k)}\Big) \cdot \big(\sigma(d)/d\big).$$

Then $c^p = 1$. *The group* $G = \mathrm{Gal}(L/F)$ *is the semidirect product iff* $c = 1$.

https://doi.org/10.4153/CMB-1994-019-4 Published online by Cambridge University Press

PROOF. By definition $a_{i+1} = \sigma(a_i)/a_i$, and hence we can choose the roots w_i with $w_{i+1} = \sigma_1(w_i)/w_i$. The binomial expansion of $X^q = \big((X-1)+1\big)^q$ then shows us that

$$\sigma_1^q(w_0) = \prod_{k=0}^{q} w_k^{\binom{q}{k}}.$$

Thus

$$\sigma_1^q(w_0)/w_0 = \prod_{k=1}^{q} w_k^{pe(k)}.$$

We denote this quantity by c. We have $w_0^p = a_0$ and $\sigma_1^q(a_0) = \sigma^q(a_0) = a_0$, so $c^p = 1$. For $k < q$, we can replace $w_k^{pe(k)}$ by the element $a_k^{e(k)}$ in K. By hypothesis, we have $d^p = a_{q-1}$, and thus w_{q-1} is $d\zeta^s$ for some s. As ζ is in F, we have $w_q = \sigma_1(w_{q-1})/w_{q-1} = \sigma(d)/d$. Thus the c defined in the proof is indeed given by the expression stated in the theorem. We know from the proof of Theorem 2 that σ_1^q is a power of τ_0, and thus it is trivial iff its action on w_0 is trivial. Hence we see that G is the semidirect product iff $c = 1$. ■

When s is smaller than $q-1$, it is possible to rewrite the formula for c to express all factors beyond $k = s$ in terms of the p-th root of a_s (which by definition will be in K). Suppose in particular that $s = 1$, and let us write $a_1 = b^p$. For convenience, we switch again to additive notation, treating $K^\times$ as a module over the ring $\mathbf{Z}[\sigma]$. Thus, for instance, $\sigma(b)/b$ is the result of applying $\sigma - 1$ to b. For $i \geq 1$, we get w_i as the result of applying $(\sigma-1)^i$ to b. In particular, up to an irrelevant power of ζ, we get d as the result of applying $(\sigma-1)^{q-2}$ to b, and hence $\sigma(d)/d$ is the result of applying $(\sigma-1)^{q-1}$ to b. Thus c is obtained by applying to b the operation

$$\sum_{k=1}^{q-1}\binom{q}{k}(\sigma-1)^{k-1} + (\sigma-1)^{q-1} = (\sigma^q - 1)/(\sigma - 1) = \sum_{k=0}^{q-1}\sigma^k.$$

In $K^\times$, this means that c is the product of all conjugates of b, or $N_{K/F}(b)$. Thus in this case our theorem does indeed reduce to Albert's result.

5. **When ζ is not in the base field.** To conclude, we show how the results can be extended to the case where ζ is not in the base field. We take K_0/F_0 to be a cyclic extension of degree $q = p^n$, where F_0 is an arbitrary field with $\mathrm{char}(F_0) \neq p$. We let F and K be the fields obtained by adjoining ζ to F_0 and K_0. The extensions K_0/F_0 and F/F_0 are Galois of relatively prime degrees. Thus K is Galois over F_0, and its group is the direct product of a group $\langle\sigma\rangle$ of order p^n and a group $\langle\rho\rangle \simeq \mathrm{Gal}(K/K_0) \simeq \mathrm{Gal}(F/F_0)$.

We need one preliminary result; it is basically due to Albert [1; 3, 209–211], who proved it in the cyclic case (*cf.* [14, 452]).

PROPOSITION. *(1) Let L_0/K_0 be Galois with group $A \simeq (\mathbf{Z}/p\mathbf{Z})^s$, and let $L = L_0(\zeta)$. Then L is Galois over K_0 with group $A \times \langle\rho\rangle$.*

(2) Let $\rho(\zeta) = \zeta^t$. If N is the subgroup of $K^\times$ corresponding to the Kummer extension L/K, then $\rho(n)/n^t$ is a p-th power for all n in N.

(3) Conversely, if $N/(K^\times)^p \simeq A$ has this behavior under ρ, then it gives a Kummer extension L/K that equals $L_0(\zeta)$ for a unique Galois L_0/K_0 of p-power degree.

PROOF. Part (1) follows from the relative primality of the degrees. Since the Galois group is abelian, we also see that L_0 is uniquely determined by L. For (2) and (3), we consider an arbitrary N for which the corresponding Kummer extension L/K has group A. We see by Section 1 that L/K_0 will be Galois iff $\rho(N) = N$. For such N, choose some ρ_1 in $\mathrm{Gal}(L/K_0)$ extending ρ. Consider any $y^p = n \in N$ and $\tau \in A$. Computing as at the end of Section 1, we see that

$$\Big(\rho_1\tau\rho_1^{-1}\big(\rho_1(y)\big)\Big)/\rho_1(y) = \rho_1\big(\tau(y)/y\big) = \big(\tau(y)/y\big)^t = \tau(y^t)/y^t,$$

and thus the value of the Kummer pairing on $\rho(n)$ and $\rho_1\tau\rho_1^{-1}$ is the same as on n^t and τ. It follows that ρ_1 commutes with A, and there is a Galois L_0, iff $\rho(n)$ and n^t are equal modulo $(K^\times)^p$. ■

THEOREM 4. *Let M_0/K_0 be a cyclic extension of degree p. Let L_0 be its normal closure over F_0. Set $M = M_0(\zeta)$ and $L = L_0(\zeta)$. Then M is cyclic of degree p over K, the field L is the normal closure of M over F, and* $\mathrm{Gal}(L/F) \simeq \mathrm{Gal}(L_0/F_0)$.

