EQUIVALENCE OF ALGEBRAIC EXTENSIONS†

BY REINHOLD BAER

The commutative fields‡ K and H are *equivalent* with regard to their common subfield L, if there exists an isomorphism between K and H which maps every element of L upon itself. If H and K are equivalent with regard to L, then the same equations with coefficients in L have solutions in H and in K. It is the aim of this note to establish a criterion for the validity of the converse of the above proposition.

The field F is *completely algebraic* with regard to its subfield S, if F and S satisfy:

(1) *F is algebraic with regard to S;*

(2) *if $\mathfrak{f}$ is an isomorphism of S upon the subfield S' of the field G' such that every equation (with coefficients) in S which has a solution in F is mapped by $\mathfrak{f}$ upon an equation in S' which has a solution in G', then $\mathfrak{f}$ is induced by an isomorphism of F upon a field F' between S' and G' ($S' \leqq F' \leqq G'$).*

E. Steinitz§ has proved that every simple algebraic extension|| and every normal algebraic extension¶ is completely algebraic.

LEMMA 1. *If the algebraic extension F of the field S satisfies the condition* (i) *to every pair of fields U and V such that $S \leqq U \leqq V \leqq F$, V finite with regard to U, there exists a field W between V and F such that W is finite and completely algebraic with regard to U, then F is completely algebraic with regard to S.*

PROOF. There exists a chain of fields F_v (v an ordinal number

---

† Presented to the Society, October 31, 1936.

‡ Only commutative fields will be considered in this note.

§ See E. Steinitz, *Algebraische Theorie der Körper*; *Mit Erläuterungen und einem Anhang*: *Abriss der Galois-schen Theorie*, neu herausgegeben von Reinhold Baer und Helmut Hasse, 1931.

|| S is the simple algebraic extension of the field F, generated by the element b, if b satisfies an algebraic equation with coefficients in F and S is a smallest field containing F and b.

¶ N is normal with regard to its subfield S if every irreducible polynomial in S which has zeros in N is in N a product of linear polynomials.

taking all values between 0 and a certain ordinal number k) such that $F_0 = S$, $F_{v+1} = F_v(e_v)$ is a simple (algebraic) extension of F_v for $0 \leqq v \leqq k$, F_v is the join of all the F_u with $0 \leqq u < v$, if v is a limit ordinal, $F_k = F$. This chain of fields F_v satisfies in particular the relations $S \leqq F_u \leqq F_v \leqq F$, if $u < v$.

Assume now that G' is an algebraic extension of the field S' and that there exists an isomorphism $\mathfrak{s}$ of S upon S' such that (I) every equation in S with solutions in F is mapped by $\mathfrak{s}$ upon an equation in S' with solutions in G'.

There will now be constructed by complete (transfinite) induction a chain of fields F_v' and of isomorphisms $\mathfrak{f}_v$ of F_v upon F_v' such that $S' \leqq F_u' \leqq F_v' \leqq G'$ for $u < v$; $\mathfrak{f}_0 = \mathfrak{s}$, $\mathfrak{f}_v$ induces $\mathfrak{f}_u$ in F_u for $u < v$; every $\mathfrak{f}_v$ satisfies (I). Since $F_0' = S'$ and $\mathfrak{f}_0 = \mathfrak{s}$ is a suitable beginning for this construction, it may be assumed that F_v', $\mathfrak{f}_v$ have been defined for every v with $0 \leqq v < u$ ($\leqq k$) and that they satisfy the above conditions.

CASE 1. *$u = w + 1$ is not a limit ordinal.*

Denote by $g(x)$ the irreducible polynomial in F_w whose zero is e_w. It is mapped by $\mathfrak{f}_w$ upon a certain polynomial $g^*(x)$ in F_w' and $g^*(x)$ has zeros in G', since $\mathfrak{f}_w$ satisfies (I). Let $b_1, \cdots, b_n$ be the set of all the zeros of $g^*(x)$ in G'; n is finite and positive. Since $g(x)$ is irreducible in F_w, $\mathfrak{f}_w$ is an isomorphism, it follows that $g^*(x)$ is irreducible in F_w', and consequently there exists for every i exactly one isomorphism $\mathfrak{h}_i$ which induces $\mathfrak{f}_w$ in F_w and maps F_u upon $F_w'(b_i)$ and e_u upon b_i.

