RADICAL EXTENSIONS AND CROSSED CHARACTERS

REINHOLD BAER

E. Witt[1] has given a theory of abelian extensions of fields containing sufficiently many roots of unity which consists essentially, as has been remarked before,[2] in applying the theory of characters of finite abelian groups. There exists now a sufficiently developed theory of crossed characters,[3] and it is the object of this note to show that a fairly complete and simple theory of radical extensions may be obtained if one follows Witt's treatment[4] of abelian extensions, only substituting for the classical theory of characters the theory of crossed characters.[5]

Suppose that the commutative field[6] K is a finite, normal, and separable extension of the field F, that the characteristic of the field K is either 0 or prime to the given integer m, and that E is the group of the mth roots of unity contained[7] in K. The Galois group G of the extension K of F consists of all the F-automorphisms of the field K (automorphisms of the field K which leave the elements in F invariant). Every automorphism g in G induces in E an automorphism which we also denote by g, and the correspondence mapping the automorphism g in G upon the automorphism g of E shall be denoted by C.

A C-character of the group G is a single-valued G to E function $f(g)$, satisfying the functional equation $f(u)^v f(v) = f(uv)$.

LEMMA 1. *The function v^{1-g} of the element g in G, for v an element in K, is a C-character of G if, and only if, v^m is an element, not 0, in F.*

PROOF. If v^{1-g} is a C-character of G, then v^{1-g} is for every g in G an element in E, so that $(v^m)^{1-g} = 1$ for every g in G. Thus v^m is a fixed element of the Galois group of K over F, proving that v^m is an element, not 0, in F.

Assume conversely that $v^m \neq 0$ is in F. Then $(v^{1-g})^m = (v^m)^{1-g} = 1$ for

Presented to the Society, April 24, 1943, received by the editors December 21, 1942.

[1] Witt [1], [2]; the references refer to the bibliography at the end of the paper.

[2] Baer [1].

[3] Baer [2].

[4] Or the treatment as suggested in Baer [1].

[5] The importance of the theory of crossed characters for the theory of radical extensions has recently been stressed by MacLane-Schilling [1].

[6] As all the fields will be commutative, we shall omit the word "commutative" in the future.

[7] K need not contain m distinct mth roots of unity; cp. Theorem 3 below.

every g in G, so that v^{1-g} is a single-valued G to E function. If s, t are elements in G, then $v^{1-st}=v^{1-t}v^{t-st}=(v^{1-s})^t v^{1-t}$, and we have shown that v^{1-g} is a C-character of G.

We denote, as customary, by F^* the multiplicative group of the elements, not 0, in F, and it will be convenient to denote by K_m the multiplicative group of those elements in K whose mth power is in F^*. Clearly F^* is a subgroup of K_m.

THEOREM 1. *An isomorphism of the group K_m/F^* upon the group of all the C-characters of G is effected by mapping the element v in K_m upon the function v^{1-g} of the elements in G.*

PROOF. It is a consequence of Lemma 1 that v^{1-g} is a C-character of G whenever v is an element in K_m, and it is readily seen that a homomorphism of K_m into the group of all the C-characters of G is effected by mapping v upon the function v^{1-g} of the elements in G. Furthermore $v^{1-g}=1$ for every g in G if, and only if, v is an element in F^*, as follows from the fundamental theorem of Galois theory, and this shows that exactly the elements in F^* are mapped upon the C-character 1. To complete the proof of our theorem we need show only that[8] every C-character of G may be represented in the form v^{1-g} for some v in K_m. Suppose therefore that $f(g)$ is a C-character of G. Assume that there did not exist an element w in K such that $\sum_{g \text{ in } G} w^g f(g)\neq 0$. Then $\sum_{g \text{ in } G}(w^h)^g f(g)=0$ for every h in G and every w in K. Since the elements $f(g)$ are different from 0 as elements in E, this implies that the determinant $D(w)=|w^{hg}|=0$ for every w in K. But this is impossible, since the normal basis theorem[9] assures the existence of elements w in K such that $D(w)\neq 0$. Consequently there exists an element w in K such that $v=\sum_{g \text{ in } G} w^g f(g)\neq 0$. If h is some element in G, then

$$v^h f(h) = \sum_{g \text{ in } G} w^{gh} f(g)^h f(h) = \sum_{g \text{ in } G} w^{gh} f(gh) = v,$$

since f is a C-character and gh ranges over G with g. Since $v\neq 0$, we find that $v^{1-h}=f(h)$ for every h in G, and it is a consequence of Lemma 1 that v belongs to K_m, as was to be shown.

