ON NORMAL KUMMER FIELDS OVER A NON-MODULAR FIELD*

BY

A. ADRIAN ALBERT

1. Let F be any non-modular field, p an odd prime, $\zeta \neq 1$ a pth root of unity. Suppose that μ in $F(\zeta)$ is not the pth power of any quantity of $F(\zeta)$ so that the equation $y^p = \mu$ is irreducible in $F(\zeta)$. Then the field $F(y, \zeta)$ is called a *Kummer*† *field over F*.

In the present paper we shall give a formal construction of all *normal* Kummer fields over F. This is equivalent to a construction of all fields $F(x)$ of degree p over F such that $F(x, \zeta)$ is cyclic of degree p over $F(\zeta)$. In particular we provide a construction of *all cyclic fields of degree p over F*.

We shall also apply the cyclic case to prove that a normal division algebra D of degree p over F is cyclic if and only if D contains a quantity y not in F such that $y^p = \gamma$ in F.

2. The equation

$$g(\xi) \equiv \xi^{p-1} + \xi^{p-2} + \cdots + \xi + 1 = 0$$

is irreducible in the field R of all rational numbers and has all the primitive pth roots of unity as roots. If F is any non-modular field, then $g(\xi)$ has an irreducible factor $h(\xi) = 0$ in F and with ζ as a root. The roots of $h(\xi) = 0$ are all powers of ζ and hence are in a sub-field L of $R(\zeta)$. But then the coefficients of $h(\xi) = 0$ are in L so that the group of $h(\xi)$ with respect to F is its group with respect to L. This latter group is the group of all the automorphisms of the cyclic field $R(\zeta)$ leaving the quantities of L invariant and is a sub-group of the group of $R(\zeta)$. Every sub-group of a cyclic group is cyclic, so that $h(\xi) = 0$ has a cyclic group generated by

$$T: \qquad \zeta \longleftrightarrow \zeta^t,$$

where t is an integer *belonging* to the degree n of $h(\xi) = 0$, $t^n \equiv 1 \pmod{p}$. We may write

$$(1) \qquad \zeta_k = \zeta^{t^{k-1}}, \quad \zeta_{n+1} = \zeta_1 = \zeta^{t^n} \qquad (k = 1, \cdots, n),$$

so that we have

* This paper is a revision and amplification of the paper *On cyclic equations of prime degree*, which I presented to the Society on December 27, 1933; it was received by the editors March 17, 1934.

† If F is the field of all rational numbers, then $F(y, \zeta)$ is the ordinary Kummer field of modern arithmetic. Our work is a generalization to any non-modular field of that special case.

(2) $$\zeta_k = \zeta^{t_k},\ t_k \equiv t^{k-1} \pmod{p},\ 1 \leqq t_k < p.$$

Then T is equivalent to the cyclic substitution $(\zeta_1, \zeta_2, \cdots, \zeta_n)$ on the roots of $h(\xi)=0$.

If λ and μ are any two quantities of $K=F(\zeta)$ we say that λ is p-equal to μ and write

(3) $$\lambda \underset{(p)}{=} \mu.$$

H. Hasse* has then given a purely algebraic proof of

Lemma 1. *If*

$$y^p \underset{(p)}{=} \mu \neq 1,$$

then $Z=K(y)$ is cyclic of prime degree p over K and with generating automorphism

S: $$y \longleftrightarrow \zeta y.$$

Conversely every cyclic field Z of degree p over K is equal to a field $K(y)$,

$$y^p \underset{(p)}{=} \mu \neq 1.$$

Moreover if also $Z=K(z)$, $z^p=\mu'$ in K, then

$$\mu' \underset{(p)}{=} \mu^a,$$

so that $z=\lambda y^a$ where λ is in K.

3. We now assume that Z is any normal field of degree pn over F containing $K=F(\zeta)$ of degree n over F. Then K is the set of all quantities of Z unaltered by a cyclic sub-group H of Z of order p and Z is cyclic of degree p over K. By Lemma 1, $Z=F(y, \zeta)$, $y^p=\mu$ in K and $H=(I, S, \cdots, S^{p-1})$ where S is given above. We can then decompose the group G of Z relative to H and write $G=H+H\sigma_1+\cdots+H\sigma_{n-1}$. Then $I, \sigma_1, \cdots, \sigma_{n-1}$ carry ζ to the other roots of the irreducible equation $h(\xi)=0$. In particular one $\sigma_i=\tau$ carries ζ to ζ^t.

We let $T=\tau^p$ so that T also carries ζ to ζ^t since $t^p \equiv t \pmod{p}$. Then τ^n leaves ζ unaltered and is in H. Hence $\tau^n=S^r$, $T^n=S^{pr}=I$.

