ON THE COMPOSITION OF FIELDS

CLAUDE CHEVALLEY

Let K/k, K'/k be two extensions of a basic field k. By a *composite extension* of these two extensions, we understand the complex notion formed of an extension $\mathfrak{K}/k$ of k, of an isomorphism τ of K/k into $\mathfrak{K}/k$ and of an isomorphism τ' of K'/k into $\mathfrak{K}/k$, provided the following conditions are verified:

(1) $\mathfrak{K}$ is generated by the two fields K^τ, $K'^{\tau'}$.

(2) If A, A' are subsets of K, K' respectively which are algebraically independent over k, the set $A^\tau \cup (A')^{\tau'}$ is algebraically independent over k. In other words, the algebraic relations which hold in $\mathfrak{K}$ between elements of K^τ, $K'^{\tau'}$ are consequences of the algebraic relations which hold between elements of K^τ alone or of $K'^{\tau'}$ alone.[1]

THEOREM 1. *Any two given extensions K/k, K'/k have at least one composite extension.*

Let B' be a transcendence basis for K'/k. We can find a purely transcendental extension Ω/K which has a transcendence basis $B'^{\tau'}$ with the same cardinal number as B' (τ' stands for a one-to-one mapping of B' onto $B'^{\tau'}$). The algebraic closure $\bar{\Omega}$ of Ω contains the algebraic closure $\bar{\mathrm{P}}$ of the field $\mathrm{P}=k(B'^{\tau'})$. The mapping τ' may be extended to an isomorphism of K'/k with an extension $K'^{\tau'}/k$ contained in $\bar{\mathrm{P}}/k$, and a fortiori in $\bar{\Omega}$. We set $\mathfrak{K}=KK'^{\tau'}$, and denote by τ the identity mapping of K/k into $\mathfrak{K}/k$. We claim that the system $(\mathfrak{K}/k, \tau, \tau')$ is a composite extension of K/k, K'/k.

It is sufficient to check the condition (2), and we may assume without loss of generality that A, A' are finite. There exists a finite subset B_1' of B' such that $k(A', B_1')$ is algebraic over $k(B_1')$. Let d, d', e be the number of elements in A, A_1', B_1'. The elements of B_1', being algebraically independent over K, are *a fortiori* algebraically independent over $k(A)$. Therefore, the degree of transcendency of $k(A, A'^{\tau'}, B_1'^{\tau'})$ over k is $d+e$. The degree of transcendency of $k(A_1'^{\tau'}, B_1'^{\tau'})$ over $k(A_1'^{\tau'})$ is $e-d'$. The degree of transcendency f of $k(A, A'^{\tau'}, B_1'^{\tau'})$ over $k(A)$ is therefore less than or equal to $e-d$. It follows that the degree of transcendency of $k(A, A'^{\tau'})$ over k, which

Received by the editors October 1, 1941.

[1] The problem of composite extensions has been considered by Zariski (*Algebraic varieties over ground fields of characteristic zero*, American Journal of Mathematics, vol. 62 (1940), pp. 187–221) in the case when one of the extensions K/k, K'/k is algebraic and normal.

is $d+e-f$, is at least equal to $d+d'$, which proves that $A \cup A'^{\tau'}$ is algebraically independent over k.

Let $(\mathfrak{K}/k, \tau, \tau')$ and $(\mathfrak{K}_1/k, \tau_1, \tau_1')$ be two composite extensions of K/k, K'/k. We shall say that these extensions are isomorphic if there exists an isomorphism σ of $\mathfrak{K}/k$ with $\mathfrak{K}'/k$ such that $\tau_1 = \sigma\tau$, $\tau_1' = \sigma\tau'$.