The following restatement of Theorem 1 will prove helpful: If V is a coset of K_m/F^*, then V^{1-g} is a C-character of G, and every C-character of G may be represented in one and only one way in the form V^{1-g}.

---

[8] The following arguments are essentially a restatement of a proof of Speiser [1] p. 3.

[9] Cp. Deuring [1].

We recall that a group B of C-characters of G is termed[10] *complete* if $B(g)=1$ implies $g=1$.

THEOREM 2. *If M is a multiplicative group between F^* and K_m, then the following two properties of M are equivalent:*

(i) $K=F(M)$.

(ii) *The group of the C-characters V^{1-g} for V in M/F^* is complete.*

PROOF. The statement (ii) is obviously equivalent to the fact that 1 is the only $F(M)$-automorphism of K, and that this fact is equivalent to (i) is readily deduced from the Galois theory.

The group G has been termed[11] *C-complete* if 1 is the only element in G which is mapped upon 1 by every C-character of G. The following statement is an immediate consequence of Theorem 2.

COROLLARY 1. *The group G is C-complete if, and only if, K may be obtained by adjoining to F mth roots of elements in F.*

The C-characters of G which have the form e^{1-g} for suitable e *in the group* E have been termed *principal* C-characters of G, and the group of principal C-characters is called the *principal genus*. A complete group of C-characters of G is said to be *strictly complete* if it contains the principal genus.[12]

COROLLARY 2. *If M is a multiplicative group between F^* and K_m, then the following two conditions are necessary and sufficient for the group of C-characters of the form V^{1-g} with V in M/F^* to be strictly complete:*

(a) $K=F(M)$;

(b) *M is the set of all the elements in K whose mth powers are in the subgroup M^m of F^*.*

PROOF. It is readily seen that condition (b) is equivalent to the inequality $E\leqq M$, and hence (b) is true if, and only if, the group of C-characters of the form V^{1-g} for V in M/F^* contains the principal genus. Thus Corollary 2 is an immediate consequence of Theorem 2.

The importance of Corollary 2 stems from the comparative rarity of strictly complete groups of C-characters which are different from the group of all the C-characters.[13]

If M is a group between F^* and K_m, then M^m is a group between F^{*m} and $K_m^m\subseteq F^*$. However, the groups M/F^* and M^m/F^{*m} need not be isomorphic, since the homomorphism $x\to x^m$ maps upon 1 all the mth roots of unity in M, and these need not be in F^*.

[10] Baer [2] introduction to chapter IV.

[11] Baer [2] I.3.

[12] Baer [2] introduction to chapter IV.

[13] Baer [2] Corollary IV.4.2.

In an investigation of extensions by mth roots it is clearly no loss of generality to assume that m has been chosen as small as possible. Then the positive integer m has been determined in such a way that $K=F(K_m)$, though $F(K_{m'})<K$ for every proper divisor m' of m, and this signifies in group-theoretical language that m is the maximum order of the elements in the multiplicative abelian group K_m/F^*. If we use the notation $m=\prod_p p^{m(p)}$, where the product ranges over all the prime numbers p and where almost all the exponents $m(p)$vanish, then the maximum order of the elements in K_m/F^* is m if, and only if, K_m/F^* contains elements of order $p^{m(p)}$ for every p, since the orders of the elements in K_m/F^* are clearly divisors of m.

