CYCLIC FIELDS OF DEGREE p^n OVER F OF CHARACTERISTIC p*

BY A. A. ALBERT

1. *Introduction.* The theory of cyclic fields is a most interesting chapter in the study of the algebraic extensions of an abstract field F. When F is a modular field of characteristic p, a prime, particular attention is focussed on the case of cyclic fields Z of degree p^n over F. Such fields of degree p, p^2 were determined by E. Artin and O. Schreier.†

In the present paper I shall give *a determination of all cyclic fields Z of degree p^n over F of characteristic p.*

2. *Normed Equations.* An equation

$$\lambda^p = \lambda + a, \qquad (a \text{ in } F), \tag{1}$$

is called a *normed equation.* If x is any root of (1), then so are $x+1, x+2, \cdots, x+p-1$. Using this fact, Artin-Schreier have proved the following lemmas.

LEMMA 1. *A normed equation is either cyclic or has all of its roots in F. Every cyclic field of degree p over F may be generated by a root of a normed equation.*

LEMMA 2. *Let $F(x)$ be cyclic of degree p over F,*

$$x^p = x + a, \qquad (a \textit{ in } F). \tag{2}$$

Then a quantity y of $F(x)$ which is not in F satisfies a normed equation if and only if

$$y = kx + b, \quad (k = 1, 2, \cdots, p; b \textit{ in } F). \tag{3}$$

LEMMA 3. *Let c in Z have degree $t \leqq p-2$ in x. Then there exists a quantity $g = g(x)$ in Z such that*

$$g(x+1) - g(x) = c. \tag{4}$$

Moreover, g is uniquely determined up to an additive constant in F.

---

* Presented to the Society, March 30, 1934.

† Hamburg Abhandlungen, vol. 5 (1926–7), pp. 225–231.

By applying Lemmas 1, 2, 3, Artin-Schreier proved the following fact.

LEMMA 4. *Every cyclic field Z of degree p over F is the sub-field of cyclic overfields Z_2 of degree p^2 over F. If $Z_1 = F(x_1)$, $x_1^p = x_1 + a_1$, a_1 in F, then all such fields Z_2 are obtained by*

$$Z_2 = F(x_2), \qquad x_2^p = x_2 + a_2, \qquad (a_2 \text{ in } Z_1), \tag{5}$$

where a_2 ranges over all solutions of (4) *in the case*

$$c = (x_1 + a_1)^{p-1} - x_1^{p-1}. \tag{6}$$

A generating automorphism S of Z_2 is given by

$$x_1^S = x_1 + 1, \qquad x_2^S = x_2 + x_1^{p-1}, \tag{7}$$

so that

$$x_2^{S^\nu} = x_2 + x_1^{p-1} + (x_1 + 1)^{p-1} + \cdots + (x_1 + \nu - 1)^{p-1}, \qquad (\nu = 1, 2, \cdots), \tag{8}$$

and in particular

$$x_2^{S^p} = x_2 + x_1^{p-1} + \cdots + (x_1 + p - 1)^{p-1} = x_2 - 1. \tag{9}$$

As an immediate corollary of (9) we have the following lemma.

LEMMA 5. *Let $Z = F(x)$, $x^p = x + a$, be cyclic of degree p over F. Then*

$$T_{Z|F}(x^{p-1}) \equiv x^{p-1} + (x+1)^{p-1} + \cdots + (x + p - 1)^{p-1} = -1. \tag{10}$$

3. *Generating Automorphisms.* Now let $Z = Z_n$ be any cyclic field of degree p^n over F and let S be a generating automorphism of the cyclic automorphism group of Z. It is well known that

$$Z_n > Z_{n-1} > \cdots > Z_1 > Z_0 = F, \tag{11}$$

where Z_i is uniquely determined, is cyclic of degree p^i over F, cyclic of degree p over Z_{i-1}. Moreover the automorphism S applied in Z_i may be taken as generating the automorphism group of Z_i with

$$Q_i = S^{p^i} \tag{12}$$

as identity automorphism for Z_i. In fact Z_i is defined as the set of all quantities of Z_n (and no others) unaltered by the automorphism Q_i.

We may consider Z_i as cyclic of degree p over Z_{i-1}. Then the group of Z_i over Z_{i-1} is evidently generated by Q_{i-1},

$$(Q_{i-1})^p = Q_i. \tag{13}$$

If b_i is any quantity of Z_i, then we write

$$T_{Z_i|F}(b_i) = b_i + b_i^S + \cdots + b_i^{S^{p^i-1}}. \tag{14}$$

We then evidently have

$$T_{Z_i|F}(b_i) = T_{Z_{i-1}|F}[T_{Z_i|Z_{i-1}}(b_i)], \tag{15}$$

where

$$T_{Z_i|Z_{i-1}}(b_i) = b_i + b_i^{Q_{i-1}} + \cdots + b_i^{Q_{i-1}^{p-1}} \tag{16}$$

is evidently in Z_{i-1}.

