ON CYCLIC FIELDS*

BY

A. ADRIAN ALBERT

1. Introduction. The most interesting algebraic extensions of an arbitrary field $F$ are the cyclic extension fields $Z$ of degree $n$ over $F$. I have recently given constructions of such fields for the case $n = p; \dagger$ a prime, when the characteristic of $F$ is not $p$, and for the case $n = p^t \ddagger$ when the characteristic of $F$ is $p$. Moreover it is well known that when $F$ contains all the $n$th roots of unity then $Z = F(x), x^n = \alpha$ in $F$.

The last result above does not provide a construction of all cyclic fields $Z$ over $F$ since in general $F$ does not contain these $n$th roots. Moreover if we adjoin these roots to $F$ and so extend $F$ to a field $K$ the composite $(Z, K)$ over $K$ may not have degree $n$. Finally even if $(Z, K)$ over $K$ does have degree $n$ then it is necessary to give conditions that a given field $K(x), x^n = \alpha$ in $F$, shall have the form $(Z, K)$ with $Z$ cyclic over $F$. This has not been done and is certainly not as simple as the considerations I shall make here.

It is well known that if $n = \prod_{i=1}^t p_i^{e_i}$ with $p_i$ distinct primes, then $Z$ is the direct product $Z = Z_1 \times \cdots \times Z_t$ where $Z_i$ is cyclic of degree $p_i$ over $F$. Hence it suffices to consider the case $n = p^t, p$ a prime. I have already done so for the case where $F$ has characteristic $p$. In the present paper I shall make analogous considerations for the case where $F$ has characteristic not $p$ by first studying the case where $F$ contains a primitive $p$th root of unity $\xi$ and later giving complete conditions for the case where $F$ does not contain $\xi$.

2. Algebraic units of $Z$. Let $Z$ be cyclic of degree $n$ over a field $F$ and $S$ be a generating automorphism of the automorphism group of $Z$. Then we define the relative norm

$$N_{Z/F}(a) = a a_S \cdots a_S^{n-1},$$

a quantity of $F$ for every $a$ of $Z$. We shall now give a new proof of a theorem of Hilbert.||

* Presented to the Society, September 7, 1934; received by the editors July 30, 1934.
† See my paper in these Transactions, 1934, On normal Kummer fields over a non-modular field.
§ For let $Z$ be the field of the $2^{n+1}$ roots of unity so that $Z$ has degree $2^n$ over $\mathbb{Q}$, the rational field. Then $K$ is actually a sub-field of degree $2^{n-1}$ of $Z$ and $Z$ has degree $2$ over $K$.
|| Cf. Hilbert's Abhandlungen I, p. 149. Hilbert's proof uses the assumption that $F$ is infinite and is very different from the rather interesting proof given here. The proof here also goes more deeply into the true reason for the theorem.
Theorem 1. A quantity $a$ of $Z$ has the property

\[ N_{Z/P}(a) = 1 \]

if and only if there exists a quantity $b \neq 0$ of $Z$ such that

\[ a = b^s/b. \]

For obviously if $a$ has the form (3) then $N_{Z/P}(a) = N_{Z/P}(b)N_{Z/P}(b^{-1}) = 1$. Conversely let $N_{Z/P}(a) = 1$.

Consider the cyclic algebra $M$ whose quantities are all $\sum_{i=0}^{n-1} z_i y^i$ with $z_i$ in $Z$ and $1, y, \ldots, y^{n-1}$ left linearly independent in $Z$. Let

\[ y^t z = z^s y^i, \ y^n = 1 \quad (z \text{ in } Z), \]

so that $M$ is equivalent to the algebra of all $n$-rowed square matrices. Then $Z$ may be thought of as a field of $n$-rowed square matrices, $y$ is a matrix whose minimum equation is $y^n - 1 = 0$, its characteristic equation. The matrix $a^{-1}y = y_0$ has the property $y_0^n = N(a^{-1}) = 1$ and has the same minimum equation as $y$. Since this equation defines the only invariant factor of $y$ which is not unity, the two matrices $y$ and $y_0$ have the same invariant factors and are similar. Thus $y_0 = A y A^{-1}$ with $A = \sum z_i y^i \neq 0$ and

\[ yA = A y = \sum z_i S y^{i+1} = a \sum z_i y^{i+1}. \]

Then $az_i = z_i^S \neq 0$ for at least one $z_i$ so that we take $b = z_i \neq 0$.

