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 $n = p^\ell, ^\ddagger$ 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 $n = p_1^{\ell_1} \cdots p_t^{\ell_t}$ 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 $p$ over $F$. Hence it suffices to consider the case $n = p^\ell, p$ a prime. I have already done so$^\ddagger$ 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 $\zeta$ and later giving complete conditions for the case where $F$ does not contain $\zeta$.

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

\begin{equation}
N_{Z/F}(a) = aaS \cdots aS^{n-1},
\end{equation}

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. The results and proofs hold if $F$ is any field of characteristic not $p$.
§ For let $Z$ be the field of the $2^{n+1}$ roots of unity so that $Z$ has degree $2^n$ over $R$, 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.

454

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
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

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

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

$y A = a A y = \sum z_i S y^{i+1} = a \sum z_i y^{i+1}.$

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 $p^e$ over $K$. Let $K$ be a field of characteristic not $p$ containing a primitive $p^e$th root of unity $\zeta$ and let $Z$ be cyclic of degree $p^e$ over $K$, $e > 1$. Then $Z$ contains a unique cyclic sub-field $Y$ of degree $m = p^{e-1}$ 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 $(I, Q, \cdots, Q^{p-1})$.

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 $Y$.  

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
morphism of \( Z, \) \( Q_0 \) is a generator of the group \((I, Q, \cdots, Q^{p-1})\). Then \( z^{Q} = \xi^m z = z \). Hence by properly choosing \( S \) we may assume

\[
(8) \quad z^Q = \xi z,
\]

instead of (6).

Now \((z^b)^p = a^S\) so that, by a well known theorem on Kummer fields,\(^*\) we have \( z^S = b \xi^a, \beta \) in \( Y, 1 \leq \nu < p \). Then

\[
z^{S^2} = \beta^2 \beta^2 z^S = \beta^2 \beta \xi \theta, \quad \cdots, \quad z^{S^m} = \beta^m \xi \theta = z^Q = \xi z
\]

and hence \( z^{m-1} = \beta^{-1} \xi \) is in the field \( Y \). But then \( \nu = 1 \) (mod \( p \)) and, since \( m = p^{e-1} \) so that \( \nu = \nu (\text{mod } p) \) we have \( \nu = 1 \) (mod \( p \)), \( \nu = 1 \).

Then

\[
(9) \quad z^S = \beta z, \quad \beta \text{ in } Y.
\]

Also

\[
z^{S^2} = \beta^2 \beta z, \quad \cdots, \quad z^{S^m} = z^Q = \xi \theta = \beta^m \xi \theta
\]

and

\[
(10) \quad N_{Y/K}(\beta) = \xi.
\]

The quantity \( \beta \) is in \( Y \) and has the property (10) so that \( N_{Z/K}(\beta) = N_{Y/K}(\beta^p) = \xi = 1 \). By Theorem 1 applied in \( Y \) we have

\[
(11) \quad \beta^p = \frac{\alpha^S}{\alpha}, \quad \alpha \text{ in } Y.
\]

But now \( a^S = (z^S)^p = \beta^p a \) so that

\[
(12) \quad (\alpha \theta^{-1})^S = \alpha \theta^{-1},
\]

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 \( m = p r, R = S^r \), we have \( R^p = Q, a^R = a \). Then \( a^S = a \beta^p, a^R = a(\beta \beta^S \cdots \beta^{r-1})^p = a \) so that \([N_{H/K}(\beta)]^p = 1, N_{H/K}(\beta) = \xi, N_{Y/K}(\beta) = \xi \theta^p = 1 \), 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

\[
(13) \quad N_{Y/K}(\beta) = \xi, \quad a^S a^{-1} = \beta^p.
\]

