CHAPTER IV
SYSTEMS OF ALGEBRAIC EQUATIONS

1. The preceding chapters contain, of course, a theory of systems of algebraic equations. One has only to suppose oneself working with a system of d.p. which are of order zero in each indeterminate. It is, however, desirable to make a separate examination of algebraic equations.

For instance, the theory of algebraic equations can be developed from the algorithmic standpoint, so that every entity whose existence is established is constructed with a finite number of operations. The results of the algebraic theory will permit us, in Chapter V, to give an algorithmic treatment of various questions connected with finite systems of d.p.

Again, we shall obtain an approximation theorem for systems of algebraic equations (§39) which will be found useful in the study of algebraic differential manifolds in the analytic case.

Our account of algebraic equations differs in certain respects from the classical treatments. On the one hand, it is convenient for us to use the methods of the preceding chapters; on the other, it is necessary for us to develop formal procedures which can be applied later to differential equations.

POLYNOMIALS AND THEIR IDEALS

2. In the present chapter, we use an algebraic field \( \mathfrak{F} \) of characteristic zero (I, §1), without requiring that an operation of differentiation exist in \( \mathfrak{F} \). We study polynomials in algebraic indeterminates \( y_1, \ldots, y_n \), with coefficients in \( \mathfrak{F} \). The totality of such polynomials is represented by \( \mathfrak{F}[y_1, \ldots, y_n] \). Polynomials will be represented by capital italics and systems of polynomials by large Greek letters.

We carry over definitions from Chapter I as follows. Let \( \mathfrak{F} \) be regarded momentarily as a differential field in which all derivatives are zero, and the \( y \) as differential indeterminates. We then define, as in Chapter I, the terms class, separant, initial, chain, characteristic set and remainder.

3. Let \( \Sigma \) be a system of polynomials in \( \mathfrak{F}[y_1, \ldots, y_n] \). We shall call \( \Sigma \) a polynomial ideal (p.i.) if, for every finite subset \( A_1, \ldots, A_r \) of \( \Sigma \) and for all \( C_1, \ldots, C_r \) in \( \mathfrak{F}[y_1, \ldots, y_n] \), the polynomial \( C_1 A_1 + \cdots + C_r A_r \) is contained in \( \Sigma \).

If \( \Sigma_1 \) and \( \Sigma_2 \) are p.i., and if \( \Sigma_2 \) contains \( \Sigma_1 \), \( \Sigma_2 \) is called a divisor of \( \Sigma_1 \).

Let \( \Lambda \) be any system of polynomials. Let (\( \Lambda \)_0) be the totality of linear combinations of polynomials in \( \Lambda \) with polynomials for coefficients. Then (\( \Lambda \)_0) is a p.i. We call (\( \Lambda \)_0 the p.i. generated by \( \Lambda \).

Let \( \Sigma \) be a p.i. Suppose that, whenever a polynomial \( \Lambda \) is such that some
positive integral power of $A$ is in $\Sigma$, $A$ itself is in $\Sigma$. We shall then call $\Sigma$ a 
perfect p.i. Let $\Lambda$ be any system of polynomials. Let $\{ \Lambda \}_0$ be the totality of 
those polynomials $A$ for which a positive integer $p$, depending on $A$, exists such 
that $A^p$ is in $(\Lambda)_0$. It is easy to see that $\{ \Lambda \}_0$ is a perfect p.i. We call $\{ \Lambda \}_0$ 
the perfect p.i. determined by $\Lambda$.

Let $\Sigma$ be a p.i. We shall say that $\Sigma$ is prime if, for every pair of polynomials 
$A$ and $B$ with $AB$ in $\Sigma$, at least one of $A$ and $B$ is in $\Sigma$. Every prime p.i. is 
perfect.

For p.i., the following theorem holds.

**Theorem:** Every perfect p.i. is the intersection of a finite number of prime p.i.

In §4, we shall show how this theorem can be proved using only material developed in the present book. Let us, however, first found a proof on Hilbert's classic basis theorem for systems of polynomials.

According to Hilbert's theorem, given an infinite system $\Sigma$ of polynomials, 
$\Sigma$ has a finite subset $\Phi$ such that $(\Phi)_0$ contains $\Sigma$. Now let $\Sigma$ be a perfect 
ideal for which our theorem is not true. Then $\Sigma$ is not prime. Let $AB$ be in 
$\Sigma$ while neither $A$ nor $B$ is. We see easily that

$$\{ \Sigma + AB \}_0 = \{ \Sigma + A \}_0 \cap \{ \Sigma + B \}_0$$

and the proof is completed as in I, §16.

4. We may also operate as follows. Let us consider $\mathfrak{A}$ as a differential field 
in which all derivatives are zero and let the $y$ be regarded as differential indeterminates. 
Let $\Sigma$ be an infinite system of polynomials, and $\Phi$ a basis for $\Sigma$ as in 
I, §12. We consider any polynomial $A$ in $\Sigma$. Let $A^p$ be linear in polynomials 
of $\Phi$, and their derivatives, with d.p. for coefficients. The $j$th derivative of a 
 polynomial of positive class is isobaric and of weight $j$. If, in the linear expression 
for $A^p$, we cast out all terms of positive weight, we have for $A^p$ an expression linear in polynomials in $\Phi$, with polynomials for coefficients. We secure in this way a basis theorem for systems of polynomials which, to be sure, is 
weaker than Hilbert's theorem, but which is adequate for the purposes of §3.

5. If $\Sigma$ is a perfect p.i., a prime divisor of $\Sigma$ which is not a divisor of any 
other prime divisor of $\Sigma$ will be called an **essential prime divisor** of $\Sigma$. Every 
perfect p.i. has a finite number of essential prime divisors, and is the intersection of 
those divisors.

**Algebraic manifolds**

6. Let $\Sigma$ be a system of polynomials $\mathfrak{A}[y_1, \cdots, y_n]$. Let $\mathfrak{A}'$ be any extension 
of $\mathfrak{A}$, that is, any algebraic field which contains $\mathfrak{A}$. Let there exist in $\mathfrak{A}'$ a 
set of elements $\eta_1, \cdots, \eta_n$ which cause every polynomial in $\Sigma$ to vanish when 
$\eta_i$ is substituted for $y_i$. The set $\eta_1, \cdots, \eta_n$ will be called a zero of $\Sigma$. If $\Sigma$ 
has zeros, the totality of its zeros, for all extensions $\mathfrak{A}'$ of $\mathfrak{A}$, will be called the 
manifold of $\Sigma$. The manifold of a system of polynomials will be called an 
algebraic manifold.
Let an algebraic manifold \( \mathcal{M} \) be the union of two algebraic manifolds, each a proper part of \( \mathcal{M} \). We shall then call \( \mathcal{M} \) reducible. If \( \mathcal{M} \) is not reducible, it is called irreducible.

Let \( \mathcal{M} \) be an algebraic manifold. The totality \( \Sigma \) of polynomials which vanish over\(^1\) \( \mathcal{M} \) is a perfect p.i., the perfect p.i. associated with \( \mathcal{M} \). \( \Sigma \) is prime if and only if \( \mathcal{M} \) is irreducible. If \( \mathcal{M} \) is irreducible, we call \( \Sigma \) the prime p.i. associated with \( \mathcal{M} \).

We see readily that every algebraic manifold is the union of a finite number of irreducible algebraic manifolds.

Let \( \mathcal{M} \) be the union of irreducible algebraic manifolds \( \mathcal{M}_1, \cdots, \mathcal{M}_p \). We suppose that no \( \mathcal{M}_i \) contains any \( \mathcal{M}_j \) with \( j \neq i \). We then call each \( \mathcal{M}_i \) a component of \( \mathcal{M} \), or of any system of polynomials whose manifold is \( \mathcal{M} \). If \( \Sigma \) is the perfect p.i. associated with \( \mathcal{M} \) and \( \Sigma_i \) the prime p.i. associated with \( \mathcal{M}_i \), \( \Sigma \) is the intersection of the \( \Sigma_i \) and the \( \Sigma_i \) are the essential prime divisors of \( \Sigma \).

**Generic zeros of prime polynomial ideals**

7. Let \( \Sigma \) be a prime p.i. distinct from the unit p.i., \((1)_0\). Let \( A \) be any polynomial, not necessarily contained in \( \Sigma \). We form a class \( \alpha \) of polynomials, putting into \( \alpha \) every polynomial \( G \) such that \( G - A \) is in \( \Sigma \). We call \( \alpha \) a remainder class modulo \( \Sigma \). If \( \alpha \) and \( \beta \) are remainder classes, \( \alpha + \beta \) is defined as the remainder class which contains every \( A + B \) with \( A \) in \( \alpha \) and \( B \) in \( \beta \).

We define \( \alpha \beta \) similarly. We call \( \Sigma \), which is a remainder class, the zero class. Because \( \Sigma \) is prime, the product of two nonzero remainder classes is distinct from the zero class.

We now consider pairs \((\alpha, \beta)\) of remainder classes in which \( \beta \) is not the zero class. Equivalence is defined as in II, §6, and the totality of pairs of classes separates into sets of equivalent pairs. For the sets of equivalent pairs, addition and multiplication are defined, as in II, §6. Subtraction and division are then performable and unique, with the usual reservation in regard to division. The sets of equivalent pairs constitute an algebraic field \( \mathfrak{F}_1 \) which, after an adjustment, becomes an extension of \( \mathfrak{F} \).

Let \( \omega \) be the remainder class which contains \( 1 \). Let \( \alpha_i, i = 1, \cdots, n \), be the class which contains \( y_i \). Let \( \eta_i \) be the set in \( \mathfrak{F}_1 \) which contains \((\alpha_i, \omega)\). We find that \( \eta_1, \cdots, \eta_n \) is a zero of \( \Sigma \). Every polynomial in \( \mathfrak{F}[y_1, \cdots, y_n] \) which vanishes when each \( y_i \) is replaced by \( \eta_i \) is contained in \( \Sigma \).

Let \( \Sigma \) be as above. Every zero \( \eta_1, \cdots, \eta_n \) of \( \Sigma \) which is such that every polynomial in \( \mathfrak{F}[y_1, \cdots, y_n] \) which is annulled by the \( \eta \) is in \( \Sigma \) is called a generic zero of \( \Sigma \).

**Resolvents**

8. A prime p.i. distinct from \((1)_0\) and from \((0)_0\) will be said to be nontrivial. Let \( \Sigma \) be a nontrivial prime p.i. in \( \mathfrak{F}[y_1, \cdots, y_n] \). The \( y \) can be divided

---

\(^1\) Language as in Chapter II.
into two sets, \( u_1, \cdots, u_q \) and \( y_1, \cdots, y_p, \) \( p + q = n, \) such that no nonzero polynomial of \( \Sigma \) is free of the \( y_i \), while, for \( j = 1, \cdots, p \), there is a nonzero polynomial in \( \Sigma \) in \( y_j \) and the \( u \) alone. We call the \( u \) a parametric set. Let the indeterminates be listed in the order

\[
u_1, \cdots, u_q; \quad y_1, \cdots, y_p,\]

and let

\[
(1) \quad A_1, \cdots, A_p
\]

be a characteristic set of \( \Sigma \).