The field Z_i is cyclic of degree p over Z_{i-1} so that, by Lemma 1,

$$Z_i = Z_{i-1}(x_i), \qquad x_i^p = x_i + a_i, \qquad (a_i \text{ in } Z_{i-1}). \tag{17}$$

Moreover, x_i is not in Z_{i-1}, so that $F(x_i)$ is in Z_i but not in Z_{i-1}. The cyclic field Z_{i-1} contains every proper sub-field of Z_i and hence must contain $F(x_i)$, if $F(x_i)$ is a proper sub-field of Z_i. Thus, in fact, we have

$$Z_i = F(x_i). \tag{18}$$

We may now prove the following fact.

LEMMA 6. *Let* $b_{i+1} = (x_1x_2 \cdots x_i)^{p-1} = x_i^{p-1}b_i$. *Then* b_{i+1} *is in* Z_i *and*

$$T_{Z_i|F}(b_{i+1}) = (-1)^i. \tag{19}$$

For b_i is in Z_{i-1} and is unaltered by the automorphism Q_{i-1}. Hence $T_{Z_i|Z_{i-1}}(b_{i+1}) = b_iT_{Z_i|Z_{i-1}}(x_i^{p-1})$. Since Q_{i-1} is a generating automorphism of Z_i over Z_{i-1}, some power S_i of Q_{i-1} carries x_i into x_i+1. But then Lemma 5 implies $T_{Z_i|Z_{i-1}}(x_i^{p-1}) = -1$. Hence

$$T_{Z_i|F}(b_{i+1}) = T_{Z_{i-1}|F}[b_iT_{Z_i|Z_{i-1}}(x_i^{p-1})] = -T_{Z_{i-1}|F}(b_i). \tag{20}$$

By repeated application of this recursion formula, we evidently obtain (19).

Let S be a generating automorphism of Z_n. Then

$$(x_i^S)^p = x_i^S + a_i^S.$$

But evidently x_i^S is a primitive quantity of Z_i of degree p over Z_{i-1}, so that, by Lemma 2,

$$x_i^S = k_i x_i + b_i, \qquad (k_i = 1, 2, \cdots, p-1;\ b_i \text{ in } Z_{i-1}). \tag{21}$$

Then $x_i^{S^2} = k_i x_i^S + b_i^S = k_i^2 x_i + b_{i2}$, and finally $x_i^{S^\nu} = k_i^\nu x_i + b_{i\nu}$. Hence, if $m = p^n$, we have $x_i^{S^m} = k_i^m x_i + b_{im} = x_i$. But then $k_i^m = 1$. Since $k_i^p = k_i$, we evidently have $k_i^m = k_i = 1$. Thus

$$x_i^S = x_i + b_i, \qquad (i = 1, 2, \cdots, n). \tag{22}$$

Moreover,

$$(x_i^S)^p = x_i^p + b_i^p = x_i + a_i + b_i^p = x_i + b_i + a_i^S,$$

$$a_i^S - a_i = b_i^p - b_i. \tag{23}$$

The automorphism Q_{i-1} is a generating automorphism of Z_i over Z_{i-1} and replaces x_i by $x_i + h_i$, $(h_i = 1, 2, \cdots, p-1)$. But

$$x_i^{Q_{i-1}} = x_i + T_{Z_{i-1}|F}(b_i) = x_i + h_i,$$

so that

$$T_{Z_{i-1}|F}(b_i) = h_i \neq 0 \qquad (h_i = 1, 2, \cdots, p-1;\ i = 1, \cdots, n). \tag{24}$$

Conversely, let b_i satisfy (24), a_i be determined by (23), and let $x_1^p = x_1 + a_1$ be irreducible in F. Then $Z_n = F(x_n)$ is cyclic of degree p^n over F when Z_n is defined by (17), $Z_i = F(x_i)$, and S generates the automorphism group of Z_n. For assume this true for $Z_1, Z_2, \cdots, Z_{n-1}$, and define $Z_n = Z_{n-1}(x_n)$. The degree of Z_n over F is then p^n, for otherwise x_n is in Z_{n-1}, by Lemma 1, and hence $(x_n)^{Q_{n-1}} = x_n$, contrary to (24) and (22). Moreover, (22) defines an automorphism S of Z_n which has order at least p^{n-1}, since S generates the automorphism group of Z_{n-1}. But S actually has order p^n, since $Q_{n-1} = S^{p^{n-1}}$ alters x_n. Hence the group of automorphisms of Z_n has a cyclic sub-group of order p^n, the degree of Z_n, and Z_n is cyclic. It follows that $Z_n = F(x_n)$. We have proved the following result.

