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, $\xi \neq 1$ a $p$th root of
unity. Suppose that $\mu$ in $F(\xi)$ is not the $p$th power of any quantity of $F(\xi)$
so that the equation $\gamma^p = \mu$ is irreducible in $F(\xi)$. Then the field $F(\gamma, \xi)$ is
called a Kummer\dagger 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 $F(x, \xi)$ is cyclic of degree $p$ over $F(\xi)$. In par-
ticular 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 $\gamma$ not in $F$
such that $\gamma^p = \gamma$ in $F$.

2. The equation

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

is irreducible in the field $R$ of all rational numbers and has all the primitive
$p$th 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 $\xi$ as a root. The roots of $h(\xi) = 0$ are
all powers of $\xi$ and hence are in a sub-field $L$ of $R(\xi)$. 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 $R(\xi)$ leaving the quantities of $L$ invariant and is a sub-group of
the group of $R(\xi)$. Every sub-group of a cyclic group is cyclic, so that $h(\xi) = 0$
has a cyclic group generated by

$$T: \xi \mapsto \xi^t,$$

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

$$\xi_k = \xi^{k-1}, \quad \xi_{n+1} = \xi_1 = \xi^n \quad (k = 1, \ldots, n),$$

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 $F(\gamma, \xi)$ is the ordinary Kummer field of modern
arithmetic. Our work is a generalization to any non-modular field of that special case.

885
(2) \[ \xi_k = \xi^t_k, \ t_k = t^{k-1} \pmod{p}, \ 1 \leq t_k < p. \]

Then \( T \) is equivalent to the cyclic substitution \((\xi_1, \xi_2, \cdots, \xi_n)\) on the roots of \( h(\xi) = 0 \).

If \( \lambda \) and \( \mu \) are any two quantities of \( K = F(\xi) \) we say that \( \lambda \) is \( p \)-equal to \( \mu \) and write

(3) \[ \lambda \equiv \mu \pmod{p}. \]

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

**Lemma 1.** If

\[ y^p = \mu \neq 1, \pmod{p}, \]

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

\( S: \ y \mapsto \xi y. \)

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

\[ y^p = \mu \neq 1, \pmod{p}. \]

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

\[ \mu' \equiv \mu^a, \pmod{p}, \]

so that \( z = \lambda y^a \) where \( \lambda \) is in \( K \).

3. We now assume that \( Z \) is any normal field of degree \( pn \) over \( F \) containing \( K = F(\xi) \) 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, \( Z = F(y, \xi) \), \( y^p = \mu \) in \( K \) and \( H = (I, S, \cdots, S^{n-1}) \) where \( S \) is given above. We can then decompose the group \( G \) of \( Z \) relative to \( H \) and write \( G = H + HS_1 + \cdots + HS_{n-1} \). Then \( I, \sigma_1, \cdots, \sigma_{n-1} \) carry \( \xi \) to the other roots of the irreducible equation \( h(\xi) = 0 \). In particular one \( \sigma_i = \tau \) carries \( \xi \) to \( \xi^t \).

We let \( T = \tau^p \) so that \( T \) also carries \( \xi \) to \( \xi^t \) since \( t^p = t \pmod{p} \). Then \( \tau^a \) leaves \( \xi \) unaltered and is in \( H \). Hence \( \tau^a = S^r, \ T^a = S^{pr} = I \).

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

The group \( G \) has a cyclic sub-group \( (T^i) \) of order \( n \) and hence \( Z \) has a sub-field \( F(x) \) of degree \( p \) over \( F \). Moreover
\[
y^{(T)} = \lambda y^r
\]
(\( \lambda \) in \( K \)).

For \( y^{(T)} \) in \( Z \) evidently generates \( K(y) \) and we may apply Lemma 1. But
\[
y^{(TS)} = \lambda T y^r = y^{(ST)} = \xi^* \lambda y^r,
\]
where \( e \equiv r \pmod{p} \) so that \( e \equiv rt^{n-1} \pmod{p} \). Hence \( TS = S^*T \). Conversely if \( TS = S^*T \) then \( r \equiv et \pmod{p} \) is determined and we have proved

**Theorem 1.** Let \( F(x) \) have degree \( p \) over \( F \) and \( F(x, \xi) = Z \) be normal over \( F \). Then \( Z \) has the group
\[
S^*T^i \quad (i = 0, 1, \ldots, p - 1; j = 0, 1, \ldots, n - 1),
\]
such that \( S^p = T^n = I \), the identity automorphism, and
\[
TS = S^*T \quad (0 < e < p).
\]
Moreover \( Z = F(y, \xi) \) where \( y^p = \mu, \xi \) in \( F(\xi) \),
\[
\xi^{(T)} = \xi^t, \quad y^{(T)} = \lambda y^r, \quad \xi^{(S)} = \xi, \quad y^{(S)} = \xi y, \quad \mu^{(T)} = \mu^r, \quad \mu^{(S)} = \mu^s,
\]
and \( r \equiv et \pmod{p} \).