A regular zero of (1) is defined as a zero of (1) which does not annul the initial of any \( A \). Every regular zero of (1) is a zero of \( \Sigma \).²

9. Let \( K \) be any polynomial not contained in \( \Sigma \). We shall prove that

\[
(A_1, \cdots, A_p, K)_0,
\]

which we represent by \( \Lambda \), contains a nonzero polynomial in the \( u \) alone.

We start with the observation that the polynomials in \( \Sigma \) which involve no \( y_i \) with \( i \geq j \), where \( 1 \leq j < p \), constitute a prime p.i.; we designate this p.i. by \( \Sigma_j \).

\( \Lambda \) contains the remainder of \( K \) with respect to (1). Of all nonzero polynomials in \( \Lambda \) which are reduced with respect to (1), let \( B \) be one which is of a lowest rank. We say that \( B \) is free of the \( y \).

Suppose that this is not so, and let \( B \) be of class \( q + r \) with \( r > 0 \). The initial \( C \) of \( B \) is not in \( \Sigma \). There is a relation

\[
C^m A_r = DB + E
\]

where \( E \), if not zero, is of lower degree than \( B \) in \( y_r \). We say that \( E \) is in \( \Sigma \). Let this be false. If \( r > 1 \), the remainder of \( E \) with respect to \( A_1, \cdots, A_{r-1} \) is a nonzero polynomial contained in \( \Lambda \), which is reduced with respect to (1) and of lower rank than \( B \). If \( r = 1 \), a similar statement can be made of \( E \) itself. Thus \( E \) is in \( \Sigma \), so that \( DB \) is in \( \Sigma \). Then \( D \) is in \( \Sigma \). \( D \) is of positive degree in \( y_r \). As the initial of \( DB \) is that of \( C^m A_r \), the initial \( I \) of \( D \) is not in \( \Sigma \).

If we had \( r = 1 \), \( D \) would be a nonzero polynomial in \( \Sigma \) which is reduced with respect to (1); this is because \( D \) is of lower degree in \( y_r \) than \( A_r \). Thus \( r > 1 \). The remainder of \( D \) with respect to \( A_1, \cdots, A_{r-1} \) is zero. Thus \( JD \), with \( J \) some product of powers of the initials of \( A_1, \cdots, A_{r-1} \), is linear in \( A_1, \cdots, A_{r-1} \). If we write \( JD \) as a polynomial in \( y_r \), its coefficients will be in \( \Sigma_{r-1} \). Thus \( JI \) is in \( \Sigma_{r-1} \). This is false because neither \( J \) nor \( I \) is in \( \Sigma_{r-1} \).

Thus \( B \) is free of the \( y \) and our statement is proved.

²We are applying here, to the theory of characteristic sets, an idea due to van der Waerden. See Mathematische Annalen, vol. 96 (1927), p. 189; also Moderne Algebra, first edition, vol. 2, p. 56.
10. We are going to show the existence of a nonzero polynomial $G$, free of the $y$, and the existence of a polynomial

$$Q = M_1 y_1 + \cdots + M_p y_p$$

where the $M$ are polynomials free of the $y$, such that, for two distinct zeros of $\Sigma$ with the same $u$ (if $u$ exist) lying in the same extension of $\mathfrak{F}$ and having

$G \neq 0$, $Q$ assumes two distinct values.

We consider the system $\Sigma'$ obtained from $\Sigma$ by replacing each $y_i$ by a new indeterminate $z_i$. Using $p$ more indeterminates $\lambda_1, \cdots, \lambda_p$ we consider the system $\Lambda$ composed of $\Sigma, \Sigma'$ and

$$\lambda_1 (y_1 - z_1) + \cdots + \lambda_p (y_p - z_p).$$

As $\Lambda$ contains $\Sigma$, $\Lambda$ has, for $j = 1, \cdots, p$, a nonzero polynomial $B_j$ in $y_j$ and the $u$, $u$ alone. Similarly, let $C_j, j = 1, \cdots, p$, be a nonzero polynomial of $\Lambda$ in $z_j$ and the $u$, $u$ alone.

Let $D$ be the product of the initials\(^3\) of the $B$ and $C$.

Consider a zero of $\Lambda$ for which $(y_1 - z_1) D \neq 0$. For it, we have

$$\lambda_1 = \frac{-\lambda_1 (y_2 - z_2) + \cdots + \lambda_p (y_p - z_p)}{y_1 - z_1}. \quad (2)$$

Let $m$ be the maximum of the degrees of the $B_j$ in the $y_j$ and of the degrees of the $C_j$ in the $z_j$. Let $\alpha$ be any positive integer. We write, for $s = 0, \cdots, \alpha$ and for the above zero,

$$\lambda_1^s = \frac{E_s}{(y_1 - z_1)^{\alpha}}$$

where $E_s$ is a polynomial. Now it is plain that, using the relations $B_j = 0$, $C_j = 0$, we can depress the degree of $E_s$ in each $y$ and in each $z$ to be less than $m$.

The new expression for each $\lambda_1^s$ will be of the form

$$\lambda_1^s = \frac{F_s}{(y_1 - z_1)^{\alpha} D_s},$$

where $D_s$ is a product of powers of the initials of the $B$ and $C$. Let $L$ be the least common multiple of the $D_s$. We write

$$\lambda_1^s = \frac{H_s}{(y_1 - z_1)^{\alpha} L}, \quad (3)$$

$s = 0, \cdots, \alpha$, each $H_s$ being a polynomial of degree less than $m$ in each $y$ and $z$.

Now the number of power products of the $y$ and $z$, of degree less than $m$ in each $y$ and $z$, is $m^{2p}$. Consequently, if we take $\alpha \geq m^{2p}$, we find a nonzero polynomial in $\lambda_1$, of degree not greater than $\alpha$, whose coefficients are polynomials in $\lambda_2, \cdots, \lambda_p$ and the $u$, which vanishes for every zero of $\Lambda$ which does not annihilate $(y_1 - z_1) D$. The product $K_1$ of this polynomial by $D$ vanishes for every zero of $\Lambda$ which does not annihilate $y_1 - z_1$.

---

\(^3\) The initial of $C_j$ is the coefficient of the highest power of $z_j$. 
Similarly, for \( i = 2, \ldots, p \), we find a \( K_i \) which vanishes for every zero of \( \Lambda \) which does not annul \( y_i - z_i \).

Let \( M_i, i = 1, \ldots, p \), be polynomials in the \( u \), which, when substituted for the \( \lambda_i \) in \( K_1 \cdots K_p \), reduce that polynomial to a nonzero polynomial \( G \) in the \( u \). Any such set of \( M \) will furnish a \( Q \) as above. The \( M \) may be taken as integers.

11. Introducing a new indeterminate \( w \), we let \( \Omega \) represent the p.i. \((\Sigma, w - Q)_0\) in \( \mathfrak{F}[u_1, \ldots, u_q; w; y_1, \ldots, y_p] \). It is easy to prove, as in II, §26, that \( \Omega \) is prime. The polynomials of \( \Omega \) which are free of \( w \) are precisely the polynomials of \( \Sigma \).

As above, we prove that \( \Omega \) has a nonzero polynomial free of the \( y \).

We arrange the indeterminates in \( \Omega \) in the order

\[
u_1, \ldots, u_q; w; y_1, \ldots, y_p
\]

and take a characteristic set for \( \Omega \),

\[
u A, A_1, \cdots, A_p.
\]

Here \( w, y_1, \ldots, y_p \) are introduced in succession.

We take \( A \) irreducible in \( \mathfrak{F} \).

We are going to prove that each \( A_i \) is linear in \( y_i \), so that the equation \( A_i = 0 \) expresses \( y_i \) rationally in terms of \( w \) and the \( u \).

12. Let us suppose that our claim is false and let \( A_k \) be the \( A_i \) of highest subscript for which it breaks down. Then every \( A_i \) with \( i > k \) which may exist is linear in \( y_k \).

Let \( U \) be the remainder with respect to (5) of

\[I_k + I_{k+1} \cdots I_p.
\]

Of course, \( U \) is free of \( y_k+1, \ldots, y_p \). By §9,

\[
(A, A_1, \cdots, A_k, U)_0
\]

in \( \mathfrak{F}[u_1, \cdots, u_q; w; y_1, \cdots, y_k] \) contains a nonzero polynomial \( B \) in the \( u \) alone. If \( k = p \), there is no \( B \).

Let

\[
u u_i = \tau_i, \quad i = 1, \cdots, q; \quad w = \xi; \quad y_i = \eta_i, \quad i = 1, \cdots, p.
\]

be a generic zero of \( \Omega \), lying in an extension \( \mathfrak{F}_1 \) of \( \mathfrak{F} \).

We replace the \( u, w \) and \( y_1, \ldots, y_k-1 \) in \( A_k \) by the corresponding quantities in (6). Then \( A_k \) goes over into polynomial \( H_k \) in \( y_k \) over \( \mathfrak{F}_1 \), whose degree in \( y_k \) equals that of \( A_k \). Let \( K \) be a factor of \( H_k \), irreducible in \( \mathfrak{F}_1 \). Then \( (K)_0 \), in \( \mathfrak{F}_1[y_k] \), is a prime p.i. Let \( \xi \) be a generic zero of \( (K)_0 \).

The quantities

\footnote{That is, with coefficients in \( \mathfrak{F}_1 \).}

\footnote{The irreducibility of \( K \) implies that every zero of \( K \) is a generic zero of \( (K)_0 \).}
(7)  \( \tau_1, \ldots, \tau_q; \xi; \eta_1, \ldots, \eta_k - 1; \xi_h \)
do not annul \( I_{k+1} \cdots I_p \). If they did, they would annul \( U \) and therefore \( B \).
Now \( B \), which is a nonzero polynomial in the \( u \), cannot vanish for the \( \tau \). We
obtain thus a zero of \( \Omega \),

(8)  \( \tau_1, \ldots, \tau_q; \xi; \eta_1, \ldots, \eta_k - 1; \xi_h, \ldots, \xi_p \)
lying in an extension of \( \mathfrak{S}_1 \). The zeros (6) and (8) do not annul \( G \) and they
have the same \( v \). They are thus identical. This means that \( \xi_h = \eta_h \). The
proof that \( A_k \) is linear in \( y_k \) is now completed as in II, §30.

We shall call the equation \( A = 0 \) a resolvent of \( \Sigma \).

It is now easy to prove that \( q \), in §8, is independent of the manner in which
the \( u \) are selected. We call \( q \) the dimension of \( \Sigma \). Following II, §36, we can
show that if a prime p.i. \( \Sigma' \) is a proper divisor of \( \Sigma \), the dimension of \( \Sigma' \) is
less than that of \( \Sigma \).