If $\mathfrak{h}_i$ does not satisfy (I), then there exists a polynomial $q_i(x)$ in F_u which has zeros in F such that the polynomial $q_i^*(x)$ upon which $q_i(x)$ is mapped by $\mathfrak{h}_i$ has no zero in G'. Assume that none of the isomorphisms $\mathfrak{h}_i$ satisfies (I). The set of all the solutions in F of the equation $g(x)q_1(x) \cdots q_n(x) = 0$ generates a certain field V between F_w and F which contains F_u and is finite with regard to F_w. There exists therefore by condition (i) a field W between V and F which is finite and completely algebraic with regard to F_w. Since the isomorphism $\mathfrak{f}_w$ of the subfield F_w of W satisfies (I), it follows that there exists an isomorphism $\mathfrak{h}$ of W upon a field W' between F_w' and G' which induces $\mathfrak{f}_w$ in F_w. Since the isomorphisms $\mathfrak{h}_1, \cdots, \mathfrak{h}_n$ are all the possible isomorphisms of the subfield F_u upon a field between F_w' and G' which induce $\mathfrak{f}_w$ in F_w, and since F_u is a subfield of W, $\mathfrak{h}$ induces in F_u exactly one of the isomorphisms $\mathfrak{h}_i$, say $\mathfrak{h}_1$. Since $q_1(x)$ has zeros in W, $q_1(x)$ is mapped by $\mathfrak{h}$ and by $\mathfrak{h}_1$ upon a polynomial in $F_w'(b_1)$ which has zeros in G' in contradiction to the above assumption. Therefore at least one of the isomorphisms $\mathfrak{h}_i$, say $\mathfrak{h}_n$, satisfies (I) and it may be defined by $\mathfrak{f}_u=\mathfrak{h}_n$, $F_u'=F_w'(b_n)$, and thus the chain of fields and isomorphisms has been prolongated in the required way.

CASE 2. *u is a limit ordinal.*

Then F_u is the join of the increasing chain of fields F_v with $v<u$. If F_u' is defined as the join of the increasing chain of fields F_v' with $v<u$, then there exists one and only one isomorphism† $\mathfrak{f}_u$ of F_u upon F_u' which induces $\mathfrak{f}_v$ in F_v for $v<u$. Since every polynomial in F_u is contained in a certain F_v with $v<u$, and since every $\mathfrak{f}_v$ with $v<u$ satisfies (I), it follows that also $\mathfrak{f}_u$ satisfies (I).

Thus it has been proved that fields F_u' and isomorphisms $\mathfrak{f}_u$, satisfying the above conditions, exist for every u with $0 \leqq u \leqq k$. There exists therefore, in particular, an isomorphism $\mathfrak{f}_k$ of $F_k=F$ upon a field F_k' between S' and G' which induces the given isomorphism $\mathfrak{s}$ in S, and therefore F is completely algebraic with regard to S.

COROLLARY 1. *If F is algebraic and separable‡ with regard to its subfield S, then F is completely algebraic with regard to S.*

PROOF. If $S \leqq U \leqq V \leqq F$, then F and V are separable with regard to U. V is therefore a simple algebraic extension of U if, and only if, V is finite with regard to U. Since simple algebraic extensions are completely algebraic, it follows therefore that F satisfies (i) with regard to S, and consequently Lemma 1 implies that F is completely algebraic with regard to S.

THEOREM 1. *Assume that F is completely algebraic with regard to its subfield S, that F' is algebraic with regard to its subfield S', and that $\mathfrak{s}$ is an isomorphism of S upon S'. Then there exists an*

† See E. Steinitz, loc. cit., *Erläuterungen*, pp. 17–18.

‡ F is separable (and algebraic) with regard to its subfield S, if every element of F is a solution of a separable irreducible equation in S. An irreducible equation $g(x)=0$ in S is not separable if the characteristic of S is a prime number p and $g(x)=\sum_{i=0}^{n} s_i x^{pi}$. All the solutions of a separable equation are *different*. Every finite separable extension is simple.

isomorphism of F upon F' which induces $\mathfrak{s}$ in S if, and only if, every polynomial $g(x)$ in S has the same number of zeros in F as the polynomial $g(x)\mathfrak{s}=g^*(x)$ (upon which $g(x)$ is mapped by $\mathfrak{s}$) has zeros in F'.

PROOF. Clearly it suffices to prove that the condition is sufficient. From the assumptions it follows that there exists an isomorphism $\mathfrak{f}$ of F upon a field F^* between S' and F' which induces $\mathfrak{s}$ in S. Since $g(x)$ has as many zeros in F as $g(x)\mathfrak{f}=g(x)\mathfrak{s}$ has zeros in F^* and in F', it follows that all the elements of F' which are algebraic with regard to S' are contained in F^*, and since F' is algebraic with regard to S', it follows that $F'=F^*$, that is that $\mathfrak{s}$ is induced by the isomorphism $\mathfrak{f}$ of F upon F'.

COROLLARY 2. *If F is algebraic and separable with regard to its subfield S, and F' is algebraic with regard to its subfield S', then the isomorphism $\mathfrak{s}$ of S upon S' is induced by an isomorphism of F upon F' if, and only if, the polynomial $g(x)$ in S has a zero in F if, and only if, $g(x)\mathfrak{s}$ has a zero in F'.*

PROOF. It suffices to prove the sufficiency of the condition. Since an algebraic extension of a field is separable if, and only if, the solved irreducible equations of the subfield are separable,† F' is separable with regard to S'. By Corollary 1, F and F' are completely algebraic with regard to S and S', respectively. There exists therefore

an isomorphism $\mathfrak{f}$ of F upon a field G' between S' and F' which induces $\mathfrak{s}$ in S.	an isomorphism $\mathfrak{g}$ of F' upon a field G between S and F which induces $\mathfrak{s}^{-1}$ in S'.

