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 $n=p$,† a prime, when the characteristic of F is not p, and for the case $n=p^e$‡ when the characteristic of F is p. Moreover it is well known that when F contains all the nth 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 nth 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 $n=p_1^{e_1}\cdots p_t^{e_t}$ 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 $n=p^e$, 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 pth root of unity ζ and later giving complete conditions for the case where F does not contain ζ.

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

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

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*. The results and proofs hold if F is any field of characteristic not p.

‡ Bulletin of the American Mathematical Society, vol. 40 (1934), pp. 625–631.

§ 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.

THEOREM 1. *A quantity a of Z has the property*

$$N_{Z/F}(a) = 1 \tag{2}$$

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

$$a = b^S/b. \tag{3}$$

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

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

$$y^i z = z^{S^i} y^i, \quad y^n = 1 \qquad (z \text{ in } Z), \tag{4}$$

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 $y_0 = AyA^{-1}$ with $A = \sum z_i y^i \neq 0$ and

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

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 pth root of unity ζ 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*

$$Z = Y(z), \quad z^p = a \text{ in } Y. \tag{5}$$

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

$$z^Q = \zeta^\mu z \qquad (0 \leqq \mu < p). \tag{6}$$

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,

$$\mu\mu_0 = 1 + \mu_1 p, \qquad (\mu_0, p) = 1, \tag{7}$$

for integers μ_0, μ_1. Define $S_0 = S^{\mu_0}$, $Q_0 = Q^{\mu_0}$ so that S_0 is a generating auto-

* For every cyclic field of degree p over Y containing ζ is a Kummer field $Y(z)$, $z^p = a$ in Y.

morphism of Z, Q_0 is a generator of the group $(I, Q, \cdots, Q^{p-1})$. Then $z^{Q_0} = \zeta^{\mu\mu_0} z = \zeta z$. Hence by properly choosing S we may assume

$$z^Q = \zeta z, \tag{8}$$

instead of (6).

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

$$z^{S^2} = \beta^S \beta^\nu z^{\nu^2} = \beta_2 z^{\nu^2}, \cdots, z^{S^m} = \beta_\nu z^{\nu^m} = z^Q = \zeta z$$

and hence $z^{\nu^m - 1} = \beta_\nu^{-1}\zeta$ is in the field Y. But then $\nu^m \equiv 1 \pmod{p}$ and, since $m = p^{e-1}$ so that $\nu^m \equiv \nu \pmod{p}$ we have $\nu \equiv 1 \pmod{p}$, $\nu = 1$.

Then

$$z^S = \beta z, \quad \beta \text{ in } Y. \tag{9}$$

Also

$$z^{S^2} = \beta^S \beta z, \cdots, z^{S^m} = z^Q = \beta^{S^{m-1}} \cdots \beta^S \beta z$$

and

$$N_{Y/K}(\beta) = \zeta. \tag{10}$$

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

$$\beta^p = \frac{\alpha^S}{\alpha}, \quad \alpha \text{ in } Y. \tag{11}$$

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

$$(\alpha a^{-1})^S = \alpha a^{-1}, \tag{12}$$

and hence $\alpha = \lambda a$ with λ 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 $a^S = a\beta^p$, $a^R = a(\beta\beta^S \cdots \beta^{S^{r-1}})^p = a$ so that $[N_{H/K}(\beta)]^p = 1$, $N_{H/K}(\beta) = \zeta^\rho$, $N_{Y/K}(\beta) = \zeta^{\rho p} = 1$, 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 β such that*

$$N_{Y/K}(\beta) = \zeta, \quad a^S a^{-1} = \beta^p. \tag{13}$$

* Cf. Hasse's *Bericht über Klassenkörper*, Jahresbericht der Deutschen Mathematiker Vereinigung, vol. 36 (1927), pp. 233–311; p. 262.

Moreover the generating automorphism S of Z is given by that in Y and

$$z^S = \beta z. \tag{14}$$

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 β such that $N_{Z/K}(\beta)=\zeta$. 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*

$$a^S a^{-1} = \beta^p, \tag{15}$$

and λ ranges over all quantities of K.