**Hilbert's theorem of zeros**

13. We prove the following theorem.

**Theorem:** If \( \Sigma \) is a perfect p.i. distinct from the unit p.i., \( \Sigma \) has zeros and
every polynomial which holds\(^7\) \( \Sigma \) is contained in \( \Sigma \).

Let \( \Sigma_1, \ldots, \Sigma_p \) be the essential prime divisors of \( \Sigma \). No \( \Sigma_i \) is the unit p.i.
If \( G \) holds \( \Sigma \), \( G \) vanishes for the generic zeros of each \( \Sigma_i \) and is thus in each \( \Sigma_i \).
Then \( G \) is in \( \Sigma \).

We present now

**Hilbert's theorem of zeros:** Let, in \( \mathfrak{S}[y_1, \ldots, y_n] \),

(9)  \( F_1, \ldots, F_s \)
be any finite system of polynomials, and \( G \) any polynomial which holds that system.
Then some power of \( G \) is linear in the \( F \), with polynomials for coefficients.

It is a matter of showing that \( G \) is contained in the perfect ideal determined by
the \( F \). If that ideal is the unit p.i., \( G \) is certainly contained in it. Otherwise,
we have merely to apply the theorem which precedes.

14. The analytic case, in which \( \mathfrak{S} \) consists of functions meromorphic in an
open region \( A \), needs more detailed treatment. We use analytic zeros of (9),
the definition being as in Chapter II. Hilbert's theorem then becomes:

If \( F \) vanishes for every analytic zero of \( F_1, \ldots, F_s \), some power of \( G \) is linear in
the \( F \), with polynomials for coefficients.

Let \( \Sigma \) be the perfect ideal determined by the \( F \) and suppose that \( G \) is not con-
tained in \( \Sigma \). Then \( \Sigma \) is not the unit ideal. Let \( \Sigma' \) be an essential prime
divisor of \( \Sigma \) in which \( G \) is not contained. It will be seen that we may sup-

---

\(^6\) The dimension is zero when there are no \( u \).

\(^7\) As in Chapter II.
pose $\Sigma'$ to be distinct from the zero ideal. Let the indeterminates be written $u_1, \ldots, u_q; y_1, \ldots, y_p$ with the $u$ parametric for $\Sigma'$.

We form a resolvent for $\Sigma'$. Let (5) be a characteristic set for the system $\Omega$, associated with $\Sigma'$ as in §11. We shall prove the legitimacy of assuming that the initials of the $A_i$ in (5) are free of $w$. Let

$$A_1 = MY_1 + N.$$ 

As $A$ and $M$ are relatively prime polynomials, there is a relation

$$PA + QM = L$$

where $P$ and $Q$ are polynomials in $w$ and the $u_i$ and $L$ is a nonzero polynomial in the $u$ alone.\(^7\) Then $\Omega$ contains $LY_1 + QN$. If $I$ is the initial of $A$, there is a relation

$$I^sQN = CA + R$$

with $R$ reduced with respect to $A$. Then $I^sLY_1 + R$ is in $\Omega$ and may be used in place of $A_1$ in (5). We treat the other $A_i$ similarly.

Let $H$ be the remainder of $G$ with respect to (5). Some linear combination of $H$ and $A$ is a nonzero polynomial $K$ in the $u$ alone. Every zero of $\Sigma'$ which annuls $G$ annuls $K$.

To complete our proof, we have to show that $\Sigma'$ has a zero which does not annul $K$. We fix $u_1, \ldots, u_q$ as analytic functions which annul neither $K$ nor any initial in (5). We can then find an analytic $w$ which annuls $A$ with the selected $u$. The equations $A_i = 0$ then determine $y_1, \ldots, y_p$.

**Characteristic sets of prime polynomial ideals**

15. We consider, in $\mathfrak{F}[u_1, \ldots, u_q; y_1, \ldots, y_p]$, a chain

$$(10) \quad A_1, A_2, \ldots, A_p,$$ 

$A_i$ being of class $g + i$. We are going to find a condition for (10) to be a characteristic set of a prime p.i.

Since a nontrivial prime p.i. consists of those polynomials which have zero remainders with respect to any characteristic set, (10) cannot be a characteristic set for more than one prime p.i.

16. If $\mathfrak{F}$ is an extension of $\mathfrak{F}$ and if $\eta_1, \ldots, \eta_r$ is a finite subset of elements of $\mathfrak{F}$, the totality of rational combinations of $\eta_1, \ldots, \eta_r$ with coefficients in $\mathfrak{F}$ will be denoted by $\mathfrak{F}(\eta_1, \ldots, \eta_r)$ and will be called the field obtained by the adjunction of the $\eta$ to $\mathfrak{F}$. Thus, we represent by\(^9\) $\mathfrak{F}(u_1, \ldots, u_q)$ the totality of the rational combinations of the $u$ with coefficients in $\mathfrak{F}$.

17. Considering (10), we suppose first that $p = 1$. We shall show that for $A_1$ to be a characteristic set of a prime p.i. in $u_1, \ldots, u_q; y_1$, it is necessary and

---

\(^7\) Chapter II, §42.

\(^9\) Abbreviated below as $\mathfrak{F}(u)$.
sufficient that $A_1$, considered as a polynomial in $y_1$, be irreducible in $\mathcal{F}(u)$. We first prove sufficiency. Let $A_1$ be irreducible, as indicated. Then $A_1 = BC$ with $B$ free of $y_1$ and $C$ irreducible in $\mathcal{F}$ as a polynomial in $y_1$ and the $u$. Now $(C)_0$ is a prime p.i. for which $C$ is a characteristic set. Then $A_1$ is also a characteristic set for $(C)_0$. For the necessity proof, let $A_1$ be a characteristic set for a prime p.i. $\Sigma$. Let $A_1 = BC$, where $B$ and $C$ are polynomials of positive degree in $\mathcal{F}(u)[y_1]$. Clearing fractions, we secure a relation $GA_1 = HK$ among polynomials in $\mathcal{F}[u; y_1]$ with $H$ and $K$ of lower degree than $A_1$ in $y_1$. As one of $H$ and $K$ is in $\Sigma$, we have a contradiction.

18. We understand now that $a < 1$. We furnish a necessary and sufficient
Writing each coefficient in $C$ and $D$ in the form $\varphi/\psi$ as indicated above, we clear fractions. We obtain a relation

\[(13) \quad \delta B = EF\]

where $\delta$ is a polynomial in the quantities in (11) and $E$ and $F$ are polynomials in $y_p$, of positive degree, whose coefficients are polynomials in the quantities in (11). We write (13)

\[(14) \quad \delta B - EF = 0.\]

In the first member of (14) we replace each quantity in (11) by the indeterminate which corresponds to it. We obtain a polynomial

\[(15) \quad G A_p - H K.\]

If this polynomial is arranged according to powers of $y_p$, its coefficients will vanish for (11) and thus are in $\Sigma_{p-1}$. Hence $HK$ is in $\Sigma_p$. Suppose that $H$ is in $\Sigma_p$. The degree of $H$ in $y_p$ is less than that of $A_p$. As $G$ and the initial of $A_p$ are not in $\Sigma_p$, the initial of $H$ is not in $\Sigma_p$. Let $L$ be the remainder of $H$ with respect to $A_1, \ldots, A_{p-1}$. Then $L$ is reduced with respect to (10). Furthermore, $L$ is not zero (§9). As $\Sigma_p$ cannot contain a nonzero polynomial reduced with respect to (10), the necessity of (b) is proved.

20. Suppose now that (a) and (b) are satisfied. When (11) is substituted into $A_p, A_p$ becomes a polynomial $B$, irreducible in $\mathfrak{F}_{p-1}$. Let $\eta_p$ be a zero of $B$. Let $\Sigma_p$ be the totality of those polynomials in $\mathfrak{F}[u; y]$ which vanish for

\[\tau_1, \ldots, \tau_q; \eta_1, \ldots, \eta_p.\]

Then $\Sigma_p$ is a prime p.i. We shall prove that (10) is a characteristic set of $\Sigma_p$. Let the contrary be assumed. Then $\Sigma_p$ contains a nonzero $G$ which is reduced with respect to (10). Now $G$ must be of class $p$, else, vanishing for (11), it would be in $\Sigma_{p-1}$ in spite of being reduced with respect to (10). For (11), $G$ becomes a polynomial $H$ in $\mathfrak{F}_{p-1}[y_p]$ which is annulled by $\eta_p$ and is of lower degree than $B$. The sufficiency of conditions (a) and (b) is thus established.

**Construction of resolvents**

21. Before we can give a method for the effective construction of a resolvent for a prime p.i. for which a characteristic set is given, we must have a solution of the following problem.

Let $\mathfrak{F}$ represent $\mathfrak{F}(u_1, \ldots, u_q)$. Let $A$ be a polynomial in $\mathfrak{F}[u_1, \ldots, u_q; w]$ irreducible as a polynomial in $w$ over $\mathfrak{F}$. Let $A_1$ be a polynomial in $\mathfrak{F}[u_1, \ldots, u_q; w; y]$, of positive degree in $y$. Let $w = \eta_1$ be a zero of $A$ considered as a polynomial in $\mathfrak{F}_0[w]$; of course, $\eta_1$ lies in an extension of $\mathfrak{F}$. Let $\mathfrak{F}_1$ represent $\mathfrak{F}_0(\eta_1)$. We assume that the initial of $A_1$ does not vanish when $w$ is replaced by $\eta_1$. We represent by $B$ the polynomial in $\mathfrak{F}_1[y]$ obtained by re-
placing \( w \) by \( \eta_i \) in \( A_1 \). It is required to find the irreducible factors of \( B \) over \( \mathfrak{F}_1 \).\(^{10}\)

It will be seen that the only knowledge of \( \eta_i \) which we need is that it annuls \( A \).

Let \( m \) be the degree of \( A \) in \( w \). We shall show the existence of an extension \( \mathfrak{F}' \) of \( \mathfrak{F}_1 \) in which \( A \) has \( m \) distinct zeros \( \eta_1, \ldots, \eta_m \). Let \( C \) be the polynomial in \( \mathfrak{F}_1[w] \), of degree \( m - 1 \), obtained by dividing \( A \) by \( w - \eta_i \). Then \( C \) has a zero \( \eta_2 \), lying in an extension \( \mathfrak{F}_2 \) of \( \mathfrak{F}_1 \). The irreducibility of \( A \) in \( \mathfrak{F}_1 \) implies that \( \eta_1 \) and \( \eta_2 \) are distinct. Let \( D = C/(w - \eta_2) \). We secure a zero of \( D \). Continuing, we obtain a set \( \eta_1, \ldots, \eta_m \).