The consideration of the case where K/k, K'/k are algebraic over k (but not normal) shows immediately that there are in general several non-isomorphic types of composite extensions. The extreme opposite case occurs when k is algebraically closed in K and K' (k is said to be algebraically closed in K if every element of K which is algebraic over k lies already in k). In that case, the composite extension $\mathfrak{K}/k$ turns out to be unique; but, unfortunately, k may fail to be algebraically closed in $\mathfrak{K}$. For instance, let us take $K = K' = k(x, (a+bx^p)^{1/p})$, where $p \neq 0$ is the characteristic of k, and where a, b are elements of k such that $k((a)^{1/p}, (b)^{1/p})$ is of degree p^2 over k. It is easy to verify that k is algebraically closed in K; on the other hand, the composite extension is $k(x, y, (a+bx^p)^{1/p}, (a+by^p)^{1/p})/k = k(x, y, (a)^{1/p}, (b)^{1/p})/k$.

We shall get around this difficulty by introducing the following notion:

DEFINITION 1. *A field k is said to be quasi-algebraically closed (q.a.c.) in K if every element a of K which is algebraic over k is purely inseparable over k (that is, is the unique root of some equation with coefficients in k).*

We shall prove the following theorem:

THEOREM 2. *Let $(\mathfrak{K}/k, \tau, \tau')$ and $(\mathfrak{K}_1/k, \tau_1, \tau_1')$ be two composite extensions of the extensions K/k, K'/k. Let L, L' be fields such that: (1) $k \subset L \subset K$, $k \subset L' \subset K'$; (2) L, L' are algebraic over k; (3) L is q.a.c. in K and L' is q.a.c. in K'. If an isomorphism σ_0 of $L^\tau L'^{\tau'}/k$ with $L^{\tau_1} L'^{\tau_1'}/k$ is such that $\sigma_0\tau$ coincides on L with τ_1 and $\sigma_0\tau'$ coincides on L' with τ_1', then σ_0 may be extended to an isomorphism of $(\mathfrak{K}/k, \tau, \tau')$ with $(\mathfrak{K}_1/k, \tau_1, \tau_1')$.*

In other words, the type of the composite extension $(\mathfrak{K}/k, \tau, \tau')$ is determined by the type of the composite extension $(L^\tau L'^{\tau'}/k, \tau, \tau')$ of L/k, L'/k.

We shall first prove three lemmas. The fields which are considered in the first two of these lemmas are assumed to be all subfields of some all-inclusive field.

LEMMA 1. *Let k be a q.a.c. sub-field of a field K. Let Z be a field such that $k \subset Z \subset K$, and y be an element of K which is a root of an irreducible equation $F=0$ with coefficients in Z. Let Ω/k be an algebraic extension* *of k, α be an element of Ω and $\Phi=0$, the irreducible equation in k which is satisfied by α. Then the polynomial F is a power of an irreducible polynomial in the field ΩZ, and Φ is a power of an irreducible polynomial in K. Moreover, Ω is q.a.c. in the field $K\Omega$.*

We may assume without loss of generality that $\Omega=k(\alpha)$. Let L be the algebraic closure of k in K (that is, the field consisting of the elements of K which are algebraic over k). Let $\Phi_1=0$ be the irreducible equation satisfied by α in L. Therefore Φ_1 divides Φ. On the other hand, if p is the characteristic of k, the polynomial $\Phi_1^{p^u}$ has its coefficients in k if u is large enough, and therefore Φ divides $\Phi_1^{p^u}$. It follows that Φ is a power of Φ_1.

If $\Phi_1'=0$ is the irreducible equation satisfied by α in K then Φ_1' divides Φ_1. Therefore, every root of the equation $\Phi_1'=0$ is also a root of $\Phi_1=0$, which shows that the coefficients of Φ_1' are algebraic over k. It follows that $\Phi_1'=\Phi_1$ which proves that Φ is a power of an irreducible polynomial in K.