LEMMA 7. *Every cyclic field of degree p^n over F is generated by a quantity x_n such that*

$$(25) \quad x_i^p = x_i + a_i, \qquad a_i \text{ in } Z_{i-1} = F(x_{i-1}), \quad (i = 1, 2, \cdots, n),$$

and $x_1^p = x_1 + a_1$ is irreducible in F. If S is a generating automorphism of the group of Z_n, then

$$(26) \quad x_i^S = x_i + b_i, \qquad T_{Z_i|F}(b_{i+1}) = h_i, \qquad (h_i = 1, \cdots, p-1;\ i = 1, \cdots, n),$$

with

$$(27) \quad b_i^p - b_i = a_i^S - a_i, \qquad (i = 2, \cdots, n).$$

Conversely, every field Z_n defined by (25), (26), (27) *and $x_1^p = x_1 + a$ irreducible in F, is cyclic of degree p^n over F with generating automorphism S given by* (26).

Let c_i be an arbitrary quantity of Z_i and write

$$c_i = \sum_{j_r = 0, 1, \cdots, p-1} \lambda_{j_1 j_2 \cdots j_i} x_1^{j_1} x_2^{j_2} \cdots x_i^{j_i}$$

with coefficients λ in F. If $\lambda_{p-1, p-1, \cdots, p-1} = 0$, we call c_i a non-maximal quantity of Z_i. We may prove the following lemma.

LEMMA 8. *If $b_i \doteq (x_1 x_2 \cdots x_{i-1})^{p-1}$, the polynomials*

$$(28) \quad c_{i-1} = b_i^p - b_i = [(x_1 + a_1)(x_2 + a_2) \cdots (x_{i-1} + a_{i-1})]^{p-1} - (x_1 x_2 \cdots x_{i-1})^{p-1}, \qquad (i = 2, \cdots, n),$$

are non-maximal and (27) *have solutions a_i in Z_{i-1} which are unique up to an arbitrary additive constant in F. Then the a_i define cyclic fields Z_i, $(i = 2, \cdots, n)$, containing Z_1, where Z_i is cyclic of degree p^i over F. In fact, if c_i is any non-maximal quantity of Z_i, there exist solutions d_i in Z_i of*

$$(29) \quad c_i = d_i^S - d_i, \qquad d_i^S \equiv d_i(x_1 + b_1, \cdots, x_i + b_i), \qquad (i = 1, \cdots, n),$$

which are unique up to an additive constant in F.

For evidently $T_{Z_i|F}(b_{i+1}) = (-1)^i = h_i \neq 0$, so that $(26)_2$ are satisfied. It is thus sufficient to prove the existence of the a_i satisfying (27) and hence sufficient to prove the existence and uniqueness of solutions of (29) of which (27) is a special case.

We know that Lemma 8 is true for $n=1, 2$* by Lemmas 3, 4. Hence assume Lemma 8 true in its entirety for Z of degree $p, p^2, \cdots, p^{i-1}$. Then, by our assumption (29), there *exists* a Z_i of degree p^i over F, the equation (29) has a unique solution in Z_{i-1}, and we wish to prove (29) also has a unique solution in Z_i and hence the existence of Z_{i+1}.

Write

$$c_i = \lambda_t x_i^t + \cdots + \lambda_0, \qquad (\lambda_j \text{ in } Z_{i-1}).$$

If λ_t is a non-maximal quantity of Z_{i-1}, then, by our above assumption, $\lambda_t = \mu_t^S - \mu_t$, ($\mu_t$ in Z_{i-1}). But then

$$(\mu_t x_i^t)^S - \mu_t x_i^t = \mu_t^S (x_i + b_i)^t - \mu_t x_i^t = \lambda_t x_i^t + \cdots,$$

so that $c_i - [(\mu_t x_i^t)^S - (\mu_t x_i^t)]$ has degree at most $t-1$.