Let \( z \) be an indeterminate and let \( E_i \) be the polynomial in \( \mathfrak{F}_1[y, z] \) which results on replacing \( y \) in \( B \) by \( y - z\eta_i \). Let \( E_i, i = 2, \ldots, m \), result from \( E_i \) on replacing \( \eta_i \) by \( \eta_i \). Let \( G = E_1 E_2 \cdots E_m \).

Then \( G \) is a polynomial in \( \mathfrak{F}_0[y, z] \), the coefficients in \( G \) being capable of determination by the theory of symmetric functions. Let \( G \) be resolved into factors irreducible in \( \mathfrak{F}_0 \). This is possible, provided we are able to factor a polynomial in one indeterminate over \( \mathfrak{F} \).\(^{11}\) Let

\[
G = H_1 \cdots H_r
\]

with each \( H \) a polynomial in \( \mathfrak{F}_0[y, z] \), irreducible in \( \mathfrak{F}_0 \).

We wish to show that, for \( j = 1, \ldots, r \), \( E_i \) and \( H_j \) have a common factor, of positive degree, over \( \mathfrak{F}_1 \). Let this be false for some definite \( j \). Then there exists a relation

\[
U_i E_i + V_i H_j = W_1
\]

with \( U_i, V_i, W_1 \) polynomials over \( \mathfrak{F}_1 \) and with \( W_1 \) free of \( z \) and distinct from zero. In (17), we replace \( \eta_i \) by \( \eta_i \), where \( 1 < i \leq m \). We secure a relation\(^{12}\)

\[
U_i E_i + V_i H_j = W_i.
\]

This shows that \( H_j \) has no common factor over \( \mathfrak{F}' \), of positive degree in \( z \), with any \( E_i \). Similarly \( H_j \) has no common factor over \( \mathfrak{F}' \), of positive degree in \( y \), with any \( E_i \). On the other hand, the factors of \( H_j \) irreducible over \( \mathfrak{F}' \) must be factors of the \( E \). This proves our statement.

Let \( K, i = 1, \ldots, r \), be the highest common factor of \( E_i \) and \( H_i \), the field being \( \mathfrak{F}_1 \). We determine \( K \) by the Euclid algorithm, bearing in mind that a polynomial \( \xi \) in \( \eta_1, u_1, \ldots, u_q \) is zero when and only when the polynomial in \( w \) and the \( u \), obtained by replacing \( \eta_i \) by \( w \) in \( \xi \), is divisible by \( A \).

We shall prove that the \( K \) become, for \( z = 0 \), the irreducible factors of \( B \) in \( \mathfrak{F}_1 \).\(^{13}\) Let

\[
B = M_1 \cdots M_k
\]


\(^{12}\) Every \( \eta \) is a generic zero of \( (A)_0 \), the field being \( \mathfrak{F}_0 \).

\(^{13}\) We do not establish a one-to-one correspondence between the \( K \) and the irreducible factors. The knowledge of the essentially distinct irreducible factors of \( B \) permits the representation of \( B \) as a product of powers of irreducible factors.
be a resolution of \( B \) into factors irreducible in \( \mathfrak{F}_1 \). Then
\[
E_1 = N_1 N_2 \cdots N_k
\]
where each \( N_i \) results from \( M_i \) on replacing \( y \) by \( y - z\eta_i \). It is easy to see that each \( N_i \) as a polynomial in \( y \) and \( z \) is irreducible in \( \mathfrak{F}_1 \).

Manifestly each \( N_i \) is a common factor of \( E_1 \) and some \( H_j \) in (16). If we can prove that, in this case, \( N_i \) is the highest common factor of \( E_1 \) and \( H_j \), we will have our result.

Let \( N_1^{(m_j)} \), for \( j = 2, \cdots, m \), be the polynomial obtained from \( N_i \) on replacing \( \eta_1 \) by \( \eta_j \). Let
\[
P_i = N_i N_i^{(m)} \cdots N_i^{(m)}.
\]
Then \( P_i \) is a polynomial in \( \mathfrak{F}_0 [y, z] \) and
\[
G = P_1 P_2 \cdots P_k.
\]
Each \( H_i \) in (16) is a factor of some \( P_j \).

Suppose that \( N_1 \) is a factor of \( H_1 \) and that \( H_1 \) is a factor of \( P_1 \). If we can prove that \( N_1 \) is the highest common factor of \( E_1 \) and \( P_1 \), we will have our result.

Suppose, for instance, that \( P_1 \) is divisible by \( N_1 N_2 \). Then by (18),
\[
N_1^{(m)} \cdots N_1^{(m)} = R(y, z)N_2,
\]
where \( R \) is a polynomial in \( \mathfrak{F}_1 [y, z] \).

The set of terms of highest degree in the first member of (19) is of the form
\[
b(y - z\eta)^s \cdots (y - z\eta)^t
\]
with \( b \) a rational combination of the \( u \) and \( \eta \). The terms of highest degree in the second member give an expression of the type
\[
S(y, z) (y - z\eta)^t.
\]
Now (20) and (21) cannot be equal, since no \( y - z\eta_i \) with \( i > 1 \) is divisible by \( y - z\eta_1 \). This completes the proof.

22. We consider a nontrivial prime p.i. \( \Sigma \) in \( \mathfrak{F} [u_1, \cdots, u_q; y_1, \cdots, y_p] \) for which
\[
A_1, \cdots, A_p
\]
is a characteristic set, \( A_i \) introducing \( y_i \). In §§24, 25 we show how, when the \( A \) are given, a resolvent can be constructed for \( \Sigma \).

23. Let \( \lambda_1, \cdots, \lambda_p \) be new indeterminates. If \( \Sigma \) is regarded as a system of polynomials in the \( u, \lambda, y, \Sigma \) generates a p.i. \( (\Sigma)_0 \) which can be seen, as in I, §27, to be prime. Furthermore \( (\Sigma)_0 \) contains no nonzero polynomial in the \( u \) and \( \lambda \).

We see as in §10 that there exists a nonzero \( G \) in the \( u \) and \( \lambda \) such that, for
two distinct zeros of \((\Sigma)_0\) with the same \(u\) and \(\lambda\), lying in the same extension of \(\mathfrak{F}\) and not annulling \(G\),

\[ Q = \lambda y_1 + \cdots + \lambda y_p \]

assumes two distinct values.\(^{14}\)

By §§11, 12, a resolvent exists for \((\Sigma)_0\) for which \(w = Q\). Let \(\Omega = (\Sigma, \ w - Q)_0\) in \(\mathfrak{F}[u; \lambda; w; y]\). We consider a characteristic set for \(\Omega\)

\[(23) \quad R, R_1, \cdots, R_p\]

in which \(w, y_1, \cdots, y_p\) are introduced in succession and in which \(R\) is irreducible in \(\mathfrak{F}\). Then \(R = 0\) is a resolvent for \((\Sigma)_0\) and each \(R_i\) is linear in \(y_i\).

24. We shall show how a characteristic set (23) can actually be constructed.

Using the polynomials in (22), and also \(w - Q\), we can, by the method of elimination of \(\Pi\), §34, determine, by means of a finite number of rational operations, a nonzero \(U\) in \(w\), the \(u\), and \(\lambda\), which vanishes for every generic zero of \(\Omega\). It is a matter of considering relations \(w^j = Q^j\) and depressing the degrees of \(Q^j\) in the \(y\) by using the relations \(A_i = 0\). Then \(U\) is in \(\Omega\). Now let

\[ U = U_1 \cdots U_r \]

with each \(U_i\) irreducible in \(\mathfrak{F}\). Some \(U_i\) is in \(\Omega\). The selection of such a \(U_i\) can be made as follows. Consider any \(U_i\) and let \(V\) be the polynomial obtained from it by replacing \(w\) by \(Q\). For \(U_i\) to be in \(\Omega\), it is necessary and sufficient that \(V\) be in \((\Sigma)_0\). Let \(V\) be arranged as a polynomial in the \(\lambda\). For \(V\) to be in \((\Sigma)_0\), it is necessary and sufficient that every coefficient in the polynomial be in \(\Sigma\). A coefficient will be in \(\Sigma\) if and only if its remainder with respect to (22) is zero.

A polynomial in \(w\), the \(u\), and \(\lambda\) which is in \(\Omega\) is divisible by \(R\). Thus an irreducible factor of \(U\) which is in \(\Omega\) must be the product of \(R\) in (23) by an element of \(\mathfrak{F}\).

We have then a method for constructing a resolvent for \((\Sigma)_0\). It remains to show how a complete set (23) can be determined.

Let \(W\) be the polynomial which results from \(R\) on replacing \(w\) by \(w + y_1\) and \(\lambda_1\) by \(\lambda_1 + 1\). Then \(W\) holds \(\Omega\) and is thus in \(\Omega\). The degree of \(W\) in \(y_1\) is that of \(R\) in \(w\) and the coefficient of the highest power of \(y_1\) in \(W\) is free of \(w\).

Let \(\mathfrak{F}_0\) represent \(\mathfrak{F}\) \((u_1, \cdots, u_q; \lambda_1, \cdots, \lambda_p)\) and let \(B\) be considered as a polynomial in \(\mathfrak{F}_0[w]\). Let \(w = \eta\) be any zero of \(R\). We represent by \(B\) the polynomial in \(y_1\) over \(\mathfrak{F}_0(\eta)\) obtained by replacing \(w\) in \(W\) by \(\eta\). Let

\[(24) \quad B = B_1 \cdots B_m\]

be a decomposition of \(B\) into factors irreducible in \(\mathfrak{F}_0(\eta)\), obtained as in §21. The coefficients in the \(B_i\) are rational in \(\eta\), the \(u\) and \(\lambda\). Let \(a\) be the product of the denominators of these coefficients. We write

\(^{14}\) At present we have no way of determining \(G\).
\[ \alpha B = C_1 \cdots C_m. \]

The \( C \) are irreducible in \( \mathbb{F}_0(\eta) \) and their coefficients are polynomials in \( \eta, u, \) and \( \lambda \). Let \( D \) be the polynomial which results from \( \alpha \) on replacing \( \eta \) by \( w \). Let \( E_i \) result similarly from \( C_i \). Let

\[ F = DW - E_1 \cdots E_m. \]

Then \( F \) vanishes identically in \( y_1 \) if \( w \) is replaced by \( \eta \). Hence, if \( F \) is arranged as a polynomial in \( y_1 \), its coefficients are divisible by \( R \). Thus \( F \) is in \( \Omega \). Then one of the \( E_i \) is in \( \Omega \). Suppose that \( E_1 \) is found (by test) to be in \( \Omega \). We say that \( E_1 \) is linear in \( y_1 \). If \( I_1 \) is the initial of \( R_1 \) in (23), we have

\[ I_1^* E_1 = HR_1 + K \]

where \( K \) is free of \( y_1 \). Thus, if \( E_1 \) were not linear, it would follow that \( C_1 \) is reducible in \( \mathbb{F}_0(\eta) \).\(^{15}\)

It is only necessary, then, to take the remainder of \( E_1 \) with respect to \( R \) to have a polynomial which will serve as \( R_i \) in (23).