For if Z is cyclic of degree p^e over K then the existence of β is given by Theorem 2. Conversely let $N_{Z/K}(\beta)=\zeta$ for β 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 $a^S a^{-1} =(b^S b^{-1})^p=\beta^p$, $\beta=\zeta^\nu b^S b^{-1}$, $N_{Y/K}(\beta)=1$, a contradiction. Hence the field $Z=Y(z)$, $z^p=a_0$, has degree p over Y for every solution a_0 of $a^S a^{-1}=\beta^p$. 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 β_0 with $N_{Y/K}(\beta_0)=\zeta$. Then $N_{Y/K}(\beta_0\beta^{-1})=1$ and

$$\beta_0 = \beta d^S d^{-1}, \tag{16}$$

with d in Y by Theorem 1. Moreover $Z_0=K(z_1)$, $z_1^p=a_1$, where $a_1^S a_1^{-1}=\beta_0^p$. But if $a_{01}=\lambda a d^p$ with λ in K and $a^S a^{-1}=\beta^p$, then $a_{01}^S a_{01}^{-1}=\beta^p(d^S d^{-1})^p=\beta_0^p$. But then a_{01} is a constant multiple of a_1, and, by proper choice of λ, $a_1=a_{01}=\lambda a d^p$. The field $Z_0=K(z)$, $z=d^{-1}z_1$, $z^p=\lambda a$ is evidently equivalent to $K(z)$. Moreover $z^S=(d^S)^{-1}z_1^S=(d^S)^{-1}\beta d^S d^{-1}z=\beta z$ as desired.

We have determined the structure of cyclic fields of degree p^e over K when K contains a primitive pth root of unity ζ. We now study the more general case where ζ 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 pth roots of unity

$$\zeta^i \qquad (i = 1, 2, \cdots, p-1), \tag{17}$$

---

* Such cyclic overfields define new quantities β_0 but we prove below that in fact we may replace β_0 by β.

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 ζ 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

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

where n divides $p-1$ and is prime to p, t is an integer *belonging* to the exponent n (mod p),

$$t^n \equiv 1 \pmod{p}, \quad t^e \not\equiv 1 \pmod{p}, \quad e < n. \tag{18}$$

If we define

$$\zeta_k = \zeta^{t_k}, \quad t_k \equiv t^{k-1} \pmod{p}, \; 1 \leqq t_k < p, \tag{19}$$

$$\rho t \equiv 1 \pmod{p}, \quad \rho_k \equiv \rho^{k-1} \pmod{p}, \tag{20}$$

then I have proved*

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

$$\mu^T = \mu(\zeta^t) = \delta^p \mu^t \tag{21}$$

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

$$\mu = \prod_{k=1}^{n} \lambda(\zeta_k)^{\rho_k}. \tag{22}$$

We shall also require the known*

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

$$Z_0 = Z \times K, \tag{23}$$

where Z is cyclic of degree p over F, if and only if μ 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

$$S^iT^j \qquad (i = 0, 1, \cdots, p^{e-1}-1; \; j = 0, 1, \cdots, n-1).$$

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 β such that*

$$N_{Y_0/K}(\beta) = \zeta \tag{24}$$

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

$$\alpha^S\alpha^{-1} = \beta_0{}^p. \tag{25}$$

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

$$\alpha = \lambda a, \ \lambda \text{ in } K. \tag{26}$$

Then we have proved that z may always be chosen so that

$$z^S = \beta z, \tag{27}$$

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

THEOREM 5. *The quantities β, a may be chosen so that*

$$\beta^T = \delta^p\beta^t, \ a^T = d^p a^t, \tag{28}$$

with δ, d in Y.

For we have $a^S = a\beta^p$ and may define

$$\beta_0 = \prod_{k=1}^{n}\beta(\zeta_k)^{\rho k}, \quad a_0 = \prod_{k=1}^{n}a(\zeta_k)^{\rho k}, \tag{29}$$

so that by Lemma 1 we have $\beta_0{}^T = \delta_0{}^p\beta_0{}^t$, $a_0{}^T = d_0{}^p a_0{}^t$. Since $ST = TS$ in Y, we also have

$$\begin{aligned} a_0{}^S a_0^{-1} &= \prod_{k=1}^{n}\left[a^S(\zeta_k)^{\rho k}\right]\left[a(\zeta_k)^{\rho k}\right]^{-1} \\ &= \prod_{k=1}^{n}\beta(\zeta_k)^{\rho k\cdot p} = \beta_0{}^p. \end{aligned} \tag{30}$$

We also compute

$$N_{Y_0/K}(\beta_0) = \prod_{k=1}^{n}N_{Y_0/K}\beta(\zeta_k)^{\rho k} = \prod_{k=1}^{n}\zeta_k{}^{\rho k} = \zeta^\tau$$

where

$$\tau = \sum_{k=1}^{n} t_k\rho_k \equiv \sum_{k=1}^{n}(t\rho)^{k-1} \equiv n \pmod{p}. \tag{31}$$

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

$$N_{Y_0/K}(\beta_1) = \zeta^{\mu n} = \zeta, \tag{32}$$

and obviously

$$a_1^S a_1^{-1} = \beta_1^p. \tag{33}$$

Moreover

$$\beta_1^T = (\beta_0^T)^\mu = (\delta_0^p \beta_0^t)^\mu = (\delta_0^\mu)^p \beta_1^t = \delta^p \beta_1^t, \tag{34}$$

$$a_1^T = (a_0^T)^\mu = (d_0^p a_0^t)^\mu = (d_0^\mu)^p a_1^t = d^p a_1^t, \tag{35}$$

as desired. We have proved Theorem 5.