The group G now has the decomposition $G=H+HT+\cdots+HT^{n-1}$. For otherwise $T^r=S^iT^j$ where $n>r>j$ so that $T^{r-j}=S^i$ leaves ζ unaltered, which is impossible. We have proved that

* *Bericht über Klassenkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 36 (1927), pp. 232–311, p. 262.

$$G = (S^i T^j) \qquad (i = 0, 1, \cdots, p-1; j = 0, 1, \cdots, n-1).$$

The group G has a cyclic sub-group (T^j) of order n and hence Z has a sub-field $F(x)$ of degree p over F. Moreover

$$y^{(T)} = \lambda y^r \qquad (\lambda \text{ in } K).$$

For $y^{(T)}$ in Z evidently generates $K(y)$ and we may apply Lemma 1. But

$$(4) \qquad y^{(TS)} = \lambda \zeta^r y^r = y^{(S^e T)} = \zeta^{et} \lambda y^r,$$

where $et \equiv r \pmod{p}$ so that $e \equiv rt^{n-1} \pmod{p}$. Hence $TS = S^e T$. Conversely if $TS = S^e T$ then $r \equiv et \pmod{p}$ is determined and we have proved*

THEOREM 1. *Let $F(x)$ have degree p over F and $F(x, \zeta) \equiv Z$ be normal over F. Then Z has the group*

$$(5) \qquad S^i T^j \qquad (i = 0, 1, \cdots, p-1; j = 0, 1, \cdots, n-1),$$

such that $S^p = T^n = I$, the identity automorphism, and

$$(6) \qquad TS = S^e T \qquad (0 < e < p).$$

Moreover $Z = F(y, \zeta)$ where $y^p = \mu$ in $F(\zeta)$,

$$(7) \qquad \zeta^{(T)} = \zeta^t, \; y^{(T)} = \lambda y^r, \; \zeta^{(S)} = \zeta, \; y^{(S)} = \zeta y, \; \mu^{(T)} \underset{(p)}{=} \mu^r,$$

and $r \equiv et \pmod{p}$.

Conversely every normal field $Z > F(\zeta)$ of degree p^n over $K = F(\zeta)$ is generated as a field $Z = F(y, \zeta)$, $y^p = \mu = \mu(\zeta)$ in $F(\zeta)$ such that

$$(8) \qquad \mu \underset{(p)}{\neq} 1, \quad \mu(\zeta^t) \underset{(p)}{=} \mu^r \qquad (1 \leqq r < p).$$

The group of Z is then given by (5), (6), (7) where e is determined by $r \equiv et \pmod{p}$ and Z contains a sub-field $F(x)$ of degree p over F, the field of all quantities of Z unaltered by the automorphism T.

It is evident that $F(x)$ is uniquely determined in the sense of equivalence and is generated by any quantity

$$(9) \qquad x = \sum_{i=0}^{p-1} \alpha_i(\zeta) y^i = \sum_{i=0}^{p-1} \alpha_i(\zeta^t) \lambda^i y^{ri}$$

for which at least one $\alpha_i \neq 0$ for $i > 0$. Moreover the equation

$$(10) \qquad \phi(\eta) \equiv (\eta - x)(\eta - x^{(S)}) \cdots (\eta - x^{(S^{p-1})})$$

has coefficients in F, is irreducible in F, and has x as a root. Hence Theorem 1

* A similar result was obtained by Hilbert for the case $F = R$.

gives a formal construction of all fields $F(x)$ of degree p over F with the property that $F(x, \zeta)$ is normal over F in terms of the construction of all quantities μ satisfying (8).

If in particular $F(y, \zeta)$ has an abelian group, then $F(y, \zeta)=F(x)\times F(\zeta)$, where $F(x)$ is cyclic over F. Conversely if $F(x)$ is cyclic over F, then $F(x) \times F(\zeta)=F(y, \zeta)$ has an abelian group, $e=1$, $r=t$ and we have

THEOREM 2. *Let μ range over all quantities of $F(\zeta)$ such that*

$$\mu \underset{(p)}{\neq} 1, \quad \mu(\zeta^t) \underset{(p)}{=} \mu^t. \tag{11}$$

Then $Z=F(x)\times F(\zeta)$ where $F(x)$ is cyclic of degree p over F. Conversely every cyclic field $F(x)$ of degree p over F is the uniquely defined sub-field of such an $F(\mu^{1/p}, \zeta)$.

4. We proceed now to the construction of the quantities μ. The condition

$$\mu \underset{(p)}{\neq} 1$$

is evidently an irreducibility condition depending intrinsically on F itself and so must remain in our final conditions. We first prove

LEMMA 2. *The integer r satisfies the congruence*

$$r^n \equiv 1 \pmod{p}. \tag{12}$$

For

$$\text{if } \mu^{(T)} \underset{(p)}{=} \mu^r \text{ then } \mu \underset{(p)}{=} \mu^{r^n}$$

and hence

$$\mu^{r^n-1} \underset{(p)}{=} 1.$$

But then if $y^p=\mu$ the quantity $y^{r^n-1}=\lambda y^s$ where $r^n-1\equiv s \pmod{p}$, $0\leqq s<p$ and λ is in $F(\zeta)$. But y^{sp} is then in $F(\zeta)$ so that $s=0$.