3. Cyclic fields of degree $p^s$ over $K$. Let $K$ be a field of characteristic not $p$ containing a primitive $p^s$th root of unity $\zeta$ and let $Z$ be cyclic of degree $p^s$ over $K$, $s > 1$. Then $Z$ contains a unique cyclic sub-field $Y$ of degree $m = p^{s-1}$ and $Z$ is cyclic of degree $p$ over $Y$. But then

\[ Z = Y(z), \ z^p = a \text{ in } Y. \]

Let $S$ be a generating automorphism of $Z$ so that $S$ may also be considered as a generating automorphism of $Y$. Then $S^m = Q, Q^p = I$, the identity automorphism of $Z$, and $Y$ is the set of all quantities of $Z$ unaltered by the cyclic group $(I, Q, \ldots, Q^{p-1})$.

We compute $(z^Q)^p = a^Q = a$. Then $z^Q$ is a root of $\omega^p = a$ and hence

\[ z^Q = \zeta^\mu z \quad (0 \leq \mu < p). \]

If $\mu = 0$ then $z^Q = z$ is in $Y$ contrary to our hypothesis that $Z = Y(z) \neq Y$. Hence $\mu > 0$ is prime to $p$,

\[ \mu \mu_0 = 1 + \mu_1 p, \quad (\mu_0, \ p) = 1, \]

for integers $\mu_0, \mu_1$. Define $S_0 = S^{\mu_0}, Q_0 = Q^{\mu_1}$ so that $S_0$ is a generating auto-

* For every cyclic field of degree $p$ over $Y$ containing $\zeta$ is a Kummer field $Y(z), z^p = a$ in $Y$.
morphism of \( Z \), \( Q_0 \) is a generator of the group \((I, Q, \ldots, Q^{p-1})\). Then 
\[ z_0^\mu = \xi^\mu z_0 = \xi z. \]
Hence by properly choosing \( S \) we may assume 
\[ z^Q = \xi z, \]
instead of (6).

Now \((z^S)^p = a^S\) so that, by a well known theorem on Kummer fields,\(^*\) we have 
\[ z^s = \beta z, \beta \in Y, 1 \leq \nu < p. \]
Then 
\[ z^{s^2} = \beta^{s^2} \beta^s z = \beta^{s^2} \beta^s = \beta z, \]
and hence \( z^{s^m-1} = \beta^{p-1} z \) is in the field \( Y \). But then \( \nu^m = 1 \) (mod \( p \)) and, since \( m = p^{e-1} \) so that \( \nu^m = \nu \) (mod \( p \)) we have \( \nu = 1 \) (mod \( p \), \( \nu = 1 \).

Then 
\[ z^S = \beta z, \beta \in Y. \]

Also 
\[ z^{s^2} = \beta^{s^2} \beta z, \ldots, z^{s^m} = z^Q = \beta^{s^m-1} \beta^s \beta z \]
and
\[ N_{Y/K}(\beta) = \xi. \]

The quantity \( \beta \) is in \( Y \) and has the property (10) so that 
\[ N_{Y/K}(\beta^p) = \xi^p = 1. \]
By Theorem 1 applied in \( Y \) we have 
\[ \beta^p = \frac{\alpha^S}{\alpha}, \quad \alpha \in Y. \]
But now \( a^S = (z^S)^p = \beta^p a \) so that 
\[ (\alpha a^{-1})^S = \alpha a^{-1}, \]
and hence \( \alpha = \lambda a \) with \( \lambda \) in \( K \).