The \( R_i \) with \( i > 1 \) are determined in the same way.

It can be arranged, as in §14, so that, for each \( i \), the initial \( I_i \) of \( R_i \) is free of \( w \). We suppose this to be done. If two zeros of \( \Omega \) have the same \( u, \lambda, w \), they will have the same \( y \) if no \( I_i \) vanishes for their \( u, \lambda \). We may thus take \( G \) as \( I_1 I_2 \cdots I_p \).

25. It remains to construct a resolvent for \( \Sigma \). Let \( I \) be the initial of \( R \) in (23). Let \( a_1, \cdots, a_p \) be integers for which \( IG \), with \( G \) as above, becomes a nonzero polynomial in the \( u \) when each \( \lambda_i \) is replaced by \( a_i \).

We shall show how (23) yields a resolvent for \( \Sigma \) with

\[ w = a_1 y_1 + \cdots + a_p y_p. \]

Let \( \Omega' = (\Sigma, w - a_1 y_1 - \cdots - a_p y_p) \) in \( \mathbb{F}[u; w; y] \). Then \( \Omega' \) is a prime p.i. For \( \lambda_i = a_i, i = 1, \cdots, p \), (23) becomes a system of polynomials

\[ R'_1, R'_1, \cdots, R'_p \]

each of which holds \( \Omega' \) and is therefore in \( \Omega' \). As \( R \) and \( R' \) have the same degree in \( w \), (27) is a chain.

We are going to show that \( R' \) is not the product of two polynomials over \( \mathbb{F} \) which are of positive degree in \( w \). Thus, if we free \( R' \) of its factors in the \( u \), we secure a polynomial \( R_0 \) which is irreducible in \( \mathbb{F} \). The equation \( R_0 = 0 \) will be a resolvent for \( \Sigma \).\(^{16}\) Also (27) will be a characteristic set of \( \Omega' \).

If \( R' \) is a product of two polynomials of positive degree in \( w \), \( \Omega' \) will have a characteristic set

\[ T, T_1, \cdots, T_p, \]

\(^{15}\) We note that \( I_1 \) cannot vanish for \( w = \eta \).

\(^{16}\) For \( w \) as in (26), two distinct zeros of \( \Sigma \) with the same \( u \) and \( w \) annul \( G' \), obtained from \( G \) by putting \( \lambda_i = a_i \).
with \( T \) of lower degree in \( w \) than \( R' \). We assume that the initials of the \( T_i \) are free of \( w \). If \( D \) is the product of those initials, we have, for a generic zero of \( \Sigma \),

\[
y_i = \frac{E_{w} + E_{w^2} + \cdots + E_{w^{q-1}} w^{-1}}{D},
\]

where \( g \) is the degree of \( T \) in \( w \) and the \( E \) are polynomials in the \( u \). We understand \( w \) to be given by (26).

Let us now consider the prime p.i.

\[
\Omega' = (\Sigma, v - \lambda_1 y_1 - \cdots - \lambda_p y_p)_0
\]

in \( \mathcal{F} [u; \lambda; v; y] \). We show that \( \Omega' \) contains a nonzero polynomial \( K \), free of the \( y \), which is of degree no more than \( g \) in \( v \). We consider the relations

\[
v^j = (\lambda_1 y_1 + \cdots + \lambda_p y_p)^j, \quad j = 0, \cdots, g.
\]

We replace the \( y \) by their expressions in (28) and depress the degrees in \( w \) of the second members to less than \( g \), using the relation \( T = 0 \). By a linear dependence argument, we secure the polynomial \( K \). This furnishes the contradiction that \( R \) in (23) is of degree at most \( g \) in \( w \).

Thus \( R_0 = 0 \) is a resolvent for \( \Sigma \).

**Components of finite systems**

26. Let \( \Phi \) be a finite system of polynomials in \( \mathcal{F} [y_1, \cdots, y_n] \), not all zero. We are going to show how to determine characteristic sets of a finite number of prime p.i. whose manifolds make up the manifold\(^{17} \) of \( \Phi \). Later, we shall obtain finite systems whose manifolds are the components of \( \Phi \).

A system \( \Sigma \) of polynomials will be said to be *equivalent* to the set of systems \( \Sigma_1, \cdots, \Sigma_s \) if the manifold of \( \Sigma \) is the union\(^{18} \) of the manifolds of the \( \Sigma_i \).

Let

\[
A_1, \cdots, A_p
\]

be a characteristic set of \( \Phi \), obtained as in I, §5. If \( A_1 \) is of class zero, \( \Phi \) has no zeros. We assume now that \( A_1 \) is of positive class. For every polynomial in \( \Phi \), let the remainder with respect to (29) be determined. If these remainders are adjoined to \( \Phi \), we get a system \( \Phi' \) equivalent to \( \Phi \). By I, §5, if some of the remainders are not zero, \( \Phi' \) will have a characteristic set lower than (29). We see, by I, §4, that after a finite number of repetitions of the above operation, we arrive at a finite system \( \Lambda \), equivalent to \( \Phi \), with a characteristic set\(^{19} \) (29) for which either \( A_1 \) is of class zero or for which, otherwise, the remainder of every polynomial in \( \Lambda \) is zero.

27. Let us suppose that we are in the latter case. We make a temporary relettering of the \( y \). If, in the characteristic set (29) of \( \Lambda \), \( A_i \) is of class \( j_i \), we

---

17 If \( \Phi \) has no zeros, we obtain (1)\(_a\).
18 In this, we understand that if \( \Sigma \) has no zeros, no \( \Sigma_i \) has zeros.
19 Naturally, (29) is not the same for \( \Lambda \) as for \( \Phi \).
replace the symbol $y_i$ by $y_i$. The $q = n - p$ indeterminates not among the $y_i$ we call, in any order, $u_1, \ldots, u_q$. We list the indeterminates in the order $u_1, \ldots, u_q; y_1, \ldots, y_p$.

With this change of notation, we proceed to determine, using §§17–19, whether (29) is a characteristic set for a prime p.i.

28. If $A_1$ is reducible as a polynomial in $y_1$ over $\mathcal{F}(u_1, \ldots, u_q)$ and if $A_1 = MN$ with $M$ and $N$ polynomials in $u_1, \ldots, u_q; y_1$, of positive degree in $y_1$, then $\Lambda$ is equivalent to $\Lambda + M, \Lambda + N$. Each of the latter systems, after we revert to the old notation, will have a characteristic set lower than (29).

Suppose now that $A_1$ is irreducible in $\mathcal{F}(u_1, \ldots, u_q)$. We use indeterminates $\tau_1, \ldots, \tau_q$ and the field $\mathcal{F}(\tau_1, \ldots, \tau_q)$ which we represent by $\mathcal{F}_0$. For $u_i = \tau_i, i = 1, \ldots, q$, $A_1$ becomes a polynomial $B_1$ in $\mathcal{F}_0[y_1]$. Let $y_1 = \eta_1$ be a zero of $B_1$. Let $B_2$ be the polynomial in $\mathcal{F}_0(\eta_1) [y_2]$ which $A_2$ becomes for $y_1 = \eta_1, u_i = \tau_i$. Suppose that $B_2$ is reducible in $\mathcal{F}_0(\eta_1)$. We have, in analogy to (14),

\begin{equation}
\delta B_2 - EF = 0,
\end{equation}

where $\delta$ is a polynomial in $\eta_1$ and the $\tau$. $E$ and $F$ are polynomials in $y_2$, of positive degree, whose coefficients are polynomials in $\eta_1$ and the $\tau$. When we replace $\eta_1$ and the $\tau$ by $y_1$ and the $u$, the first member of (30) becomes a polynomial

\[ GA_2 - HK \]

which, when arranged according to powers of $y_2$, has coefficients which are divisible by $A_1$.

Thus $GA_2 - HK$ is in $(A_1)_0$ so that $HK$ is in $^{20} (A_1, A_2)_0$. Let $M$ and $N$ be, respectively, the remainders of $H$ and $K$ with respect to $A_1$. Because the initial of $GA_2$ is not divisible by $A_1$, the initials of $H$ and $K$ are not so divisible. It follows that $M$ and $N$ are not zero (§19). As $MN$ is in $(A_1, A_2)_0$, we see that $\Lambda$ is equivalent to $\Lambda + M, \Lambda + N$, whose characteristic sets, in the old notation, are lower than (29).

29. Suppose that $B_2$ is irreducible in $\mathcal{F}_0(\eta_1)$. By §18, $A_1, A_2$ is a characteristic set of a prime p.i. $\Sigma_2$ in $y_1, y_2$ and the $u$. Let $\eta_2$ be any zero of $B_2$. We shall show that

\begin{equation}
\tau_1, \ldots, \tau_q; \eta_1, \eta_2
\end{equation}

is a generic zero of $\Sigma_2$. Let $G$ be a polynomial in $\Sigma_2$. The remainder of $G$ with respect to $A_1, A_2$ is zero. As the initials of $A_1$ and $A_2$ do not vanish for (31), $G$ is annulled by (31). Conversely, let $G$ be a polynomial in $y_1, y_2$ and the $u$ which is annulled by (31). The remainder $R$ of $G$ with respect to $A_1, A_2$ also vanishes for (31). Suppose that $R$ is not zero. If $R$ is arranged as a polynomial in $y_2$, its coefficients will not be divisible by $A_1$ and thus will not vanish for $\eta_1$ and the $\tau$. Substituting these quantities for $y_1$ and the $u$ in $R$, we secure

\[ ^{20} \text{in} \mathcal{F}[u; y_1, y_2]. \]
a polynomial in $y_2$ of lower degree than $B_2$ which vanishes for $y_2 = \eta_2$. This contradiction shows that $R = 0$. Then $G$ is in $\Sigma_2$. Thus (31) is a generic zero of $\Sigma_2$.

We substitute the quantities (31) into $A_3$, securing a polynomial $B_3$ in $y_3$ over $F_0(\eta_1, \eta_2)$. We need a method for finding the irreducible factors of $B_3$ in $F_0(\eta_1, \eta_2)$. Let a resolvent be constructed for $\Sigma_2$ as in §§24, 25, with

$$w - a_1y_1 - a_2y_2 = 0,$$

$a_1$ and $a_2$ being integers. Now

$$\tau_1, \ldots, \tau_6; \quad a_1\eta_1 + a_2\eta_2; \quad \eta_1, \eta_2$$

is a generic zero of the prime p.i. for which (27), with $p = 2$, is a characteristic set. Thus $a_1\eta_1 + a_2\eta_2$ annuls $R'$, but not the initials of $R'_1$ and $R'_2$. Hence $\eta_1$ and $\eta_2$ are rational in $a_1\eta_1 + a_2\eta_2$ and the $\tau$. Thus, to factor $B_3$ in $F_0(\eta_1, \eta_2)$ it suffices to factor $B_3$ in $F_0(a_1\eta_1 + a_2\eta_2)$. This we know how to do.