Let $F_1=0$ be the irreducible equation satisfied by y in LZ, and let m be the degree of F_1. If n is the degree of ϕ_1, we have

$$[LZ(y, \alpha):LZ] = [LZ(y, \alpha):LZ(y)][LZ(y):LZ] = mn$$

because Φ_1 is irreducible in K, and *a fortiori*, in $LZ(y)$. It follows that

$$[LZ(y, \alpha):LZ(\alpha)][LZ(\alpha):LZ] = mn.$$

But $[LZ(\alpha):LZ]=n$, since Φ_1 is irreducible in LZ; therefore we have $[LZ(y, \alpha):LZ(\alpha)]=n$ which shows that F_1 is irreducible in $LZ(\alpha)$. On the other hand, F_1 divides F; since LZ is purely inseparable over Z, the same argument which was used above for Φ_1 shows that F is a power of F_1. Since $Z\subset\Omega Z=Z(\alpha)\subset LZ(\alpha)$, F is also a power of an irreducible polynomial in ΩZ.

There remains to prove that $k(\alpha)$ is q.a.c. in $K(\alpha)$. Let β be an element of $K(\alpha)$ which is algebraic over $k(\alpha)$, and therefore also on k. There exists a power $\alpha^{p^s}=\alpha_1$ of α which is separable over k; we set $\beta_1=\beta^{p^s}$, whence $\beta_1\in K(\alpha_1)$ and

$$\beta_1 = \xi_0 + \xi_1\alpha_1 + \cdots + \xi_{h-1}\alpha_1^{h-1}, \qquad \xi_i \in K,$$

where $h=[K(\alpha_1):K]$. If we write the corresponding formulas for the conjugates of β_1 with respect to K, and observe that α_1 is different from its conjugates, we see that the ξ_i's may be expressed rationally by means of the conjugates of α_1, β_1. It follows that $\xi_0, \xi_1, \cdots, \xi_{h-1}$ are algebraic over k, and therefore belong to L. Since L is purely inseparable over k, we may conclude that some power $\beta_1^{p^t}$ of β_1 lies in $k(\alpha_1)$, where p is the characteristic of k ($\beta_1 \in k(\alpha_1)$) (if $p=0$). We have $\beta^{p^{s+t}} \in \Omega$ which completes the proof of the lemma.

Before stating Lemma 2, we have to introduce another notion. Two extensions K/k, Ω/k of the field k which are contained in some larger field are said to be *algebraically dissociated* if the following condition is realized: If A, B are subsets of K, Ω, respectively, which are algebraically independent over k, the set $A \cup B$ is also algebraically independent.

LEMMA 2. *The Lemma* 1 (*abstraction made of what concerns* α *and* Φ) *remains valid when* Ω/k *is any extension of* k, *provided the extensions* Ω/k, K/k *are algebraically dissociated.*

Let C be a transcendence basis of Ω/k and Ω_0 the field $k(C)$. Under our assumption the extension $K\Omega_0/K$ is purely transcendental. We claim that Ω_0 is q.a.c. in $K\Omega_0$. It will of course be sufficient to prove it in the case where C consists[2] in a single element t. Let $P(t)/Q(t)=\omega$ be an element of $K\Omega_0=K(t)$ (where $P(t)$, $Q(t)$ are polynomials with coefficients in K). We shall prove that if ω is algebraic over Ω_0, it can be expressed as a rational function in t with coefficients in L (the algebraic closure of k in K). From this result it will follow that $L\Omega_0$ is algebraically closed in $K\Omega_0$, and therefore that Ω_0 is q.a.c. in $K\Omega_0$.

The proof will proceed by induction on the number $l=d^\circ P+d^\circ Q$ where $d^\circ P$, $d^\circ Q$ denote the degrees of P, Q with respect to t. It is obvious for $l=0$; assume that the result holds for $l-1$. If either one of the elements $P(0)$, $Q(0)$ is null, we can reduce ourselves to the case $l-1$ by considering instead of ω one of the elements ω/t, $t\omega$ (these elements are also algebraic over Ω_0). So, let us assume that $P(0)Q(0)\neq 0$. We have by assumption a relation of the form

$$A_0(t)P^n(t) + A_1(t)P^{n-1}(t)Q(t) + \cdots + A_n(t)Q^n(t) = 0,$$

where $A_0(t), \cdots, A_n(t)$ are polynomials in t with coefficients in k, not all divisible by t. Putting $t=0$, we conclude that $P(0)/Q(0)$ is algebraic over k, and therefore belongs to L. The element $\omega'=P(t)/Q(t)-P(0)/Q(0)$ is again algebraic over Ω_0 and may be written in the form $tP'(t)/Q'(t)$ with $d^\circ P'+d^\circ Q'=l-1$. Therefore $\omega'/t\in L(t)$ and $\omega\in L(t)$, which proves our assertion.