We may finally prove that in fact \( Z = K(z) \). This will obviously be true if \( z^p = a \) generates \( Y \). Hence let \( a \) be in a proper sub-field of \( Y \). Then \( a \) is in the unique sub-field \( H \) of degree \( p^{e-2} \) of \( Y \) and if \( m = pr, R = S^r \), we have 
\[ R^p = Q, a^R = a. \]
Then \( a^S = a\beta^p, a^R = a(\beta\beta^{s^2} \cdots \beta^{s^p-1}) = a \) so that \([N_{H/K}(\beta)]^p = 1, N_{H/K}(\beta) = \xi, N_{Y/K}(\beta) = \xi^p = 1 \), a contradiction. We have proved

**Theorem 2.** Let \( Z \) be a cyclic field of degree \( p^e \) over \( K \), \( e > 1 \), \( S \) be a generating automorphism of \( Z \), and \( Y \) its unique sub-field of degree \( p^{e-1} \) over \( K \). Then \( Z = K(z) \) where \( z^p = a \) in \( Y \) and \( Y \) contains a quantity \( \beta \) such that 
\[ N_{Y/K}(\beta) = \xi, a^S = \beta^p. \]

Moreover the generating automorphism $S$ of $Z$ is given by that in $Y$ and
\begin{equation}
    z^8 = \beta z.
\end{equation}

We may now prove

**Theorem 3.** A necessary and sufficient condition that a cyclic field $Y$ of degree $p^{e-1}$ over $K$, $e > 1$, shall possess cyclic overfields of degree $p^e$ over $K$ is that $Y$ shall contain a quantity $\beta$ such that $N_{Y/K}(\beta) = \xi$. Every such cyclic overfield* is a field $K(z)$, $z^p = a_0$, with generating automorphism (14), where $a_0 = \lambda a$, $a$ is any root of
\begin{equation}
    a^8 a^{-1} = \beta^p,
\end{equation}
and $\lambda$ ranges over all quantities of $K$.

For if $Z$ is cyclic of degree $p^e$ over $K$ then the existence of $\beta$ is given by Theorem 2. Conversely let $N_{Z/K}(\beta) = \xi$ for $\beta$ in $Y$. By Theorem 1 there exists a quantity $a$ in $Y$ such that (15) is satisfied. If $a = b^p$ for $b$ in $K$ then $a^8 a^{-1} = (b^8 b^{-1})^p = \beta^p$, $\beta = \xi b^8 b^{-1}$, $N_{Y/K}(\beta) = 1$, a contradiction. Hence the field $Z = Y(z)$, $z^p = a_0$, has degree $p$ over $Y$ for every solution $a_0$ of $a^8 a^{-1} = \beta^p$. Moreover $a_0 = \lambda a$ for any fixed solution $a$. In our proof of Theorem 2 we showed that in fact $Y = K(a_0)$ so that $Z = K(z)$. Finally $Z$ is evidently a field of Theorem 2 and is cyclic with generating automorphism given by that in $Y$ and by (14).

Suppose now that $Z_0$ is a new cyclic overfield of $Y$ of degree $p^e$ over $K$ so that $Z_0$ defines a quantity $\beta_0$ with $N_{Y/K}(\beta_0) = \xi$. Then $N_{Y/K}(\beta_0 \beta^{-1}) = 1$ and
\begin{equation}
    \beta_0 = \beta d^8 d^{-1},
\end{equation}
with $d$ in $Y$ by Theorem 1. Moreover $Z_0 = K(z_1)$, $z_1^p = a_1$, where $a_1^8 a_1^{-1} = \beta_0 p$. But if $a_{01} = \lambda a d^p$ with $\lambda$ in $K$ and $a^8 a^{-1} = \beta p$, then $a_{01}^8 a_{01}^{-1} = \beta^p (d^8 d^{-1})^p = \beta_0 p$. But then $a_{01}$ is a constant multiple of $a_1$, and, by proper choice of $\lambda$, $a_1 = a_{01} = \lambda a d^p$. The field $Z_0 = K(z)$, $z = d^{-1} z_1$, $z^p = \lambda a$ is evidently equivalent to $K(z)$. Moreover $z^8 = (d^8)^{-1} z_1^8 = (d^8)^{-1} \beta d^8 d^{-1} z = \beta z$ as desired.

We have determined the structure of cyclic fields of degree $p^e$ over $K$ when $K$ contains a primitive $p$th root of unity $\xi$. We now study the more general case where $\xi$ is not in the reference field $F$.