We have observed that $0<r<p$ so that there exists an integer ρ such that

$$\rho r \equiv 1 \pmod{p}. \tag{13}$$

We define

$$\rho_k \equiv \rho^{k-1} \pmod{p}, \qquad 1 \leqq \rho_k < p, \tag{14}$$

for all integer values of k, where $\rho_{n+1}=\rho_1=1$, and $\rho^{-\alpha}$, $\alpha>0$, is to be defined as a corresponding positive power of ρ. Then

$$r\rho_k \equiv \rho_{k-1} \pmod{p}. \tag{15}$$

We may then prove

LEMMA 3. *Let* λ *be any quantity of* $F(\zeta)$ *and define*

$$\mu = \prod_{k=1}^{n} \lambda(\zeta_k)^{\rho_k}. \tag{16}$$

Then

$$\mu^{(T)} = \mu(\zeta^t) \underset{(p)}{=} \mu^r. \tag{17}$$

For the automorphism T carrying ζ to ζ^t carries each ζ_k to ζ_{k+1}. Hence

$$\mu^{(T)} = \prod_{k=1}^{n} \lambda(\zeta_{k+1})^{\rho_k} \equiv \prod_{k=1}^{n} \lambda(\zeta_k)^{\rho_{k-1}}, \tag{18}$$

while, by (15),

$$\mu^r = \prod_{k=1}^{n} \lambda(\zeta_k)^{r\rho_k} \underset{(p)}{=} \mu(\zeta^t)$$

as desired.

Let now

$$\mu(\zeta^t) \underset{(p)}{=} \mu^r \text{ and } \mu \underset{(p)}{\neq} 1.$$

Then define

$$M = \prod_{k=1}^{n} \Lambda(\zeta_k)^{\rho_k} \tag{19}$$

where $\Lambda = \mu$. Then $\Lambda(\zeta_k) = \mu^{r^{k-1}}$ so that

$$\Lambda(\zeta_k)^{\rho_k} \underset{(p)}{=} \mu^{(r\rho)^{k-1}} \underset{(p)}{=} \mu \tag{20}$$

and hence

$$M \underset{(p)}{=} \mu^n. \tag{21}$$

But n is not divisible by p so that $z = y^n$ generates $K(y)$,

$$z^p \underset{(p)}{=} M.$$

Hence $F(y, \zeta) = F(w, \zeta)$ where $w^p = M$ is a quantity of the form (16). Conversely if μ has the form (16) and

$$\mu \underset{(p)}{\neq} 1$$

then $F(y, \zeta)$, $y^p = \mu$, is normal of degree np over F. We have proved

THEOREM 3. *Let λ range over all quantities of $F(\zeta)$ such that*

$$y^p = \mu \equiv \prod_{k=1}^{n} \lambda(\zeta_k)^{\rho_k} \underset{(p)}{\not\equiv} 1. \tag{22}$$

Then $F(y, \zeta)$ is a normal field of Theorem 1. Conversely every normal field of Theorem 1 is generated by a μ defined by (22).

We have now succeeded in giving a formal construction of all the fields of Theorem 1. In particular we have constructed all cyclic fields of prime degree over F. For this case we have $\rho t \equiv 1 \pmod p$, and may state

THEOREM 4. *Let $\rho_k \equiv t^{p-k} \pmod p$ so that $t\rho_k \equiv t^{p-(k-1)} \equiv \rho_{k-1} \pmod p$ and let λ range over all quantities of $F(\zeta)$ such that*

$$a = \prod_{k=1}^{n} \lambda(\zeta_k)^{\rho_k} \tag{23}$$

is not the pth power of any quantity b of $F(\zeta)$. Then if

$$z^p = a, \tag{24}$$

the field $F(z, \zeta)$ is cyclic of degree np over F and

$$F(z) = F(x) \times F(\zeta),$$

where $F(x)$ is cyclic of degree p over F. Conversely every cyclic field $F(x)$ of degree p over F is generated as the uniquely defined sub-field of such an $F(z, \zeta)$.

We have thus given a construction of all cyclic fields of prime degree over any non-modular field F where the condition $a \neq b^p$ is the irreducibility condition.