If the polynomial $g(x)$ in S has n zeros in F and the polynomial $g(x)\mathfrak{s}$ has n' zeros in F', then $n\leqq n'\leqq n$, that is, $n=n'$, since the zeros of $g(x)$ are mapped by $\mathfrak{f}$ upon zeros of $g(x)\mathfrak{s}$ and the zeros of $g(x)\mathfrak{s}$ are mapped by $\mathfrak{g}$ upon zeros of $g(x)$. The isomorphism $\mathfrak{s}$ satisfies therefore the condition of Theorem 1 and is consequently induced by an isomorphism of F upon F'.

COROLLARY 3. *If F and G are algebraic with regard to their common subfield S, and if F is separable with regard to S, then F and G are equivalent with regard to S if, and only if, the same equations in S have solutions in F and in G.*

† See Steinitz, loc. cit.

Suppose that F is a field of characteristic $p \neq 0$ and that K is a subfield of F. Then the element x of F is said to be a *root* with regard to K if there exists an integer $n = n(x) \geqq 0$ such that x^{p^n} is an element of K. The set $R(K < F)$ of all the elements in F which are roots with regard to K is a subfield of F, containing K.†

LEMMA 2. *Suppose that K_i is a subfield of the field F_i of characteristic $p \neq 0$, and that there exists an isomorphism $\mathfrak{k}$ of K_1 upon K_2, satisfying the condition*(K) *an equation with coefficients in K_1 has a solution in F_1 if, and only if, the* (*under $\mathfrak{k}$*) *corresponding equation in K_2 has a solution in F_2. Then there exists one and only one isomorphism $\mathfrak{r}$ of $R(K_1 < F_1)$ upon $R(K_2 < F_2)$ which induces $\mathfrak{k}$ in K_1 and this isomorphism $\mathfrak{r}$ satisfies the condition* (R) *an equation with coefficients in $R(K_1 < F_1)$ has a solution in F_1 if, and only if, the* (*under $\mathfrak{r}$*) *corresponding equation in $R(K_2 < F_2)$ has a solution in F_2.*

PROOF. If the element b of F_i is a root with regard to K_i, then there exists a smallest not negative integer $e = e(b)$ such that $b^{p^{e(b)}} = b^*$ is an element of K_i. The polynomial‡ $f_b(x) = x^{p^{e(b)}} - b^*$ is irreducible in K_i and its only zero in F_i is b, since $f_b(x) = (x - b)^{p^{e(b)}}$ in F_i. Conversely, a polynomial of the form $x^{p^j} - c$ in K_i has at most one zero in F_i.

If now b is any element of $R(K_1 < F_1)$, then it follows from these remarks and from condition (K) that there exists exactly one zero of the polynomial $x^{p^{e(b)}} - b^*\mathfrak{k}$ in F_2, and this uniquely determined element of F_2 may be denoted by $b\mathfrak{r}$. It follows from the mentioned properties of the fields $R(K_i < F_i)$ and from the equations $(x+y)^{p^j} = x^{p^j} + y^{p^j}$, that $\mathfrak{r}$ is an isomorphism of $R(K_1 < F_1)$ upon $R(K_2 < F_2)$ which induces $\mathfrak{k}$ in K_1, and that $\mathfrak{r}$ is the only isomorphism with this property.

From the formula which has just been mentioned it follows that there exists to every polynomial $f(x)$ in $R(K_i < F_i)$ a not negative integer n such that $f(x)^{p^n}$ is a polynomial in K_i. The polynomial $f(x) = 0$ has therefore a solution in F_i if, and only if, the equation $f(x)^{p^n} = 0$ (with coefficients in K_i) has a solution in F_i. Now (R) is a consequence of (K).

† See Steinitz, loc. cit., §§11–14.

‡ See Steinitz, loc. cit., §§11–14.

A consequence of this Lemma 2 and of Corollary 2 is the following corollary.

COROLLARY 4. *Suppose that the field F_i of characteristic $p\neq 0$ is algebraic with regard to its subfield K and that F_1 is separable with regard to $R(K<F_1)$. Then F_1 and F_2 are equivalent extensions of their common subfield K if, and only if, the same equations in K have solutions in F_1 and in F_2.*

REMARK. If F is an algebraic extension of the field K of characteristic $p\neq 0$, then it may happen that F is *not* separable with regard to $R(K<F)$.† If F is algebraic and normal with regard to K, then F is always‡ separable with regard to $R(K<F)$. Corollary 4 contains therefore the analogous proposition concerning normal algebraic extensions which has been mentioned in the beginning of this note.

THE INSTITUTE FOR ADVANCED STUDY

† An example for this phenomenon may be found in R. Baer, *Abbildungseigenschaften algebraischer Erweiterungen*, Mathematische Zeitschrift, vol. 33 (1931), pp. 451–479, particularly pp. 471–472.

‡ See Baer, loc. cit., Satz 14 on p. 471; for further criteria see Sätze 15 and 16.