4. The field $K = F(\xi)$. Let $F$ be any field of characteristic not $p$ so that the equation $x^p = 1$ is separable and has as roots the primitive $p$th roots of unity
\begin{equation}
    \xi^i \quad (i = 1, 2, \cdots, p - 1),
\end{equation}

* Such cyclic overfields define new quantities $\beta_0$ but we prove below that in fact we may replace $\beta_0$ by $\beta$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
and unity itself. Suppose that \( h(x) \) is the irreducible factor in \( F \) of \( x^p - 1 \) which has \( h \) as a root. Then the field \( K = F(\zeta) \) is a normal field whose automorphisms form a group which is isomorphic to a subgroup of the cyclic group of order \( p - 1 \) which replaces \( \zeta \) by its powers (17). Every subgroup of a cyclic group is cyclic and hence \( K \) is cyclic of degree \( n \) over \( F \). Moreover a generating automorphism of \( K \) over \( F \) is given by

\[
T: \quad \zeta \mapsto \zeta^t
\]

where \( n \) divides \( p - 1 \) and is prime to \( p \), \( t \) is an integer belonging to the exponent \( n \) \((\text{mod } p)\),

\[
i^n \equiv 1 \pmod{p}, \quad t^e \not\equiv 1 \pmod{p}, \quad e < n.
\]

If we define

\[
\zeta_k = \zeta^t, \quad t_k \equiv t^{k-1} \pmod{p}, \quad 1 \leq t < p,
\]

\[
\rho \equiv 1 \pmod{p}, \quad \rho_k \equiv \rho^{k-1} \pmod{p},
\]

then I have proved*

**Lemma 1.** A quantity \( \mu = \mu(\zeta) \) of \( I \) has the property

\[
\mu^r = \mu(\zeta^r) = \delta^r \mu^r,
\]

with \( \delta \) in \( K \) if and only if there exists a quantity \( \lambda = \lambda(\zeta) \) in \( K \) such that

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

We shall also require the known*

**Lemma 2.** A cyclic field \( Z_0 \) of degree \( p \) over \( K \), \( Z_0 = K(\varepsilon) \), \( \varepsilon^p = \mu \) in \( K \), is cyclic of degree \( pn \) over \( F \), so that

\[
Z_0 = Z \times K,
\]

where \( Z \) is cyclic of degree \( p \) over \( F \), if and only if \( \mu \) satisfies (21).

5. Cyclic fields of degree \( p^e \) over \( F \). Let \( Z \) be cyclic of degree \( p^e \) over \( F \). Then \( Z_0 = Z \times K \) is evidently cyclic of degree \( np^e \) over \( F \) and cyclic of degree \( p^e \) over \( K \). Moreover \( Z \) contains a cyclic field \( Y \) of degree \( p^{e-1} \) over \( F \) and the field \( Y_0 = Y \times K \) is cyclic of degree \( np^{e-1} \) over \( F \) with automorphism group

\[
S^iT^j \quad (i = 0, 1, \ldots, p^{e-1} - 1; j = 0, 1, \ldots, n - 1).
\]

By Theorem 2 we have

* Cf. On normal Kummer fields, etc., Lemma 3, Theorem 2.
Theorem 4. Let \( Z, Z_0, Y, Y_0 \) be defined as above. Then \( Y_0 \) contains a quantity \( \beta \) such that

\[
N_{Y_0/K}(\beta) = \zeta
\]

and \( Z_0 = Y_0(z), z^p = \alpha \) in \( Y_0 \) such that

\[
\alpha^p \alpha^{-1} = \beta_0^p.
\]

Let \( a \) be a fixed quantity satisfying the equation (25) in \( \alpha \) so that every solution \( \alpha \) of (25) satisfies the condition

\[
\alpha = \lambda a, \lambda \text{ in } K.
\]

Then we have proved that \( z \) may always be chosen so that

\[
z^\delta = \beta z,
\]

for any \( \beta \) satisfying (24). We may then normalize the quantity \( \beta \) and prove

Theorem 5. The quantities \( \beta, a \) may be chosen so that

\[
\beta^T = \delta^p \beta^t, \quad a^T = d^p a^t,
\]

with \( \delta, d \) in \( Y \).