The extension $Z\Omega_0/Z$ being purely transcendental (because $K\Omega_0/K$ is), the polynomial F, which is irreducible in Z, remains irreducible

[2] This property was proved in the paper, *Pencils on an algebraic variety and a new proof of a theorem of Bertini*, by Zariski, Transactions of this Society, vol. 50 (1941), pp. 48–70.

in $Z\Omega_0$. The extension Ω/Ω_0 being algebraic, it follows from Lemma 1 (applied with Ω_0 instead of k) that F becomes a power of an irreducible polynomial in $Z\Omega$ and that Ω is q.a.c. in $K\Omega$; Lemma 2 has been proved.

We pass now to the third lemma. The notations used in this lemma are the same as those introduced in the statement of Theorem 2.

LEMMA 3. *Let Z be a field such that $L\subset Z\subset K$, and let y be an element of K. (1) If y is transcendental over Z, y^τ is transcendental over $Z^\tau K'^{\tau'}$. (2) If y is a root of the irreducible equation $F=0$ in Z, the polynomial F^τ is a power of an irreducible polynomial in $Z^\tau K'^{\tau'}$.*

(1) Let B' be a transcendence basis of K'/k and C be a transcendence basis of Z/k; hence $C^\tau\cup B'^{\tau'}$ is a transcendence basis of $Z^\tau K'^{\tau'}/k$. If y is transcendental over Z, the set $C\cup\{y\}$ is algebraically independent; therefore $C^\tau\cup B'^{\tau'}\cup\{y^\tau\}$ is algebraically independent over k, which proves that y^τ is transcendental over $Z^\tau K'^{\tau'}$.

(2) Since the extensions Z^τ/k, $K'^{\tau'}/k$ are clearly algebraically dissociated over k, assertion (2) results from Lemma 2.

We pass now to the proof of Theorem 2. We consider the set Σ of the systems $(Z, Z', \sigma(Z, Z'))$ composed (a) of fields Z, Z' such that $L\subset Z\subset K$, $L'\subset Z'\subset K'$; (b) of an isomorphism $\sigma(Z, Z')$ of $Z^\tau Z'^{\tau'}$ with $Z^{\tau_1}Z'^{\tau_1'}$ such that $\sigma(Z, Z')\tau$ coincides with τ_1 on Z, that $\sigma(Z, Z')\tau'$ coincides with τ_1' on Z', and that $\sigma(Z, Z')$ coincides with σ_0 on $L^\tau L'^{\tau'}$. We order the set Σ by the convention that

$$(Z, Z', \sigma(Z, Z')) \leqq (U, U', \sigma(U, U'))$$

if $Z\subset U$, $Z'\subset U'$ and $\sigma(U, U')$ coincides with $\sigma(Z, Z')$ on $Z^\tau Z'^{\tau'}$. It is trivial to verify that in this ordered set every completely ordered subset has an upper bound. Hence, by Zorn's theorem, Σ has a maximal element, which we denote from now on by (Z, Z', σ). Theorem 2 will be proved if we can show that $Z=K$, $Z'=K'$.