THEOREM 3. *The following conditions are necessary and sufficient for m to be the maximum order of the elements in K_m/F^*:*

(a) *K contains m distinct mth roots of unity, so that m is the order of E.*

(b) *If $0<m(p)$, and if a pth root of unity different from 1 is contained in F, then K_m^m is not part of F^{*p}.*

PROOF. If condition (a) were not satisfied by K, then the order m' of E would be a proper divisor of m; and if w is an element in K_m, g an F-automorphism of K, then $(w^{1-g})^{m'}=1$, since w^{1-g} belongs to E, proving that $w^{m'}=(w^{m'})^g$ for every F-automorphism g of K, and that therefore every $w^{m'}$, for w in K_m, is in F^*. Hence the maximum order of the elements in K_m/F^* is a divisor of the proper divisor m' of m, proving the necessity of (a).

To prove the necessity of (b) we assume that (b) does not hold for some particular prime p. Then $0<m(p)$, F contains p distinct pth roots of unity (so that every pth root of unity is in F) and $K_m^m\subseteq F^{*p}$; and we are going to show that K_m/F^* does not contain elements of order $p^{m(p)}$. Suppose namely that b is an element in K such that $b^{p^{m(p)}}$ is in F^*. Then there exists an integer r, prime to p, such that $rmp^{-m(p)}\equiv 1$ modulo $p^{m(p)}$, since $mp^{-m(p)}$ is itself prime to p. Hence $b\equiv b^{rmp^{-m(p)}}$ modulo F^*, and there exists therefore an element f in F^* such that $b=b^{rmp^{-m(p)}}f$. Since $b^{rm}=b^{p^{m(p)}}f^{-p^{m(p)}}$ is in F^*, it is in K_m^m and therefore in F^{*p}. Thus there exists an element c in F^* such that $c^p=b^{rm}$. If we put $d=cf^{p^{m(p)-1}}$, then d is an element in F^* and $(b^{p^{m(p)-1}}d^{-1})^p=b^{p^{m(p)}}f^{-p^{m(p)}}c^{-p}=1$. Hence $e=b^{p^{m(p)-1}}d^{-1}$ is a pth root of unity and as such is contained in F^*, proving finally that $b^{p^{m(p)-1}}=ed$ is an element in F^*. This completes the proof of the necessity of condition (b).

Suppose conversely that the conditions (a) and (b) are satisfied by K. If p is any prime number such that $m(p)=0$, then it is obvious

that K_m/F^* contains elements of order $p^{m(p)}$ $(=1)$. If $0<m(p)$, and if F^* does not contain any pth roots of unity different from 1, then we infer from (a) that K contains a primitive $p^{m(p)}$th root of unity e; and it is obvious that the order of e modulo F^* is exactly $p^{m(p)}$, proving again the existence of an element of order $p^{m(p)}$ in K_m/F^*. If finally $0<m(p)$, though F^* contains pth roots of unity different from 1, then we infer from condition (b) the existence of an element b in K_m^m which is not contained in F^{*p}. It is clear that b is an element in F^* and that there exists an element c in K satisfying $b=c^{p^{m(p)}}=(c^{p^{m(p)-1}})^p$. Since b is not in F^{*p}, it is impossible that $c^{p^{m(p)-1}}$ belongs to F^*, though $c^{p^{m(p)}}$ is in F^*, and this shows that c is an element in K whose order modulo F^* is exactly $p^{m(p)}$. Thus we have shown that K_m/F^* contains elements of order $p^{m(p)}$ for every p, and that consequently the maximum order of the elements in K_m/F^* is exactly m, as was to be proved.

REMARKS. 1. If $K=F(K_m)$, then condition (a) may be seen readily to be equivalent to the following condition:

(a′) *K is obtained by adjoining to F all the mth roots of the elements in the subgroup K_m^m of F^*.*

On the basis of Theorem 3 we may restrict ourselves without loss of generality to the consideration of extensions K of F which meet the requirement (a′).

2. Since the second root of unity -1 is always contained in F, it follows from $0<m(2)$ that the characteristic of F is different from 2, and that therefore condition (b) implies $K_m^m \subsetneq F^{*2}$.