Moreover the generating automorphism $S$ of $Z$ is given by that in $Y$ and
\begin{equation}
    z^g = \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 $N_{Z/K}(\beta) = \zeta$. Every such cyclic overfield is a field $K(z^p), z^p = a_0$, with generating automorphism (14), where $a_0 = \lambda a$, $a$ is any root of
\begin{equation}
    a^g 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 $N_{Z/K}(\beta) = \zeta$ 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 $a^g a^{-1} = (b^g b^{-1})^p = \beta^p$, $\beta = \zeta^y b^g b^{-1}$, $N_{Y/K}(\beta) = 1$, a contradiction. Hence the field $Z = Y(z^p), z^p = a_0$, has degree $p$ over $Y$ for every solution $a_0$ of $a^g a^{-1} = \beta^p$. 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 $N_{Y/K}(\beta_0) = \zeta$. Then $N_{Y/K}(\beta_0 \beta^{-1}) = 1$ and
\begin{equation}
    \beta_0 = \beta d^g d^{-1},
\end{equation}
with $d$ in $Y$ by Theorem 1. Moreover $Z_0 = K(z_1), z_1^p = a_1$, where $a_1^g a_1^{-1} = \beta_0 p$. But if $a_0 = \lambda a d^p$ with $\lambda$ in $K$ and $a^g a^{-1} = \beta p$, then $a_0^g a_0^{-1} = \beta p (d^g d^{-1})^p = \beta_0 p$. But then $a_0$ is a constant multiple of $a_1$, and, by proper choice of $\lambda$, $a_1 = a_0 = \lambda a d^p$. The field $Z_0 = K(z^p), z = d^{-1} z_1, z^p = \lambda a$ is evidently equivalent to $K(z)$. Moreover $z^g = (d^g)^{-1} a_1^g = (d^g)^{-1} \beta d^g d^{-1} z = \beta z$ as desired.

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

4. The field $K = F(\zeta)$. Let $F$ be any field of characteristic not $p$ so that the equation $x^p = 1$ is separable and has as roots the primitive $p^e$th roots of unity
\begin{equation}
    \zeta^i \quad (i = 1, 2, \ldots, 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 http://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 \( n \) (mod \( p \)),

\[
t^n \equiv 1 \pmod{p}, \quad t^e \not\equiv 1 \pmod{p}, \quad 0 < e < n.
\]

If we define

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

\[
r_k \equiv 1 \pmod{p}, \quad r_k \equiv r^{k-1} \pmod{p},
\]

then I have proved*

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

\[
\mu^T = \mu(\zeta^t) = \delta^e \mu^t,
\]

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

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

We shall also require the known*

**Lemma 2.** A cyclic field \( Z_0 \) of degree \( p \) over \( K \), \( Z_0 = K(\zeta) \), \( \zeta^p = \mu \) in \( K \), is cyclic of degree \( np \) 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 \( p^* \) over \( F \). Let \( Z \) be cyclic of degree \( p^* \) over \( F \). Then \( Z_0 = Z \times K \) is evidently cyclic of degree \( np^* \) over \( F \) and cyclic of degree \( p^* \) over \( K \). Moreover \( Z \) contains a cyclic field \( Y \) of degree \( p^{*i-1} \) over \( F \) and the field \( Y_0 = Y \times K \) is cyclic of degree \( np^{*i-1} \) over \( F \) with automorphism group

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

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

$$\alpha^{\delta} \alpha^{-1} = \beta^p.$$

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

$$\alpha = \lambda \alpha, \lambda \in K.$$ 

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 $\beta, \alpha$ may be chosen so that

$$\beta^T = \delta^\varphi \beta^t, \alpha^T = d^\varphi \alpha^t,$$

with $\delta, d$ in $Y$.

For we have $a^T = a\beta^t$ and may define

$$\beta_0 = \prod_{k=1}^n \beta(\xi_k)^{p^k}, \quad a_0 = \prod_{k=1}^n a(\xi_k)^{p^k},$$

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

$$a_0^T a_0^{-1} = \prod_{k=1}^n [\beta^T(\xi_k)^{p^k}] [a(\xi_k)^{p^k}]^{-1}$$

$$= \prod_{k=1}^n \beta(\xi_k)^{p^k} \cdot \delta^\varphi = \beta^T.$$

We also compute

$$N_{Y_0/K}(\beta_0) = \prod_{k=1}^n N_{Y_0/K} \beta(\xi_k)^{p^k} = \prod_{k=1}^n \xi_k^{p^k} = \zeta^T$$

where

$$\tau = \sum_{k=1}^n t_k p^k \equiv \sum_{k=1}^n (t \rho)^{k-1} \equiv n \pmod{p}.$$ 

Hence $N_{Y_0/K}(\beta_0) = \zeta^\tau$. We let $\mu n \equiv 1 \pmod{p}, \beta_1 = \beta^\varphi, a_1 = a^\varphi$ so that
\( N_{Y_s/K}(\beta) = \zeta^m = \zeta, \)

and obviously
\[ a_1^S a_1^{-1} = \beta_1^p. \]

Moreover
\[ \beta T = (\beta_0 T)^m = (\delta_0^p \beta_0^t)^m = (\delta_0^p)^m \beta_1 t = \delta_0^p \beta_1 t, \]
\[ a T = (a_0 T)^m = (d_0^p a_0^t)^m = (d_0^p)^m a_1 t = d_0^p a_1 t, \]
as desired. We have proved Theorem 5.