The automorphisms S and T of Y are commutative so that $N(\beta^T) = [N(\beta)]^T = \zeta^t = N(\beta^t)$ with $N(\beta)$ defined as $N_{Y_0/K}(\beta)$. Then by Theorem 1

$$\beta^T = f^S f^{-1} \beta^t \tag{36}$$

with f in Y_0. Also

$$\begin{aligned} (a^S a^{-1})^T &= (\beta^T)^p = a^{TS}(a^T)^{-1} = (d^S d^{-1})^p (a^S a^{-1})^t \\ &= (d^S d^{-1})^p \beta^{pt}, \end{aligned} \tag{37}$$

so that

$$\beta^T = \zeta^\nu d^S d^{-1} \beta^t \qquad (0 \leqq \nu < p). \tag{38}$$

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^{e-1} over K where Y_0 is also cyclic of degree np^{e-1} over F and assume that Y_0 contains a quantity β such that $N_{Y_0/K}(\beta) = \zeta$. We have then shown that there always exists a quantity a of Y such that $a^S a^{-1} = \beta^p$ and moreover that β and a may be so chosen that (38) and

$$a^T = d^p a^t \qquad (d \text{ in } Y) \tag{39}$$

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 $Z_0 = Y_0(z)$, $z^p = \alpha$ in Y such that*

$$\alpha = \lambda a, \ \lambda^T = \sigma^p \lambda^t \tag{40}$$

with σ in K, where then $Z_0 = Z \times K$, Z_0 is cyclic of degree np^e over F.

For we may write $Y_0 = Y(\zeta)$ so that if Z is cyclic of degree p^e over F with

Y as sub-field then $Z_0 = Y_0(z)$, $z^p = \alpha = \lambda a$ with λ in K. Moreover Z is cyclic of degree p over Y and by Lemma 2 we have

$$\alpha^T = \psi^p \alpha^t \tag{41}$$

with ψ in Y. Hence

$$\lambda^T a^T = \lambda^T d^p a^t = \psi^p \lambda^t a^t, \tag{42}$$

and

$$\lambda^T = (\psi d^{-1})^p \lambda^t. \tag{43}$$

The quantity $x_1 = d^{-1}\psi$ has its pth power $x_1{}^p = \rho = \lambda^T \lambda^{-t}$ in K. Hence either $\psi = d\sigma$ with σ 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

$$\rho^T = \sigma^p \rho^t, \tag{44}$$

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

$$\begin{aligned} \lambda^{T^2} &= \lambda^{t^2} \rho^t \rho^T = \lambda^{t^2} \sigma_1{}^p \rho^{2t}, \\ \lambda^{T^3} &= \lambda^{t^3} \rho^{t^2} (\sigma^T)^p (\sigma^{2t})^p \rho^{2t^2} = \gamma_2{}^p \lambda^{t^3} \rho^{3t^2}, \end{aligned} \tag{45}$$

so that finally

$$\lambda^{T^n} = \lambda = \overset{p}{\gamma}_{n-1} \lambda^{t^n} \rho^{nt^{n-1}}. \tag{46}$$

The quantity $\lambda^{t^n - 1} = \lambda_0{}^p$ since $t^n \equiv 1 \pmod{p}$. Hence ρ^ϕ is the pth power of a quantity of K where $\phi = nt^{n-1}$ is prime to p. This evidently implies that ρ is the pth 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

$$\beta^T = \zeta^\nu (\psi^S \psi^{-1}) \beta^t, \tag{47}$$

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

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

$$z^{TS} = \zeta^\epsilon \psi^S \beta^t z^t = z^{ST} = (\beta z)^T = \zeta^\nu \psi^S \psi^{-1} \beta^t \zeta^\epsilon \psi z^t, \tag{48}$$

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

Conversely let Y be cyclic of degree p^{e-1} over F, $Y_0 = Y \times K$, β and a be chosen in Y_0 and satisfying $N_{Y_0/K}(\beta) = \zeta$, (38), (39). Let λ range over all quantities of K such that (40) holds so that α 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 $p^e n$ 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 $\alpha^T = \psi^p \alpha^t$. Then we require only to show that $ST = TS$ so that the automorphism group of Z_0 over F is actually the cyclic group $(S^i T^j)$ $(i = 0, 1, \cdots, p^e - 1; j = 0, 1, \cdots, n-1)$. But this immediately follows from the computation in (48) with $\epsilon = 0$, and Theorem 6 is proved.

University of Chicago,
Chicago, Ill.