If λ_t is maximal, then $t < p-1$ and c_i has leading term

$$\lambda(x_1 x_2 \cdots x_{i-1})^{p-1} x_i^t = \lambda b_i x_i^t, \qquad \lambda \neq 0 \text{ in } F.$$

But then $t+1 \neq 0$,

$$\begin{aligned}\lambda(t+1)^{-1}[(x_i^{t+1})^S - x_i^{t+1}] &= \lambda(t+1)^{-1}[(x_i + b_i)^{t+1} - x_i^{t+1}] \\ &= \lambda b_i x_i^t + \cdots,\end{aligned}$$

so that $c_i - \{[\lambda(t+1)^{-1} x_i^{t+1}]^S - [\lambda(t+1)^{-1} x_i^{t+1}]\}$ has degree at most t in x_i and non-maximal leading coefficient. A repeated application of the above process may evidently be made to obtain a quantity δ_i in Z_i such that $c_i - (\delta_i^S - \delta_i) = \gamma_{i0}$, ($\gamma_{i0}$ in Z_{i-1}). But γ_{i0} may be taken non-maximal as above with $t=0$, $t+1=1$, and hence

$$\gamma_{i0} = \gamma_i^S - \gamma_i, \qquad c_i = d_i^S - d_i, \qquad d_i = \delta_i + \gamma_i.$$

Now let $c_i = d_i^S - d_i = d_{i0}^S - d_{i0}$. Then $(d_{i0} - d_i)^S = d_{i0}^S - d_i^S = d_{i0} - d_i$. The only quantities of Z_i unaltered by S are quantities of F. Hence $d_{i0} - d_i = \lambda$ in F. We have proved Lemma 8. We shall now prove our principal theorem.

THEOREM. *Every cyclic field Z_1 of degree p over F of characteristic p is the sub-field of cyclic overfields of degree p^n. Write*

$$(30) \qquad Z_1 = F(x_1), \qquad x_1^p = x_1 + a_1, \qquad (a_1 \textit{ in } F).$$

---

* Note that (28) is true for $n=2$ by Lemma 3, is vacuous for $n=1$. Hence Z_2 is defined by Lemma 4. This is the *first* step in our induction, the case $i=2$.

Then all such fields Z_n are given by

(31) $Z_i = F(x_i),\ \ x_i^p = x_i + a_i,\ \ a_i$ *in* $F(x_{i-1}),\ (i = 2, \cdots, n),$

where a_i is the unique (up to an arbitrary additive constant in F) solution of

$$\begin{aligned} &a_i(x_1 + b_1, \cdots, x_{i-1} + b_{i-1}) - a_i \\ (32)\qquad &\quad = [(x_1 + a_1) \cdots (x_{i-1} + a_{i-1})]^{p-1} - (x_1x_2 \cdots x_{i-1})^{p-1}, \\ &b_i \equiv (x_1x_2 \cdots x_{i-1})^{p-1}, \qquad\qquad (i = 2, \cdots, n). \end{aligned}$$

Conversely, all fields defined by (30), (31), (32) *with $x_1^p = x_1 + a_1$ irreducible in F are cyclic of degree p^n with generating automorphism S given by*

(33) $x_0 = 1,\ \ x_i^S = x_i + (x_0x_1x_2 \cdots x_{i-1})^{p-1},\quad (i = 1, \cdots, n).$

For we have proved that the fields defined above are cyclic, in Lemma 8. Assume now, conversely, that Z_n is cyclic of degree p^n over F and that we have proved the above result for its subfields $Z_1, \cdots, Z_{n-1}$. Let $x_n^S = x_n + d_n$ by Lemma 7 and write $d_n = \beta b_n + g_n$, where $b_n = (x_1x_2 \cdots x_{i-1})^{p-1}$, β is in F, and $-g_n$ is a non-maximal polynomial in Z_{n-1}. By Lemma 8, we have also

$$- g_n = h_n^S - h_n, \qquad (h_n \text{ in } Z_{n-1}).$$

We then let $y_n = x_n + h_n$, so that

$$y_n^S = x_n^S + h_n^S = x_n + \beta b_n + g_n + h_n - g_n = y_n + \beta b_n.$$

Moreover, $Z_n = F(x_n) = F(y_n)$, since it is evident that y_n generates $Z_{n-1}(x_n)$ over Z_{n-1} and hence also $F(x_n)$, by Lemma 7 (in which we proved $Z_{n-1}(x_n) = F(x_n)$).

But now we have shown that we may take $d_n = \beta b_n$ without loss of generality. Since

$$T_{Z_{n-1}|F}(d_n) = \beta T_{Z_{n-1}|F}(b_n) = (-1)^{n-1}\beta = k_n, \qquad (k_n = 1, \cdots, p - 1),$$

the quantity β is a non-zero integer. There exists an integer γ such that $\gamma\beta = 1$ and, if we write $z_n = \gamma x_n$, we have $z_n^S = \gamma x_n^S = \gamma(x_n + \beta b_n) = z_n + b_n$. Evidently $F(x_n) = F(z_n)$ while z_n satisfies (33). By Lemma 7, (27), we have also (32) for $i = n$; and we have proved the theorem.

THE INSTITUTE FOR ADVANCED STUDY