Suppose that $B_3$ is reducible in $F_0(\eta_1, \eta_2)$. We have, as in (30), a relation

$$\delta B_3 - EF = 0$$

where $\delta$ is a polynomial in $\eta_1, \eta_2$ and the $\tau$. If, in the first member, we replace $\eta_1, \eta_2$ and the $\tau$ by $y_1, y_2$ and the $u$, we secure a polynomial $GA_3 - HK$ which, when arranged in powers of $y_3$, has its coefficients in $\Sigma_2$. Let $L$ be any of these coefficients. Let $I_i$ represent the initial of $A_i$ in (29). As the remainder of $L$ with respect to $A_1, A_2$ is zero, some $I_1^3I_2^3L$ is in $(A_1, A_2)_0$. Then some

$$I_1^3I_2^3(GA_3 - HK)$$

is linear in $A_1$ and $A_2$, so that $I_1^3I_2^3HK$ is in $(A_1, A_2, A_3)_0$. Let $M$ and $N$ be, respectively, the remainders of $I_1^3I_2^3H$ and $K$ with respect to $A_1, A_2$. Then $M$ and $N$ are not zero and $MN$ is in $(A_1, A_2, A_3)_0$. Thus $\Lambda$ is equivalent to $\Lambda + M, \Lambda + N$, each of which, in the old notation, has characteristic sets lower than (29).

30. If $B$ is irreducible in $F_0(\eta_1, \eta_2)$ then $A_1, A_2, A_3$ is a characteristic set of a prime p.i. $\Sigma_3$, and we continue as above.

All in all, we have a method for testing (29) to determine whether it is a characteristic set for a prime p.i. and for replacing $\Lambda$ by a pair of systems with characteristic sets lower than (29) when the test is negative.\(^{21}\)

In developing our method, we have recast the conditions of §§17, 18 and have secured the following theorem.

**Theorem:** A chain of polynomials of positive class fails to be a characteristic set of a prime p.i. if and only if there exist two nonzero polynomials, reduced with respect to the chain, whose product is in the p.i. generated by the chain.

\(^{21}\) If, when the indeterminates are $u_1, \ldots, u_\ell; y_1, \ldots, y_r$, (29) is a characteristic set for a prime p.i. $\Omega$, then, when we revert to the old notation, (29) will be a characteristic set for the prime p.i. into which $\Omega$ goes.
31. Using now the old notation for the indeterminates, let us suppose that (29) has been found to be a characteristic set for a prime p.i. $\Sigma$. Then $\Lambda$ is equivalent to

$$\Sigma, \Lambda + I_1, \cdots, \Lambda + I_p.$$  

Each $\Lambda + I_j$ has characteristic sets which are lower than (29).

What precedes shows that the system $\Phi$ of §26 can be resolved into an equivalent set of prime p.i., as far as the determination of characteristic sets for the prime p.i. goes, by a finite number of rational operations and factorizations, if the same can be done for all finite systems whose characteristic sets are lower than those of $\Phi$. The final remark of I, §4, gives a quick abstract proof that the resolution is possible for $\Phi$. What is more, the processes used above, of reduction, factorization and isolation of prime p.i., give an algorithm for the reduction.

32. It remains to solve the following problem: Given a characteristic set

$$A_1, \cdots, A_p$$

of a nontrivial prime p.i. $\Sigma$ in $\mathfrak{F}[y_1, \cdots, y_n]$, each $A_i$ being of class $q + i$ ($p + q = n$), it is required to find a finite system of polynomials equivalent to $\Sigma$.

33. Using indeterminates $t_i$, we make the transformation

$$z_i = t_i y_1 + \cdots + t_i y_n, \quad i = 1, \cdots, n.$$  

For a zero of $\Sigma$ in an extension $\mathfrak{F}_1$ of $\mathfrak{F}$, (34) gives quantities $z$ in the field obtained by adjoining the $t$ to $\mathfrak{F}_1$. Given any $q + 1$ of the $z$

$$z_{i_1}, \cdots, z_{i_q + 1},$$

we find, by the method of elimination of II, §34, a nonzero polynomial in them and the $t$ which vanishes when the $z$ are replaced by their expressions in (34), with $y_1, \cdots, y_n$ a generic zero of $\Sigma$.

Let $B$ be such a polynomial in $z_1, \cdots, z_{q+1}$ and the $t$. Let $m$ be the degree of $B$ considered as a polynomial in the $z$. We shall show how to obtain a relation $C = 0$ among $z_1, \cdots, z_{q+1}$ and the $t$, where $C$ is of degree $m$ as a polynomial in the $z$ and, in addition, is of degree $m$ in each $z$ separately.

We make in $B$ the transformation

$$z_i = a_{i_1} z'_1 + \cdots + a_{i_q + 1} z'_{q + 1}, \quad i = 1, \cdots, q + 1,$$

where the $a$ and $z'$ are indeterminates. Then $B$ becomes a polynomial $B'$ in the $z'$ whose coefficients are polynomials in the $t$ and the $a$. The degree of $B'$

---

$^22$ Note that $\Lambda$ is contained in $\Sigma$ because the remainder of every polynomial in $\Lambda$ with respect to (29) is zero. Every zero of (29) which annihilates no initial is a zero of $\Sigma$.

$^23$ $\Phi$ of §26 leads to several $\Sigma$. For each $\Sigma$, we reletter the indeterminates appropriately. After finite systems are found, equivalent to the various $\Sigma$, we revert to the original lettering.

$^24$ Satisfied when the $y$ in (34) are a generic zero of $\Sigma$. 

---
in each $z'_i$ will be effectively $m$.\footnote{Perron, Algebra, vol. 1, p. 288.} Furthermore, we can specialize the $a$ as integers in such a way that the determinant $|a_{i,j}|$ is not zero and that the coefficient of the $m$th power of each $z'_i$ in $B'$ becomes a nonzero polynomial in the $t$. Let this be done and let $B''$ be the polynomial in the $z'$ and $t$ into which $B'$ thus goes.

The transformation (34), and (35) with the $a$ as just fixed, give a transformation

$$z'_i = \tau_0 y_1 + \cdots + \tau_i y_n, \quad i = 1, \ldots, q + 1,$$

where each $\tau$ is a linear combination, with rational coefficients, of the $t_{ij}$ with $i \leq q + 1$.\footnote{The condition for a polynomial to be contained in a prime p.i. is that its remainder with respect to the characteristic set vanish.} From (35), (36), we see that the $t_{ij}$ with $i \leq q + 1$ are linear in the $\tau$ with integral coefficients.

In $B''$, we substitute for each $t$ its expression in terms of the $\tau$ and we regard the symbols $\tau$ as indeterminates instead of linear combinations of the $t$. Then $B''$ goes over into a polynomial $B'''$ in the $z'_i$, $\tau_{ij}$, $i = 1, \ldots, q + 1$. We see that $B'''$ vanishes identically in the $\tau$ if we replace the $z'$ by their expressions in (36), with the $y$ a generic zero of $\Sigma$. We now replace, in $B'''$, each $\tau_{ij}$ by $t_{ij}$ and each $z'_i$ by $z_i$. Then $B'''$ goes over into a polynomial $C$ in $z_1, \ldots, z_{q+1}$ and the $t$, $C$ being of degree $m$ as a polynomial in the $z$ and of degree $m$ in each $z$ separately. $C$ vanishes for the $z$ as in (34) with the $y$ a generic zero of $\Sigma$.

Evidently the relation $C = 0$ just described will subsist if we replace $z_1, \ldots, z_{q+1}$ by any $q + 1$ of the $z_i$, provided that a corresponding substitution is made for the $t$ in $C$.

We now specialize the $t$ in (34) as integers with a nonvanishing determinant, in such a way that, for every set of $q + 1$ indeterminates $z$, the polynomial over $F$ obtained from $C$ remains of effective degree $m$ in each $z$ appearing in it.

34. We consider the transformation (34) with the $t$ as just fixed. If the $y$ are replaced in (33) in terms of the $z$, we get a system $\Phi$ of $p$ polynomials in the $z$. Let characteristic sets be determined for a set of prime p.i. equivalent to $\Phi$. Let $\Sigma_1, \ldots, \Sigma_n$ be those prime p.i. which do not contain the initial of any $A$ in (33), the $y$ being replaced in the initials in terms of the $z$.\footnote{This is seen from (32).} There will be one of the $\Sigma_i$ which holds the remaining $\Sigma_i$. This is because, in a resolution of (33) into an equivalent set of prime p.i., none of which is a divisor of any other, there is precisely one p.i. which contains no initial. To determine which $\Sigma_i$ holds the others, all we need do is to find a $\Sigma_i$ whose characteristic set holds the other $\Sigma_i$. Suppose, for instance, that the characteristic set of $\Sigma_1$ holds $\Sigma_2, \ldots, \Sigma_n$. Then, if $\Sigma_1$ does not hold $\Sigma_j$, the initial of some polynomial in the characteristic set of $\Sigma_1$ must hold $\Sigma_j$. Then surely $\Sigma_j$ cannot hold $\Sigma_1$. Thus, if $\Sigma_1$ does not hold all $\Sigma_i$, no $\Sigma_j$ can hold all $\Sigma_i$. Then $\Sigma_1$ holds all $\Sigma_i$. $\Sigma_1$ is obtained from $\Sigma$ of §32 by replacing the $y$ in terms of the $z$. We shall
prove that \( \Sigma_1 \) has the same dimension as \( \Sigma \). To begin with, it is easy to see that the polynomials in any \( q + 1 \) of the \( z \), found in §33, belong to \( \Sigma_1 \). On the other hand, if there were fewer than \( q \) indeterminates in a parametric set of \( \Sigma_1 \), we could use a characteristic set of \( \Sigma_1 \) to determine a nonzero polynomial in \( \mathfrak{F}[y_1, \cdots, y_q] \) belonging to \( \Sigma \).

Changing the notation if necessary, let \( z_1, \cdots, z_q \) be a parametric set for \( \Sigma_1 \). Then \( \Sigma_1 \) will have a characteristic set

\[(37) \quad B_1, \cdots, B_p\]

in which \( B_i \) introduces \( z_q + i \).

35. We construct a resolvent \( R = 0 \) for \( \Sigma_1 \), with

\[(38) \quad w = a_1 z_q + 1 + \cdots + a_p z_n,\]

the \( a \) being integers. Let \( R \) be of degree \( g \) in \( w \).

We shall prove that the initial of \( R \) is an element of \( \mathfrak{F} \). According to §33, each \( z_i, i > q \), in a zero of \( \Sigma_1 \) satisfies with \( z_1, \cdots, z_q \) a fixed equation of degree \( m \) in \( z_i \), the coefficient of \( z_i^m \) being an element of \( \mathfrak{F} \). The coefficient just mentioned will be assumed to be unity. Then (38) shows that \( w \) satisfies with \( z_1, \cdots, z_q \) an equation in which the highest power of \( w \) is unity.\textsuperscript{28} This implies that in the irreducible polynomial \( R \), the coefficient of \( w^g \) is free of \( z_1, \cdots, z_q \).