For we have \( a^g = a \beta^r \) and may define

\[
\beta_0 = \prod_{k=1}^n \beta(\zeta_k)^{\rho_k}, \quad a_0 = \prod_{k=1}^n a(\zeta_k)^{\rho_k},
\]

so that by Lemma 1 we have \( \beta_0^T = \delta^p \beta_0^t, a_0^T = d^p a_0^t \). Since \( ST = TS \) in \( Y \), we also have

\[
a_0^g a_0^{-1} = \prod_{k=1}^n [\beta(\zeta_k)^{\rho_k}] [a(\zeta_k)^{\rho_k}]^{-1}
\]

\[
= \prod_{k=1}^n \beta(\zeta_k)^{\rho_k} = \beta_0^g.
\]

We also compute

\[
N_{Y_0/K}(\beta_0) = \prod_{k=1}^n N_{Y_0/K} \beta(\zeta_k)^{\rho_k} = \prod_{k=1}^n \zeta_k^{\rho_k} = \zeta^r
\]

where

\[
\tau = \sum_{k=1}^n t_k \rho_k = \sum_{k=1}^n (t \rho)^{k-1} = n \pmod p.
\]

Hence \( N_{Y_0/K}(\beta_0) = \zeta^n \). We let \( \mu n \equiv 1 \pmod p \), \( \beta_1 = \beta_0^\mu \), \( a_1 = a_0^\mu \) so that
and obviously
\[(33) \quad a_1s_1^{-1} = \beta_1^p.\]
Moreover
\[(34) \quad \beta_1T = (\beta_0^s)^{\mu} = (\delta_0^s\beta_0^t)^{\mu} = (\delta_0^s)^p\beta_1^t = \delta_0^p\beta_1^t,\]
\[(35) \quad a_1T = (a_0^s)^{\mu} = (d_0^s a_0^t)^{\mu} = (d_0^s)^p a_1^t = d_0^p a_1^t,\]
as desired. We have proved Theorem 5.

The automorphisms $S$ and $T$ of $Y$ are commutative so that $N(\beta^T) = [N(\beta)]^T = \xi^t = N(\beta^t)$ with $N(\beta)$ defined as $N_{Y/K}(\beta)$. Then by Theorem 1
\[(36) \quad \beta^T = f{\xi^T}^{-1}\beta^t\]
with $f$ in $Y_0$. Also
\[(37) \quad (a^s a^{-1})^T = (\beta^T)^p = a^T s(a^T)^{-1} = (d^s d^{-1})^p (a^s a^{-1})^t = (d^s d^{-1})^p \beta^t,\]
so that
\[(38) \quad \beta^T = \xi^t d^s d^{-1} \beta^t \quad (0 \leq \nu < p).\]
We shall only need (38) and $a^T = d^p a^t$ in our further study of the field $Z$.

We now take as basic in our study the given field $Y_0 = Y \times K$ of degree $p^{-1}$ over $K$ where $Y_0$ is also cyclic of degree $n p^{-1}$ over $F$ and assume that $Y_0$ contains a quantity $\beta$ such that $N_{Y_0/K}(\beta) = \xi$. We have then shown that there always exists a quantity $a$ of $Y$ such that $a^s a^{-1} = \beta^p$ and moreover that $\beta$ and $a$ may be so chosen that (38) and
\[(39) \quad a^T = d^p a^t \quad (d \text{ in } Y)\]
both hold. We now seek necessary and sufficient conditions that $Y$ shall possess cyclic overfields of degree $p^e$ over $F$. We shall in fact prove the fundamental result

**Theorem 6.** The field $Y$ possesses cyclic overfields $Z$ of degree $p^e$ over $F$ if and only if in (38) $\nu = 0$. Moreover every such field is determined by $Z_0 = Y_0(\alpha)$, $z^p = \alpha$ in $Y$ such that
\[(40) \quad \alpha = \lambda a, \quad \lambda^T = \sigma^p \lambda^t\]
with $\sigma$ in $K$, where then $Z_0 = Z \times K$, $Z_0$ is cyclic of degree $n p^e$ over $F$.