Conversely every normal field \( Z > F(\xi) \) of degree \( p^n \) over \( K = F(\xi) \) is generated as a field \( Z = F(y, \xi) \), \( y^p = \mu = \mu(\xi) \) in \( F(\xi) \) such that
\[
\mu \neq 1, \quad \mu^{(T)} = \mu^r \quad (1 \leq r < p).
\]
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
\[
x = \sum_{i=0}^{p-1} \alpha_i(\xi) y^i = \sum_{i=0}^{p-1} \alpha_i(\xi^i) \lambda^i y^i
\]
for which at least one \( \alpha_i \neq 0 \) for \( i > 0 \). Moreover the equation
\[
\phi(\eta) = (\eta - x)(\eta - x^{(S)}) \cdots (\eta - x^{(S^{p-1})})
\]
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 $\mu$ 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 $\mu$ range over all quantities of $F(\zeta)$ such that

$$\mu \neq 1, \quad (\mu^t) = \mu^t.$$  

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 $\mu$. The condition

$$\mu \neq 1, \quad (\mu)$$

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

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

For

$$\text{if } \mu(\tau) = \mu^r \text{ then } \mu = \mu^{rn}$$

and hence

$$\mu^{rn-1} = 1, \quad (\mu)$$

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

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

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

We define

$$\rho_k \equiv \rho^{k-1} \pmod{p}, \quad 1 \leq \rho_k < p,$$

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 $\rho$. Then

$$r \rho_k \equiv \rho_{k-1} \pmod{p}.$$
We may then prove

**Lemma 3.** Let \( \lambda \) be any quantity of \( F(\xi) \) and define

\[
\mu = \prod_{k=1}^{n} \lambda(\xi_k)^{\rho_k}.
\]

Then

\[
\mu^{(T)} = \mu(\xi^t) = \mu^r.
\]

For the automorphism \( T \) carrying \( \xi \) to \( \xi^t \) carries each \( \xi_k \) to \( \xi_{k+1} \). Hence

\[
\mu^{(T)} = \prod_{k=1}^{n} \lambda(\xi_{k+1})^{\rho_k} = \prod_{k=1}^{n} \lambda(\xi_k)^{\rho_k-1},
\]

while, by (15),

\[
\mu^r = \prod_{k=1}^{n} \lambda(\xi_k)^{\rho_k} = \mu(\xi^t),
\]

as desired.

Let now

\[
\mu(\xi^t) = \mu^r \quad \text{and} \quad \mu \not= 1.
\]

Then define

\[
M = \prod_{k=1}^{n} \Lambda(\xi_k)^{\rho_k}
\]

where \( \Lambda = \mu \). Then \( \Lambda(\xi_k) = \mu^{\rho_k-1} \) so that

\[
\Lambda(\xi_k)^{\rho_k} = \mu^{(\rho_k)^{\rho_k-1}} = \mu
\]

and hence

\[
M = \mu^n.
\]

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

\[
z^p = M.
\]

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

\[
\mu \not= 1
\]
then $F(y, \zeta), y^p = \mu$, is normal of degree $np$ over $F$. We have proved

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

\[(22) \quad y^p = \mu = \prod_{k=1}^{n} \lambda(\zeta_k)^{p_k} \neq 1.\]

Then $F(y, \zeta)$ is a normal field of Theorem 1. Conversely every normal field of Theorem 1 is generated by a $\mu$ 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 $\lambda$ range over all quantities of $F(\zeta)$ such that

\[(23) \quad a = \prod_{k=1}^{n} \lambda(\zeta_k)^{\rho_k}\]

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

\[(24) \quad z^p = a,
\]

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 $z \mapsto z^S$ for every $z$ and corresponding $z^S$ of $Z$. Define an algebra $D$ whose quantities have the form

\[(25) \quad \sum_{i=0}^{p-1} z_i y^i \quad (z_i \text{ in } Z),\]

such that

\[(26) \quad y^t z = z^{s^t} y^i, \quad y^p = \gamma \neq 0 \text{ in } F.\]

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

\[
D = (Z, S, \gamma) = (Z, S, \delta), \quad \delta = N(c)\gamma
\]

for any \( c \) of \( Z \). For \( \gamma \) is replaced by \( \delta \) when we replace \( \gamma \) by \( cy \). Also*

\[
(Z, S, \gamma) \times (Z, S, \delta) \sim (Z, S, \gamma\delta).
\]

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 \( K = F(\xi) \) of degree \( n \) over \( F \). The algebra

\[
M = (K, T, 1),
\]

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

\[
D_0 = (Z, S, \gamma),
\]

where \( \gamma \) is in \( K \) and the automorphism \( S \) is given by the transformation

\[
yx = \xi xy, \quad xs = \xi x.
\]

Let \( M \) have a basis \( \{e_i j^k\} \) \( (i, k = 0, 1, \ldots, n) \) such that \( j^n = 1 \). Then in \( D \times M \) we have

\[
j(yx)j^{-1} = y_T x = j(\xi xy)j^{-1} = \xi^t xy_T,
\]

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

Since \( y_T x = \xi^t xy_T \) while \( y^\xi x = \xi^t xy^\xi \), we then have \( y_T = dy^t \) where \( d \) is in \( Z \). Then

\[
(y_T)^p = jy^tj^{-1} = \gamma(\xi^t) = N(d)\gamma^t,
\]

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

\[
D_0^t \sim (Z, S, \gamma^t) = (Z, S, \gamma(\xi^t)),
\]

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 $D_0 \sim (Z, S, \gamma(t^k))$, and hence

$$D_0 \sim (Z, S, \gamma(t^k)),$$

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

$$D_0 \sim D_0 \sim (Z, S, \alpha),$$

where

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

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 $D_0$ is a normal division algebra since $D$ is a normal division algebra. Hence $\alpha \not= \mathcal{N}(c)$ for any $c$ of $Z$. In particular $\alpha \not= b^p$ for any $b$ of $K$. Thus $D_0$ contains a cyclic field $W$ of prime degree $p$ over $F$. But then $D_0 \times W'$ over $W' \subseteq W_K$, 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 $D \times W$ over $W$, $W \subseteq W$. 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 $F(a^{1/p})$ defined by Theorem 4.

**The Institute for Advanced Study,**

**Princeton, N. J.**