Let y be an element of K, and assume for a moment that y is transcendental over Z. Then y^τ is transcendental over Z^τ and y^{τ_1} is transcendental over Z^{τ_1}. By Lemma 3, y is also transcendental over $Z^\tau Z'^{\tau'}$, and *a fortiori*, over $Z^\tau Z'^{\tau'}$. Similarly, y^{τ_1} is transcendental over $Z^{\tau_1}Z'^{\tau_1'}$. We set $U=Z(y)$; then it is possible to extend σ to an isomorphism σ^* of $U^\tau Z'^{\tau'}$ with $U^{\tau_1}Z'^{\tau_1'}$ in such a way that $\sigma^*(y^\tau)=y^{\tau_1}$. It follows that $\sigma^*\tau$ coincides with τ_1 on U and that $\sigma^*\tau'$ coincides with τ_1' on Z'. But this is contrary to the maximality of (Z, Z', σ).

It follows that K is algebraic over Z, and similarly that K' is algebraic over Z'.

Let us again consider the element $y\in K$; it is a root of an irreducible equation $F=0$ in Z. By Lemma 3, F^τ becomes in $Z^\tau Z'^{\tau'}$ a power of an irreducible polynomial F_1, and we have $F_1(y^\tau)=0$. The polynomial F_1^σ is irreducible in $Z^{\tau_1}Z'^{\tau_1'}$, and $F^{\sigma\tau}$ is a power of F_1^σ. On the other hand, we have $F^{\sigma\tau}=F^{\tau_1}$ and $F^{\tau_1}(y^{\tau_1})=0$, whence $F_1^\sigma(y^{\tau_1})=0$. Therefore, we may extend σ to an isomorphism σ^* of $Z^\tau Z'^{\tau'}(y^\tau)$ with $Z^{\tau_1}Z'^{\tau_1'}(y^{\tau_1})$ such that $\sigma^*(y^\tau)=y^{\tau_1}$. The isomorphism $\sigma^*\tau$ of $Z(y)$ into $K^{\tau_1}K'^{\tau_1'}$ coincides with the automorphism induced by τ_1 and $\sigma^*\tau'$ coincides on Z' with τ_1'. By the maximality property of (Z, Z', σ), we have $Z(y)=Z$, whence $K=Z$, and we see in the same way that $K'=Z'$, which completes the proof of Theorem 2.

COROLLARY. *Let K/k, K'/k be two extensions of k, and assume that k is q.a.c. in at least one of them. Then there exists only one type of composite extension of our two extensions.*

In fact, if k is q.a.c. in K', we may apply Theorem 2 with $L'=k'$. If we set $\sigma_0=\tau_1\tau^{-1}$, σ_0 is an isomorphism of L^τ with L^{τ_1} and $\sigma_0\tau$ coincides with τ_1 on L; it follows that σ_0 may be extended to an isomorphism of $(\mathfrak{K}, \tau, \tau')$ with $(\mathfrak{K}_1, \tau_1, \tau_1')$.

THEOREM 3. *Let $(\mathfrak{K}/k, \tau, \tau')$ be a composite extension of K/k, K'/k and let L, L' be fields which satisfy the conditions* (1), (2), (3) *of Theorem* 2. *Then $L^\tau L'^{\tau'}$ is q.a.c. in $\mathfrak{K}$.*

By Lemma 1, $L^\tau L'^{\tau'}$ is q.a.c. in $L^\tau K'^{\tau'}$; by Lemma 2, we see that $L^\tau K'^{\tau'}$ is q.a.c. in $K^\tau K'^{\tau'}$, because the extensions K^τ/k, $K'^{\tau'}/k$ are algebraically dissociated. Let α be an element of $\mathfrak{K}$ which is algebraic over $L^\tau L'^{\tau'}$; then, if p is the characteristic of k, the second result shows that, for s large enough, $\alpha^{p^s}\in L^\tau K'^{\tau'}$. Since α^{p^s} is also algebraic over $L^\tau L'^{\tau'}$, the first result shows that $(\alpha^{p^s})^{p^{s'}}=\alpha^{p^{s+s'}}\in L^\tau L'^{\tau'}$, for s' large enough, which proves Theorem 3.

COROLLARY. *If k is q.a.c. in both K and K', it is also q.a.c. in $K^\tau K'^{\tau'}$.*

PRINCETON UNIVERSITY