We may and shall assume that coefficient to be unity.

Referring to §25, we see that

\[(39) \quad z_i = \frac{E_{i0} w + E_{i1} w + \cdots + E_{i, q-1} w^{q-1}}{D},\]

\( i = q + 1, \cdots, n \), where \( D \) and the \( E \) are in\textsuperscript{29} \( \mathfrak{F}[z_1, \cdots, z_q] \).

36. Let \( t_1, \cdots, t_p; v \) be new indeterminates and let

\[ \Lambda = (\Sigma_1, v - t_1 z_q + 1 - \cdots - t_p z_n) \]

in \( \mathfrak{F}[z; t; v] \). Then \( \Lambda \) is a prime p.i. Also \( \Lambda \) contains an irreducible polynomial \( U \) in \( v, z_1, \cdots, z_q \) and the \( t \), the coefficient of whose highest power of \( v \), say \( v^d \), is unity.\textsuperscript{30}

We shall prove that \( d = g \). We see first, following §25, that \( d \leq g \). As \( v \), in a zero of \( \Lambda \), equals \( w \) if \( t_i = a_i, i = 1, \cdots, p \), we cannot have \( d < g \).

Let \( v \) be replaced in \( U \) by

\[(40) \quad t_1 z_q + 1 + \cdots + t_p z_n.\]

Then \( U \) becomes a polynomial \( V \) in \( z_1, \cdots, z_n \) and the \( t \). Let \( V \) be arranged as a polynomial in the \( t \) with coefficients which are polynomials in the \( z \).

\textsuperscript{28} This is analogous to the fact that the sum of several algebraic integers is an integer. See Landau, \textit{Zahlentheorie}, vol. 3, p. 71.

\textsuperscript{29} The relations (39) hold for any zero of \( \Sigma_1 \) with \( D \neq 0 \), and for the corresponding \( w \).

\textsuperscript{30} Note that each \( t_i z_q + i \) satisfies an equation in which the coefficient of the highest power of \( t_i z_q + i \) is unity.

\textsuperscript{31} As the coefficient of \( v^d \) in \( U \) is unity, \( U \) cannot vanish identically for \( t_i = a_i \).
Let \( \Psi \) be the finite system of those coefficients (polynomials in the \( z \)). We are going to prove, in the following sections, that \( \Psi \) is equivalent to \( \Sigma \). Thus, if the \( z \) are replaced in \( \Psi \) by their expressions (3.4), we get a finite system of polynomials equivalent to \( \Sigma \). We shall thus have solved the problem stated in §32.

37. We begin with the observation that for given elements \( z_1, \ldots, z_n \) of an extension \( \mathfrak{F}_1 \) of \( \mathfrak{F} \) to constitute a zero of \( \Psi \), it is necessary and sufficient that for \( z_1, \ldots, z_n \) as just given, \( V \) vanish for arbitrary \( t \) in \( \Sigma_1 \). This shows, in particular, that \( \Psi \) holds \( \Sigma \).

Let \( G \) be the discriminant of \( R \) with respect to \( w \) and let

\[
H = DG
\]

where \( D \) is as in (39). We shall prove that every zero of \( \Psi \) with \( H \neq 0 \) is a zero of \( \Sigma_1 \). Let \( \eta_1, \ldots, \eta_q \) be such a zero of \( \Psi \). For \( z_i = \eta_i, i = 1, \ldots, q \), \( R \) becomes a polynomial \( T \) in \( w \). From §21, we see that \( T \) has \( g \) zeros in some extension of \( \mathfrak{F}(\eta_1, \ldots, \eta_q) \). These zeros are distinct, because \( \eta_1, \ldots, \eta_q \) do not annul \( G \). Using each such \( w \) in (39), we get \( g \) distinct zeros,

\[
\eta_1, \ldots, \eta_q; \quad z^{(j)}_{q+1}, \ldots, z^{(j)}_n, \quad j = 1, \ldots, g,
\]

of \( \Sigma_1 \). Let \( Z \) be the polynomial which \( U \) becomes for \( z_i = \eta_i, i = 1, \ldots, q \).

Then

\[
(41) \quad Z = \prod_{j=1}^g (w - t_j z^{(j)}_{q+1} - \cdots - t_j z^{(j)}_n).
\]

But \( v - t_i \eta_{q+1} - \cdots - t_i \eta_n \) is a factor of \( Z \). This shows that, for some \( j \),

\[
z^{(j)}_i = \eta_i, \quad i = q + 1, \ldots, n,
\]

and proves our statement.

38. We have to show that a zero \( \eta_1, \ldots, \eta_n \) of \( \Psi \) which annuls \( H \) is a zero of \( \Sigma_1 \). Our proof will employ a Newton polygon process, which we can carry out rapidly by using the material of Chapter III.

For \( z_i = \eta_i, i = 1, \ldots, q \), \( R \) becomes a polynomial \( J \) in \( w \). In some extension \( \mathfrak{F}_1 \) of \( \mathfrak{F}(\eta_1, \ldots, \eta_q) \), \( J \) has \( g \) linear factors. We write

\[
J = (w - \xi_1) \cdots (w - \xi_g).
\]

Now let \( b_1, \ldots, b_q \) be integers such that

\[
H(\eta_1 + b_1, \ldots, \eta_q + b_q) \neq 0.
\]

Then, if \( c \) is an indeterminate,

\[
(42) \quad H(\eta_1 + b_1c, \ldots, \eta_q + b_qc)
\]

is a polynomial in \( c \) which is not identically zero. We put in \( R \),

\[\text{--- This means that } V \text{ vanishes identically in the } t.\]

\[\text{--- Note that } Z \text{ is a polynomial in } \nu \text{ and the } t \text{ which vanishes for } v = t_z^{(j)}_{q+1} + \cdots + t_z^{(j)}_n.\]

We have thus \( g \) distinct factors of \( Z \). As \( Z \) is of degree \( g \) in \( \nu \), with unity for the coefficient of \( \nu^g \), it has the expression in (41).
\[ z_i = \eta_i + b_i c, \quad i = 1, \ldots, q. \]

Then \( R \) goes over into a polynomial \( K \) in \( w \) whose coefficients are polynomials in \( c \). In \( K \), we put \( w = \xi_1 + w_1 \). Then \( K \) becomes an expression \( K' \) in \( w_1 \) and \( c \) which we write

\[ K' = a'(c) + \sum_{i=1}^{g} b_i'(c) w_i. \]  

We shall now regard \( \mathfrak{S}_1 \) as a differential field in which every derivative is zero. Furthermore, we regard \( w_1 \) as a differential indeterminate and \( c \) as an arbitrary constant. We wish to show that \( K' \) in \((43)\) is annulled either by \( w_1 = 0 \) or by a series

\[ w_1 = \varphi_0 c^\rho + \cdots + \varphi_k c^\rho + \cdots \]  

similar to the series employed in Chapter III, with the distinction that \( \rho_2 \), while positive, need not exceed unity.

It may be that \( K' \) is annulled by \( w_1 = 0 \). Let us suppose that this does not happen. Then \( a'(c) \) is not zero. We compare \((43)\) with \((3)\) of III, \( \S 7 \). The role of \( U_i' \) is taken over by \( w_i' \). Because \( K' \) vanishes when \( w_1 \) and \( c \) are replaced by zero, the lowest exponent of \( c \) in \( a' \) is positive. Again, the only exponent of \( c \) in \( b_i' \) is zero. Thus \( \rho_2 \) of III, \( \S 7 \), will be positive. Without further change, the work of Chapter III furnishes the series in \((44)\).

Let

\[ \alpha_1 = \xi_1 + \varphi_0 c^\rho + \cdots + \varphi_k c^\rho + \cdots. \]

We have

\[ K = (w - \alpha_1)K_1 \]

where \( K_1 \) is a polynomial in \( w \) of degree \( g - 1 \), whose coefficients are series in \( c \). The terms free of \( c \) in \( K_1 \) are annulled by \( w = \xi_1 \). When \( w \) is replaced by \( \xi_1 + w_1 \), \( K_1 \) goes over into an expression \( K' \) like that in \((43)\) except that the \( a' \) and \( b' \) are infinite series of fractional powers instead of polynomials. We secure a series like \((44)\) which annuls the \( K' \) with which we are now working.

All in all, we have a representation of \( K \)

\[ K = (w - \alpha_1) \cdots (w - \alpha_g) \]

where each \( \alpha_i \) is a series of the type

\[ \alpha_i = \xi_i + \varphi_i c^\rho + \cdots. \]  

The \( \rho \) and the \( \varphi \) depend on \( i \). If we replace \( c \) by a suitable positive integral power \( h^r \) of an indeterminate \( h \), we have, for \( i = 1, \ldots, g, \)

\[ \alpha_i = \xi_i + \psi_1 h + \psi_2 h^2 + \cdots. \]

The \( \psi \) all lie in some extension of \( \mathfrak{S}_1 \).
From this point on, we regard our fields as algebraic fields and \( h \) as an algebraic indeterminate.

The \( \alpha \) are distinct, since \( G \) does not vanish for

\[(47) \quad z_i = \eta_i + b_i h^r, \quad i = 1, \ldots, q.\]

We use (39), understanding that (47) holds and that \( w = \alpha i \). We secure \( g \) distinct zeros of \( \Sigma_1 \),

\[\eta_1 + b_1 h^r, \ldots, \eta_q + b_q h^r; \quad z_{q+1}^{(q)}, \ldots, z_n^{(q)}, \quad j = 1, \ldots, g.\]

Each \( z_i^{(q)} \) is a series of integral powers of \( h \). Such a series can contain no negative power of \( h \). This follows from the fact that \( \Sigma_1 \) contains a polynomial in \( z_1, \ldots, z_n, z_i \) in which one of the terms of highest degree is a term in \( z_i \) alone (§33).

Let \( \xi^{(q)} \) be the term of \( z_i^{(q)} \) which is of zero degree in \( h \). Then, for every \( j \),

\[\eta_1, \ldots, \eta_q; \quad \xi_{q+1}^{(q)}, \ldots, \xi_n^{(q)}\]

is a zero of \( \Sigma_1 \).

Let \( Z_k \) be the polynomial in \( v \) and \( t_1, \ldots, t_p \) which \( U \) of §36 becomes for (47). Then

\[Z_h = \prod_{j=1}^g (v - t_j z^{(q)}_{q+1} - \cdots - t_p z^{(q)}_n).\]

Letting \( Z_0 \) represent \( Z_h \) with \( h = 0 \), we have

\[Z_0 = \prod_{j=1}^g (v - t_j \xi_{q+1}^{(q)} - \cdots - t_p \xi_n^{(q)}).\]

Now \( v - t_1 \eta + 1 - \cdots - t_p \eta_n \) is a factor of \( Z_0 \). This shows that \( \eta_1, \ldots, \eta_n \) are the \( \xi^{(q)} \) for some \( j \), so that, as we undertook to prove, \( \eta_1, \ldots, \eta_n \) is a zero of \( \Sigma_1 \).