The automorphisms \( S \) and \( T \) of \( Y \) are commutative so that \( N(\beta) = [N(\beta)]T = \zeta = N(\beta_0) \) with \( N(\beta) \) defined as \( N_{Y_s/K}(\beta) \). Then by Theorem 1
\[ \beta T = f S f^{-1} \beta_0 \]
with \( f \) in \( Y_0 \). Also
\[ (a^S a^{-1}) T = (\beta T)^p = a T S (a T)^{-1} = (d^S d^{-1})^p (a^S a^{-1}) T \]
\[ = (d^S d^{-1})^p \beta T, \]
so that
\[ \beta T = \zeta^* d^S d^{-1} \beta T \]
(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 \( p^t \) over \( K \) where \( Y_0 \) is also cyclic of degree \( np^t-1 \) over \( F \) and assume that \( Y_0 \) contains a quantity \( \beta \) such that \( N_{Y_s/K}(\beta) = \zeta \). 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
\[ a T = d^p a^t \]
both hold. We now seek necessary and sufficient conditions that \( Y \) shall possess cyclic overfields of degree \( p^t \) over \( F \). We shall in fact prove the fundamental result

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

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

$$\alpha^T = \psi^p \alpha^t$$

with $\psi$ in $Y$. Hence

$$\lambda^T a^T = \lambda^T d^p a^t = \psi^p \lambda^t a^t,$$

and

$$\lambda^T = (\psi d^{-1})^p \lambda^t.$$

The quantity $x_1 = d^{-1} \psi$ has its $p$th power $x_1^p = \rho = \lambda^r \lambda^{-t}$ 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 $p$ over $K$. But $Y_0 = Y \times K$ so that then $X_{10} = X_1 \times K$ where $X$ is cyclic of degree $p$ over $F$ and in fact

$$\rho^T = \sigma^p \rho^t,$$

with $\gamma$ in $K$. Then $\lambda^T = \lambda^t \rho$ implies

$$\lambda^{T^2} = \lambda^{t^2} \rho^t \rho^T = \lambda^{t^2} \sigma^p \rho^{2t},$$

$$\lambda^{T^3} = \lambda^{t^3} \rho^{t^2} \rho^3 \gamma^p \lambda^t \rho^{3t^2},$$

so that finally

$$\lambda^{T^n} = \lambda = \gamma^p \lambda^{t^n} \rho^{n t^n - 1}.$$  

The quantity $\lambda^{t^n - 1} = \lambda^{-p}$ since $t^n \equiv 1 \pmod{p}$. Hence $\rho^t$ is the $p$th power of a quantity of $K$ where $\rho = n t^{n-1}$ is prime to $p$. This evidently implies that $\rho$ is the $p$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

$$\beta^T = \zeta^t (\psi \zeta \psi^{-1}) \beta^t,$$

since $\psi = d \sigma$, $\psi^S = \sigma d S$.

Since $ST = TS$ in $Z$ we obtain $(z^T)^p = \alpha^T = \psi^p \alpha^t = \psi^p z^t \rho$, $z^T = \zeta^t \zeta z^t$ with $0 \leq t < p$. Then $z^S = \beta z$ gives

$$z^{ST} = z^t \psi \zeta \beta^t z^t = z^S T = (\beta z)^T = (\zeta^t \psi \zeta^{-1}) \beta^t z^t,$$

so that $\zeta^t = 1$, $\nu = 0$.

Conversely let $Y$ be cyclic of degree $p^{n-1}$ over $F$, $Y_0 = Y \times K$, $\beta$ and $a$ be chosen in $Y_0$ and satisfying $N_{\gamma^t(\beta)} = \zeta$, (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 \( p^s \) over \( K \). It remains merely to show that then \( Z_0 \) is actually cyclic of degree \( p^s n \) over \( F \) if \( \nu = 0 \). We define the automorphism \( T \) of \( Z_0 \) by that in \( Y_0 \) and by

\[
z^T = \psi z^{t}, \quad \psi = \sigma d,
\]

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

University of Chicago,
Chicago, Ill.