For we may write $Y_0 = Y(\xi)$ so that if $Z$ is cyclic of degree $p^e$ over $F$ with
Y as sub-field then \( Z_0 = Y_0(z) \), \( z^p = \alpha = \lambda \beta \) with \( \lambda \) in \( K \). Moreover \( Z \) is cyclic of degree \( \rho \) over \( Y \) and by Lemma 2 we have

\[
\alpha^\rho = \psi^{\psi^\rho}
\]

with \( \psi \) in \( Y \). Hence

\[
\lambda^\rho = \lambda^\rho d^\rho \alpha^\rho = \psi^\rho \lambda^\rho \alpha^\rho,
\]

and

\[
\lambda^\rho = (\psi d^{-1})^\rho \lambda^\rho.
\]

The quantity \( x_1 = d^{-1} \psi \) has its \( \rho \)th power \( x_1^\rho = \rho = \lambda^\rho \lambda^{-\rho} \) in \( K \). Hence either \( \psi = d \sigma \) with \( \sigma \) in \( K \) or \( X_{10} = K(x_1) \) is a cyclic sub-field of \( Y_0 \) of degree \( \rho \) over \( K \). But \( Y_0 = Y \times K \) so that then \( X_{10} = X_1 \times K \) where \( X \) is cyclic of degree \( \rho \) over \( F \) and in fact

\[
\rho^\rho = \sigma^\rho \rho^\rho,
\]

with \( \gamma \) in \( K \). Then \( \lambda^\rho = \lambda^\rho \rho^\rho \) implies

\[
\lambda^\rho = \lambda^\rho \rho^\rho = \lambda^\rho \sigma \rho^\rho,
\]

so that finally

\[
\lambda^\rho = \gamma^\rho \lambda^\rho \rho^\rho = \gamma^\rho \lambda^\rho \rho^\rho.
\]

The quantity \( \lambda^\rho = \lambda^\rho \rho^\rho \) since \( t^\rho \equiv 1 \pmod{\rho} \). Hence \( \rho^\rho \) is the \( \rho \)th power of a quantity of \( K \) where \( \phi = nt^{\rho-1} \) is prime to \( \rho \). This evidently implies that \( \rho \) is the \( \rho \)th power of a quantity of \( K \) contrary to hypothesis. Hence \( x_1 = \sigma \) in \( K \) and we have proved that (40) holds.

We have shown that \( z \) may be so chosen that \( z^S = \beta z \) with (38), (39). Then (38) may be replaced by

\[
\beta^\rho = \gamma^\rho (\psi^S \psi^{-1}) \beta^\rho,
\]

since \( \psi = \sigma d, \psi^S = \sigma d^S \).

Since \( ST = TS \) in \( Z \) we obtain \( (z^\rho)^\rho = \alpha^\rho = \psi^\rho \alpha^\rho = \psi^\rho z^\rho \), \( z^\rho = \gamma^\rho \psi z^\rho \) with \( 0 \leq \epsilon < \rho \). Then \( z^S = \beta z \) gives

\[
z^\rho z = \gamma^\rho \psi z \beta^\rho = z^\rho \beta = (\beta^\rho)^\rho = \gamma^\rho \psi z^\rho \beta^\rho,
\]

so that \( \gamma^\rho = 1, \nu = 0 \).

Conversely let \( Y \) be cyclic of degree \( \rho^{-1} \) over \( F \), \( Y_0 = Y \times K \), \( \beta \) and \( a \) be chosen in \( Y_0 \) and satisfying \( N_{Y_0/K}(\beta) = \gamma \), (38), (39). Let \( \lambda \) range over all quantities of \( K \) such that (40) holds so that \( \alpha \) satisfies (47). We have proved
that then $Z_0 = Y_0(z)$ has the property $Z_0 = K(z)$ and is cyclic of degree $p^e$ over $K$. It remains merely to show that then $Z_0$ is actually cyclic of degree $p^n$ over $F$ if $v = 0$. We define the automorphism $T$ of $Z_0$ by that in $Y_0$ and by

$$z^T = \psi z^t, \; \psi = \sigma d,$$

where $\alpha^T = \psi \sigma^t$. Then we require only to show that $ST = TS$ so that the automorphism group of $Z_0$ over $F$ is actually the cyclic group $(S^iT^j)$ ($i = 0, 1, \cdots, p^e - 1; j = 0, 1, \cdots, n-1$). But this immediately follows from the computation in (48) with $e = 0$, and Theorem 6 is proved.

University of Chicago,
Chicago, Ill.