3. Suppose that $0<m(p)$. It is well known that an automorphism of a cyclic group of order $p^{m(p)}$ possesses fixed elements different from 1 if, and only if, the order of the automorphism under consideration is a power of p. We note furthermore that a pth root of unity different from 1 is contained in F if, and only if, it is contained in K and is left invariant by every F-automorphism of K. Thus it follows that the condition (b) is equivalent to the following condition (b′), provided (a) is satisfied by K.

(b′) *If $0<m(p)$, and if the group of automorphisms induced by F-automorphisms of K in the group of the $p^{m(p)}$th roots of unity in K is of order a power of p, then $K_m^m \subsetneq F^{*p}$.*

For a further analysis it will be necessary to translate the fundamental concepts of the theory of crossed characters into concepts from the theory of extensions of fields. We denote by $E(p)$ the group of the $p^{m(p)}$th roots of unity in K so that E is the direct product of its cyclic subgroups $E(p)$; we note that condition (a) of Theorem 3 is equivalent to the assertion that $E(p)$ is of order $p^{m(p)}$ for every p.

As we denoted by C the homomorphism mapping the F-automorphism g of K upon the automorphism g of E which it induces in E, so we denote by Cp the homomorphism of G which maps g in G upon the automorphism g which it induces in $E(p)$. The groups G_C and G_{Cp} consist of all those elements in G which induce in E and $E(p)$ respectively the identity automorphism, and we find that G_C is the group of $F(E)$-automorphisms of K, and that G_{Cp} is the group of $F(E(p))$-automorphisms of K. The subgroup $H(p)$ of G has been defined[14] as the group of all those elements in G which are mapped upon 1 by every Cp-character of G, and it is an immediate consequence of Theorem 1 that $H(p)$ is the group of all the $F(K_{p^{m(p)}})$-automorphisms of K.

THEOREM 4. *There exists one and only one multiplicative group S between F^{*m} and F^* such that K may be obtained by adjoining all the mth roots of elements in S to F if, and only if, the following conditions are satisfied by K:*

(i) *K contains m distinct mth roots of unity, and $K=F(K_m)$.*

(ii) *If the element g in G_{Cp} is of order p modulo $H(p)$, then it is contained in $H(p)G_C$.*

(iii) *If $1<m(2)$, and if there exists an F-automorphism of K which maps every element in $E(2)$ upon its inverse, then $G/(H(2)G_{C2}^2)$ is not commutative.*

PROOF. It is readily verified that condition (i) is necessary and sufficient for the existence of at least one group S between F^{*m} and F^* such that K may be obtained by adjoining all the mth roots of elements in S to F (take $S=K_m^m$). If (i) is satisfied, then there exists one and only one group S with the required property if, and only if, K_m is the only group T between F^* and K_m such that $K=F(T)$ and $E\subseteq T$. It is an immediate consequence of Theorem 2 and of Corollary 2 to Theorem 2 that K_m is the only group T between F^*E and K_m satisfying $K=F(T)$ if, and only if, the group of all the C-characters of G is the only strictly complete group of C-characters of G; and that this later property is equivalent to conditions (ii) and (iii) is an immediate consequence of Baer [2], Corollary IV.4.2.

On account of the considerations centered around Theorem 3 we define: *the field K is an m-extension of its subfield F if* (1) *K is finite, normal, separable over F*; (2) *K contains m distinct mth roots of unity*; (3) $K=F(K_m)$. We note that (2) implies in particular that the characteristic of K is either 0 or prime to m.

If K is an m-extension of F, then K may be obtained by adjoining to F all the mth roots of elements in the multiplicative group K_m^m be-

[14] Baer [2] I.3; for a more detailed analysis of $H(p)$, cp. Baer [2] III 2.

tween F^{*m} and F^*; and it is obvious that K is uniquely determined, up to equivalence, by m and K_m^m.