PROOF. The proposition shows that M is cyclic of degree p over K and equals $K(a^{1/p})$ for some a with $\rho(a)/a^t \in (K^\times)^p$. The normal closure of M over F then is given by the p-th roots of the various a_i with $a_0 = a$ and $a_{i+1} = \sigma(a_i)/a_i$. Since ρ and σ commute, each $\rho(a_i)/(a_i)^t$ is a p-th power in K. Hence we see that this normal closure is Galois over F_0, not just over F. Thus it contains L; but obviously L is Galois over F and contains M, so L is indeed the normal closure of M over F. The proposition shows further that there is an element ρ_1 in $\mathrm{Gal}(L/K_0)$ with $\langle\rho_1\rangle \simeq \langle\rho\rangle$. Its fixed field is the unique maximal subextension of p-power degree. All F_0-conjugates of that field still contain K_0 and have the same degree, so they are equal to it. Thus the fixed field of ρ_1 is Galois over F_0. It contains M_0, as we know the ρ_1-action on M. Hence it contains L_0. But we know $|L : L_0| \leq |F : F_0|$, and so the fixed field is equal to L_0. Thus the subgroup $\mathrm{Gal}(L/F)$ is a complement to the normal subgroup $\langle\rho_1\rangle$ and maps isomorphically onto $\mathrm{Gal}(L_0/F_0)$. ■

The proposition also shows that every $a \in K^\times$ with $\rho(a)/a^t \in (K^\times)^p$ yields such an M_0.

REFERENCES

1. A. A. Albert, *On normal Kummer fields over a non-modular field*, Trans. Amer. Math. Soc. **36**(1934), 885–892.

2. ———, *On cyclic fields*, Trans. Amer. Math. Soc. **37**(1935), 452–462.

3. ———, *Modern Higher Algebra*, University of Chicago Press, Chicago, 1937.

4. E. Artin, *Galois Theory*, Notre Dame Math. Lectures (2), Notre Dame, 1959.

5. N. Bourbaki, *Algèbre*, Chapitres 4–7, Masson, Paris, 1981.

6. R. Brauer, *Über die Konstruktion der Schiefkörper, die von endlichem Rang in bezug auf ein gegebenes Zentrum sind*, J. Reine Angew. Math. **168**(1932), 44–64; reprinted in Collected Papers 1, 121–141.

7. P. Damey and J.-J. Payan, *Existence et construction des extensions galoisiennes et non-abéliennes de degré* 8 *d'un corps de charactéristic différente de 2*, J. Reine Angew. Math. **244**(1970), 37–54.

https://doi.org/10.4153/CMB-1994-019-4 Published online by Cambridge University Press

8. M. Hall, Jr., *The Theory of Groups*, Macmillan, New York, 1959.

9. H. Hasse, *Existenz und Mannigfaltigkeit abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörper*, Math. Nachr. **1**(1948), 40–61.

10. V. V. Ishanov, *On the semidirect imbedding problem with nilpotent kernel*, Izv. Akad. Nauk SSSR Ser. Mat. **40**(1976), 3–25; Math USSR-Izv. **10**(1976), 1–23.

11. N. Jacobson, *Basic Algebra I*, Freeman, San Francisco, 1974.

12. ———, *Basic Algebra II*, Freeman, San Francisco, 1980.

13. I. Kiming, *Explicit classifications of some* 2*-extensions of a field of characteristic different from* 2, Canad. J. Math. **42**(1990), 825–855.

14. J.-J. Payan, *Critère de décomposition d'une extension de Kummer sur un sous-corps du corps de base*, Ann. Sci. École Norm. Sup. (4) **1**(1968), 445–458.

15. J.-P. Serre, *Corps locaux*, Hermann, Paris, 1962.

16. I. R. Shafarevich, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR Ser. Mat. **18**(1954), 525–578; Amer. Math. Soc. Translations (II) **4**(1956), 185–237.

17. T. P. Vaughan, *The normal closure of a quadratic extension of a cyclic quartic field*, Canad. J. Math **43**(1991), 1086–1097.

18. ———, *Constructing quaternionic fields*, Glasgow Math. J. **34**(1992), 43–54.

19. R. Ware, *A note on the quaternion group as Galois group*, Proc. Amer. Math. Soc. **108**(1990), 621–625.

Department of Mathematics
The Pennsylvania State University
University Park, Pennsylvania 16802
U.S.A

https://doi.org/10.4153/CMB-1994-019-4 Published online by Cambridge University Press