5. **On normal division algebras of degree p.** Let Z be a cyclic field of degree p over F so that every automorphism of Z is a power of an automorphism S given by $z \longleftrightarrow z^S$ for every z and corresponding z^S of Z. Define an algebra D whose quantities have the form

$$\sum_{i=0}^{p-1} z_i y^i \qquad (z_i \text{ in } Z), \tag{25}$$

such that

$$y^i z = z^{S^i} y^i, \quad y^p = \gamma \neq 0 \text{ in } F. \tag{26}$$

Then D is a cyclic algebra over F and is a normal division algebra if and only if $\gamma \neq N(z)$ for any z in Z. Evidently D is uniquely defined by Z, S, γ and we write

$$D = (Z, S, \gamma) = (Z, S, \delta), \quad \delta = N(c)\gamma \tag{27}$$

for any c of Z. For γ is replaced by δ when we replace y by cy. Also*

$$(Z, S, \gamma) \times (Z, S, \delta) \sim (Z, S, \gamma\delta). \tag{28}$$

If D is a cyclic normal division algebra of degree p over F, then D has the above form and hence contains a sub-field $F(y)$, $y^p = (\gamma)$ in F.

Conversely, let D be any normal division algebra of degree p over F with $F(x)$, $x^p = \beta$ in F as sub-field. Let $K = F(\zeta)$ of degree n over F. The algebra

$$M = (K, T, 1), \tag{29}$$

a cyclic algebra of degree n over F, is a total matric algebra. We form the direct product $M \times D$ which evidently contains $K \times D = D_0$ as sub-algebra. Algebra D_0 is a normal division algebra of degree p over K and has the cyclic sub-field $Z = K(x)$. Moreover

$$D_0 \doteq (Z, S, \gamma), \tag{30}$$

where γ is in K and the automorphism S is given by the transformation

$$yx = \zeta xy, \quad x^S \equiv \zeta x. \tag{31}$$

Let M have a basis $(\epsilon^i j^k)$ $(i, k = 0, 1, \cdots, n)$ such that $j^n = 1$. Then in $D \times M$ we have

$$j(yx)j^{-1} = y_T x = j(\zeta xy)j^{-1} = \zeta^t x y_T, \tag{32}$$

where $y_T = jyj^{-1}$ is in $D \times M$. But y is commutative with ζ since y is in D_0. Also $y\zeta = \zeta y$ implies that $y_T\zeta^t = \zeta^t y_T$ and hence y_T is also commutative with ζ. For $F(\zeta^t) = F(\zeta)$. The algebra of all quantities of $D \times M$ commutative with ζ is evidently D_0 so that y_T is in D_0.

Since $y_T x = \zeta^t x y_T$ while $y^t x = \zeta^t x y^t$, we then have $y_T = dy^t$ where d is in Z. Then

$$(y_T)^p = j\gamma j^{-1} = \gamma(\zeta^t) = N(d)\gamma^t, \tag{33}$$

where $N(d)$ is the norm of the quantity d of the cyclic field Z. But

$$D_0^t \sim (Z, S, \gamma^t) = (Z, S, \gamma(\zeta^t)), \tag{34}$$

by (33), (27).

* If A is any normal simple algebra, then $A = M \times D$, where the total matric algebra M and the normal division algebra D are uniquely determined in the sense of equivalence. If A and B are two normal simple algebras with the same D, we say that A and B are similar, and write $A \sim B$.

By applying (34) we have $D_0^{t^2} \sim (Z, S, \gamma(\zeta^{t^2}))$, and hence

$$D_0^{t_k} \sim (Z, S, \gamma(\zeta_k)),$$

from which, if $u = \sum \rho_k t_k = n + \lambda p$ by (25),

$$D_0^u \sim D_0^n \sim (Z, S, \alpha),$$

where

$$\alpha = \prod_{k=1}^{n} \gamma(\zeta_k)^{\rho_k}.$$

If D is any normal simple algebra of prime degree p over F, and K is a field of degree n not divisible by p, then D is a total matric algebra if and only if $D \times K$ over K is a total matric algebra. Moreover, if r is prime to p, then D^r is total matric if and only if D is total matric. Hence, if $D_0 = D \times K$ and D_0^r is a total matric algebra, then so is D.

Algebra D_0^n is a normal division algebra since D is a normal division algebra. Hence $\alpha \neq N(c)$ for any c of Z. In particular $\alpha \neq b^p$ for any b of K. Thus D_0 contains a cyclic field* W of prime degree p over F. But then $D_0^n \times W'$ over $W' \cong W_K$, the composite of W and K, is a total matric algebra. Hence $D_0 \times W'$ is a total matric algebra and so must be $D \times \overline{W}$ over $\overline{W}$, $\overline{W} \cong W$. But then D has a sub-field equivalent to W and is cyclic.

THEOREM 5. *A normal division algebra D of prime degree p over F is cyclic if and only if D has a sub-field $F(x)$, $x^p = \gamma$ in F.*

---

* The cyclic sub-field of $F(\alpha^{1/p})$ defined by Theorem 4.

THE INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.