THEOREM 5. *If S is a multiplicative group between F^{*m} and F^*, then the following conditions are necessary and sufficient for obtaining an m-extension of F by adjoining to F all*[15] *the mth roots of elements in S.*

(i) *The characteristic of F is either 0 or prime to m.*

(ii) *S/F^{*m} is a finite group.*

PROOF. The necessity of (i) has been pointed out before. To show the necessity of (ii), we consider an m-extension K of F which may be generated by adjoining the mth roots of elements in S to F. Then $K=F(K_m)$ and $F^{*m}\subseteq S\subseteq K_m^m\subseteq F^*$. It is a consequence of the finiteness of K over F and of Theorem 1 that K_m/F^* is a finite group. A homomorphism of K_m/F^* upon K_m^m/F^{*m} is effected by mapping the element x in K_m upon the element x^m in K_m^m, proving the finiteness of K_m^m/F^{*m}, and this implies the necessity of condition (ii).

The sufficiency of the conditions (i) and (ii) is readily verified.

Our theory would be complete if we could prove that different groups S between F^{*m} and F^*, meeting the above requirements (i), (ii), lead to essentially different m-extensions. This, however, cannot be expected, as may be seen from Theorem 4.

We are now going to impose two conditions upon the Galois group of the equation $x^m-1=0$ in the field F. This equation is supposed to be separable, a property that may be expressed in two equivalent ways by saying either that the characteristic of F, if not 0, should be prime to m, or that the equation has m distinct roots in a suitable extension of F. Properties of the Galois group of $x^m-1=0$ are best described by using some finite, normal, and separable extension of F which contains m distinct mth roots of unity, as the Galois group of the equation is independent of the particular choice of this extension. Thus we denote by E the group of the m distinct mth roots of unity contained in some finite, normal, separable extension H of F (for example, $H=F(E)$), and by $E(p)$ the subgroup of E consisting of the $p^{m(p)}$th roots of unity. Now we may state our two requirements, as follows:

(A) *If $1<m(2)$, then none of the automorphisms of the group E, contained in the Galois group of $x^m-1=0$ over F, maps every element in $E(2)$ upon its inverse.*

(B) *If the automorphisms of the Galois group of $x^m-1=0$ over F induce in $E(p)$ a group of order a power of p, and if $E(p)\neq 1$, then*

[15] This is best understood by restricting one's attention to subfields of some fixed algebraically closed extension of the field F.

the order of every automorphism in the Galois group of $x^m-1=0$ *over* F *which leaves the elements in* $E(p)$ *invariant is prime to* p.

It should be noted that condition (A) concerns only the Galois group of $x^{2^{m(2)}}-1=0$ over F, whereas (B) may be restated without reference to the groups E, $E(p)$ as follows:

(B′) *If the Galois group of* $x^{p^{m(p)}}-1=0$ *over* F *is of order a power of* p, *and if* $0<m(p)$, *then the modulo* $x^{p^{m(p)}}-1=0$ *reduced Galois group of* $x^m-1=0$ *over* F *is of an order prime to* p.

Witt in his theory of abelian extensions[16] had to require that m distinct mth roots of unity are contained in F. If we substitute for this condition the above properties (A), (B), then we obtain an extension of Witt's theory which comprises certain classes of m-extensions, as may be seen from the next theorem together with our remarks in connection with Theorem 5.

THEOREM 6. *If conditions* (A) *and* (B) *are satisfied by the field* F *and the integer* m (*which is prime to the characteristic of* F *in case the characteristic of* F *should be different from* 0), *if* S *and* T *are multiplicative groups between* F^{*m} *and* F^*, *and if* S/F^{*m} *and* T/F^{*m} *are both finite groups, then the following two properties imply each other*:

(i) $S=T$.