We have thus proved that \( \Psi \) is equivalent to \( \Sigma_1 \).

**An approximation theorem**

39. Working in the analytic case, we prove the following theorem.

**Theorem:** Let \( \Sigma \) be a prime p.i. in \( y_1, \ldots, y_n \). Let \( B \) be any polynomial not contained in \( \Sigma \). Given any zero of \( \Sigma \), consisting of functions analytic in an open region \( B \), there is an open region \( C \), contained in \( B \), in which the given zero can be approximated uniformly, with arbitrary closeness, by zeros of \( \Sigma \) for which \( B \) is distinct from zero throughout \( C \).

We assume, as we may, that \( \Sigma \) is nontrivial. If the transformation of §33 is effected, \( \Sigma \) may be replaced by \( \Sigma_1 \), while \( B \) goes over into a polynomial \( B_1 \) in \( z_1, \ldots, z_n \).

\( B_1 \) is not in \( \Sigma_1 \). Let \( z_{q+1}, \ldots, z_n \) be replaced in \( B_1 \) by their expressions (39). We find that, for every zero of \( \Sigma_1 \) with \( D \neq 0 \),
(48) \[ B_1 = \frac{M}{D^\mu} \]

where \( M \) is a polynomial in \( w; z_1, \cdots, z_q \). Because \( DB_1 \) is not in \( \Sigma_1 \), \( M \) is not divisible by \( R \) of \$35. Thus we have

\[ XR + YM = N \]

where \( N \) is a nonzero polynomial in \( z_1, \cdots, z_q \). A zero of \( \Sigma_1 \) which annuls \( B_1 \) annuls \( N \).

Let \( \eta_1, \cdots, \eta_q \) be a zero of \( \Sigma_1 \), analytic in an open region \( B \), which annuls \( N \).

Shrinking \( B \) if necessary, we assume that every one of the polynomials in \( w \) and the \( z \) which we meet in what follows has its coefficients analytic throughout \( B \).

Let \( H_1 = NH \). We use constants \( b_i \) such that

\[ H_1(\eta_1 + b_1, \cdots, \eta_q + b_q) \]

does not vanish for every \( z \). Then, if \( h \) is a complex variable,

(49) \[ H_1(\eta_1 + b_1h, \cdots, \eta_q + b_qh) \]

is a polynomial in \( h \) of the type

(50) \[ \alpha_r h^r + \cdots + \alpha_s h^s \]

where the \( \alpha \) are functions of \( z \) analytic in \( B \). As \( H_1 \) in (49) vanishes for \( h = 0 \), we have \( r > 0 \). We assume that \( \alpha_r \) is not identically zero.

Let \( B_1 \) be a simply connected open region contained with its boundary in \( B \), in which \( \alpha_r \) is bounded away from zero. Let \( h \) be small but distinct from zero. Then (50) cannot be zero at any point of \( B_1 \). Thus, if

(51) \[ z_i = \eta_i + b_ih, \quad i = 1, \cdots, q, \]

\( R = 0 \) will have \( g \) distinct solutions for \( w, \) each analytic in \( B_1 \). This is because \( H_1 \) is divisible by the discriminant of \( R \).

As \( H_1 \) is divisible by \( D \) in (39), \( \Sigma_1 \) will have \( g \) distinct zeros with \( z_1, \cdots, z_q \) as in (51),

\[ z_1, \cdots, z_q; \quad z_{q+1}^{(k)}, \cdots, z_n^{(k)}, \quad k = 1, \cdots, g, \]

each consisting of functions analytic in \( B_1 \). The \( z^{(k)} \) are given by (39).

Consider a sequence of nonzero values of \( h \) which tend towards zero,

(52) \[ h_1, h_2, \cdots, h_j, \cdots, \]

each \( h_j \) being so small that (50) is distinct from zero throughout \( B_1 \). For each \( j \), if

(53) \[ z_i = \eta_i + b_ij, \quad i = 1, \cdots, q, \]

\( U \) of \$36 will vanish if
\[(54) \quad v = t_1z_q^{(2)} + \cdots + t_nz_n^{(2)} ,\]

\(k = 1, \cdots, g.\) It is understood, of course, that the \(z^{(k)}\), which are analytic throughout \(B_1\), depend on \(h_j\). For any \(h_j\), the \(g\) expressions (54) are distinct.

As the equation of degree \(m\) which a \(z_j, j > q\), satisfies with \(z_1, \cdots, z_q\) has unity for the coefficient of \(z_j^m\), there is a positive number \(d\), such that, throughout \(B_1\),

\[(55) \quad \left| z_j^{(k)} \right| < d\]

for \(j = q + 1, \cdots, n; k = 1, \cdots, g\) and for every \(h\) in (52). This is because the coefficients of \(z_j^{m-1}, \cdots, z_j^0\) in the above mentioned equation are bounded quantities.

For each \(h_j\) of (52), let one of the \(g\) expressions (54) be selected, and be designated by \(v^{(j)}\). We form thus a sequence

\[(56) \quad v', v'', \cdots, v^{(j)}, \cdots.\]

Let \(C\) be any open region which lies with its boundary in \(B_1\). From (56) we see, using a well known theorem on bounded families of analytic functions,\(^{34}\) that, for some subsequence of (56), the coefficients of each \(t_i, i = 1, \cdots, p\), converge uniformly throughout \(C\) to an analytic function \(\eta_i\). We find thus that if

\[(57) \quad z_i = \eta_i, \quad i = 1, \cdots, q,\]

\(U\) vanishes for

\[v = t_1\eta_q^{(2)} + \cdots + t_n\eta_n^{(2)}.\]

Deleting elements of (56) if necessary, we assume that the convergence occurs when the complete sequence (56) is used, rather than one of its subsequences. For each \(h_j\), there are \(g - 1\) expressions (54) not used in (56). Let one of these be selected for each \(h_j\) and let (56) be used now to represent the sequence thus obtained. As above, we select a subsequence of (56) for which the coefficients of each \(t_i\) converge uniformly in \(C\). This gives a second expression which causes \(U\) to vanish when (57) holds. Continuing, we find \(g\) expressions

\[(58) \quad v = t_1\eta_q^{(2)} + \cdots + t_n\eta_n^{(2)}, \quad k = 1, \cdots, g,\]

which make \(U\) vanish when (57) holds.

Let \(v_k\) represent the second member of (58). Again, let \(w_k\) represent the second member of (54), it being understood that the subscripts \(k\) are assigned, for each \(h_j\), in such a way that the coefficient of \(t_i\) in \(w_k\) converges to that in \(v_k\) as \(h_j\) approaches zero.

Then, since the \(g\) expressions \(w_k\) are distinct from one another for each \(h_j\), we will have, representing by \(Z_j\) the polynomial which \(U\) becomes when (53) holds,

\[ Z_j = (v - w_1) \cdots (v - w_p). \]

By continuity, if we represent \( U \), when (57) holds, by \( Z \),
\[ Z = (v - v_1) \cdots (v - v_p). \]

As \( v - t_1 \eta_{q+1} - \cdots - t_p \eta_n \) is a factor of \( Z \), it must be that, for some \( k \),
\[ \eta_i = \eta_i^{(k)}, \quad i = q + 1, \ldots, n. \]

Thus \( \eta_1, \ldots, \eta_n \) can be approximated uniformly in \( C \), with arbitrary closeness, by zeros of \( \Sigma \), for which \( B_1 \) is distinct from zero throughout \( C \). As the \( y \) vary continuously with the \( z \), we have our theorem.

**Zeros and characteristic sets**

40. We consider a nontrivial prime p.i. \( \Sigma \) in \( \mathfrak{F}[u_1, \ldots, u_q; y_1, \ldots, y_p] \) with the \( u \) a parametric set. Let
\begin{equation}
(59) \quad A_1, \cdots, A_p
\end{equation}
be a characteristic set for \( \Sigma \). We know that every zero of (59) for which no initial vanishes is a zero of \( \Sigma \). We shall prove that every zero of (59) for which no separant vanishes is a zero of \( \Sigma \).

Let \( \eta_1, \ldots, \eta_n \) be a zero of (59) which annihilates no separant.

In \( A_1 \), we replace \( u_i \) by \( \eta_i + \tau_i, i = 1, \ldots, q \), where the \( \tau \) are indeterminates, and \( y_1 \) by \( \eta_{q+1} + y_1' \). Then \( A_1 \) goes over into a polynomial \( B_1 \) in \( y_1' \) and the \( \tau \) which vanishes when the indeterminates are all replaced by zero. Because the separant of \( A_1 \) does not vanish for the \( \eta \), \( B_1 \) contains a term \( \alpha y_1' \) with \( \alpha \) in \( \mathfrak{F}(\eta_1, \ldots, \eta_n) \) and distinct from zero. We solve the equation \( B_1 = 0 \) for \( y_1' \) in terms of the \( \tau \), using the formal process of the implicit function theorem for securing a representation of \( y_1' \) as an infinite series of powers of the \( \tau \). We can do this because of the presence of \( \alpha y_1' \). Let \( \xi_1 \) be the series thus obtained for \( y_1' \). The terms of \( \xi_1 \) are all of positive degree.

The set
\begin{equation}
(60) \quad \eta_1 + \tau_1, \ldots, \eta_q + \tau_q; \quad \eta_{q+1} + \xi_1
\end{equation}
is a generic zero of the prime p.i. in \( y_1 \) and the \( u \) for which \( A_1 \) is a characteristic set.

We substitute the quantities (60) into \( A_2 \) and replace \( y_2 \) by \( \eta_{q+2} + y_2' \). Then \( A_2 \) goes over into a polynomial \( B_2 \) in \( y_2' \). The coefficients in \( B_2 \) are series of nonnegative powers of the \( \tau \) and the coefficient of \( y_2' \) contains a term free of the \( \tau \). We can thus solve \( B_2 = 0 \) for \( y_2' \), expressing \( y_2' \) as a series \( \xi_2 \) of powers of the \( \tau \), the terms of \( \xi_2 \) being of positive degree. By §29,
\[ \eta_1 + \tau_1, \ldots, \eta_q + \tau_q; \quad \eta_{q+1} + \xi_1, \quad \eta_{q+2} + \xi_2 \]
is a generic zero of the prime p.i. \( \Sigma_2 \) for which \( A_1, A_2 \) is a characteristic set. It follows that \( \eta_1, \ldots, \eta_{q+2} \) is a zero of \( \Sigma_2 \). Continuing, we find that \( \eta_1, \ldots, \eta_n \) is a zero of \( \Sigma \).