(ii) *The extensions of* F *which are obtained by adjoining to* F *all the* m*th roots of elements in* S *and in* T *respectively are equivalent.*

PROOF. It has been pointed out before that (ii) is a consequence of (i). If conversely (ii) is satisfied by S and T, then there exists a finite, normal, separable extension K of F such that $K=F(S')=F(T')$ where X' (for $X=S$ or T) is the group of all the elements in K whose mth powers are in X and X' consists of all the mth roots of elements in X. Clearly X is a group between F^* and K_m which contains m distinct mth roots of unity. It is a consequence of Theorem 2 and of Corollary 2 that X'/F^* is (essentially) a strictly complete group of C-characters of G. It is a consequence of conditions (A), (B) and of Baer [2], Theorem IV.1.1, that the only strictly complete group of C-characters of G is the group of all the C-characters of G. But it follows from Theorem 1 that this latter group is essentially the same as K_m/F^*, proving that $X'=K_m$. Thus we have shown that $S'=T'=K_m$, and this implies clearly $S=T$.

REMARK. If m is in particular an odd prime power, then conditions (A) and (B) are satisfied by F and m; if m is a power of 2, then (B) is satisfied by F and m, and (A) would be satisfied, for example, if F

[16] Witt [1].

contained all the fourth roots of unity. In these cases the above theorem may be applied without reservation.

In case condition (B) is not satisfied by F and m, we have to analyze the situation still further in order to obtain an extension of Theorem 6.

If K is an m-extension of F, then $K=F(K_m)$, and the multiplicative group K_m is the product of the multiplicative groups $K_{p^{m(p)}}$ consisting of all the elements in K whose $p^{m(p)}$th power is in F^*. Clearly K is the composite of its uniquely determined subfields $F(K_{p^{m(p)}})=K^{(p)}$, and it is readily verified that $K^{(p)}$ is a $p^{m(p)}$-extension of F. It has been remarked just now that condition (B) is satisfied by F and $p^{m(p)}$; and thus Theorem 6 may be applied upon $K^{(p)}$, provided (A) is satisfied by F and $2^{m(2)}$. Furthermore it should be remarked that a composite of $p^{m(p)}$-extensions of F is an m-extension of F. Combining these remarks with Theorem 5 we obtain the following result.

THEOREM 7. *Suppose that the characteristic of the field F is either* 0 *or prime to the integer m.*

(a) *The field K is an m-extension of the field F if, and only if, there exists, for every prime p, a multiplicative group S_p between $F^*{}^{p^{m(p)}}$ and F^* such that $S_p/F^*{}^{p^{m(p)}}$ is finite, and such that K is obtained by adjoining to F all the $p^{m(p)}$th roots of the elements in S_p.*

(b) *If condition* (A) *is satisfied by F and m, if S_p and T_p are, for every p, multiplicative groups between $F^*{}^{p^{m(p)}}$ and F^* such that both $S_p/F^*{}^{p^{m(p)}}$ and $T_p/F^*{}^{p^{m(p)}}$ are finite, then the following two properties are equivalent:*

(b, i) *$S_p=T_p$ for every prime p.*

(b, ii) *The m-extensions of F which are determined by the S_p and by the T_p respectively through statement* (a) *are equivalent extensions of F.*

If, however, condition (A) fails to hold, then we have to fall back upon Theorem 4.

BIBLIOGRAPHY

R. BAER

1. *Abelian fields and duality of abelian groups*, Amer. J. Math. vol. 59 (1937) pp. 869–888.
2. *A theory of crossed characters*, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 103–170.

M. DEURING

1. *Galoissche Theorie und Darstellungstheorie*, Math. Ann. vol. 107 (1932) pp. 140–144.

S. MACLANE AND O. F. G. SCHILLING

1. *A general Kummer theory for function fields*, Duke Math. J. vol. 9 (1942) pp. 125–167.

A. SPEISER
1. *Zahlentheoretische Sätze aus der Gruppentheorie*, Math. Zeit. vol. 5 (1919) pp. 1–6.

E. WITT
1. *Der Existenzsatz für abelsche Funktionenkörper*, J. Reine Angew. Math. vol. 173 (1935) pp. 43–51.
2. *Zyklische Körper und Algebren der Characteristic vom Grad p*, J. Reine Angew. Math. vol. 176 (1937) pp. 126–140.

UNIVERSITY OF ILLINOIS