THEOREM. *A necessary and sufficient condition for two binary forms to have a common factor other than a constant is that their resultant be zero.*

If $a_0$ and $b_0$ are both different from zero, the non-homogeneous polynomials $F$ and $\Phi$ correspond to the forms $f$ and $\phi$ according to the definition of § 62. Accordingly, by Theorem 2 of that section a necessary and sufficient condition that $f$ and $\phi$ have a common factor other than a constant is, in this case, the vanishing of their resultant.

On the other hand, if $a_0 = b_0 = 0$, $f$ and $\phi$ have the common factor $x_2$, and the resultant of $f$ and $\phi$ obviously vanishes.

A similar remark applies to the case in which all the $a$'s or all the $b$'s are zero.

There remain then only the following two cases to be considered,

(1) $\quad a_0 \neq 0;\ b_0 = b_1 = \cdots = b_k = 0,\ b_{k+1} \neq 0 \qquad (k < m),$

(2) $\quad b_0 \neq 0;\ a_0 = a_1 = \cdots = a_k = 0,\ a_{k+1} \neq 0 \qquad (k < n).$

In Case (1), $F$ corresponds to $f$, and, if we write

$$\phi(x_1, x_2) \equiv x_2^{k+1}\phi_1(x_1, x_2),$$

$\Phi$ corresponds to $\phi_1$. Now we know in this case (cf. § 71) that $R \neq 0$ is a necessary and sufficient condition that $F$ and $\Phi$ be relatively prime. Accordingly, by Theorem 2, § 62, it is also a necessary and sufficient condition that $f$ and $\phi_1$ be relatively prime. But since $x_2$ is not a factor of $f$, the two forms $f$ and $\phi$ will be relatively prime when and only when $f$ and $\phi_1$ are relatively prime. Thus our theorem is proved in this case.

The proof in Case (2) is precisely similar to that just given.

# CHAPTER XVI

## FACTORS OF POLYNOMIALS IN TWO OR MORE VARIABLES

**73. Factors Involving only One Variable of Polynomials in Two Variables.** We have seen in the last chapter that polynomials in one variable are always reducible when they are of degree higher than the first. Polynomials in two, or more, variables are, in general, not reducible, as we have already noticed in the special case of quadratic forms.

Let $f(x, y)$ be any polynomial in two variables, and suppose it arranged according to powers of $x$,

$$f(x, y) \equiv a_0(y)x^n + a_1(y)x^{n-1} + \cdots + a_{n-1}(y)x + a_n(y),$$

the $a$'s being polynomials in $y$.

THEOREM 1. *A necessary and sufficient condition that a polynomial in $y$ alone, $\psi(y)$, be a factor of $f(x, y)$ is that it be a factor of all the $a$'s.*

The condition is clearly sufficient. To prove that it is necessary, let us suppose that $\psi(y)$ is a factor of $f(x, y)$. Then

$$(1) \qquad a_0(y)x^n + \cdots + a_n(y) \equiv \psi(y)[b_0(y)x^n + \cdots + b_n(y)],$$

where the $b$'s are polynomials in $y$. For any particular value of $y$ we deduce from (1), which is then an identity in $x$, the following equations:

$$\begin{cases} a_0(y) = \psi(y)b_0(y), \\ a_1(y) = \psi(y)b_1(y), \\ \cdots\cdots\cdots \\ a_n(y) = \psi(y)b_n(y). \end{cases}$$

Since these equations hold for every value of $y$, they are identities, and $\psi(y)$ is a factor of all the $a$'s.

THEOREM 2. *If $f(x, y)$ and $\phi(x, y)$ are any two polynomials in $x$ and $y$, and $\psi(y)$ is an irreducible polynomial in $y$ alone* which is a factor of the product $f\phi$, then $\psi$ is a factor of $f$ or of $\phi$.*

Let $$f(x, y) \equiv a_0(y)x^n + a_1(y)x^{n-1} + \cdots + a_n(y),$$
and $$\phi(x, y) \equiv b_0(y)x^m + b_1(y)x^{m-1} + \cdots + b_m(y);$$
then
$$f(x, y)\phi(x, y) \equiv a_0b_0x^{n+m} + (a_0b_1 + a_1b_0)x^{n+m-1} + (a_0b_2 + a_1b_1 + a_2b_0)x^{n+m-2} + \cdots + a_nb_m.$$

In order to prove that $\psi$ is a factor either of $f$ or of $\phi$ we must prove that it is either a factor of all the $a$'s or of all the $b$'s. If this were not the case, we could find a first $a$ in the sequence $a_0, a_1, \cdots a_n$ of which $\psi$ is not a factor. Call this function $a_i$. There would also be a first $b$ in the sequence of $b_0, b_1, \cdots b_m$ which is not divisible by $\psi$. Call this function $b_j$. Our theorem will be proved if we can show that this assumption, that $a_i$ and $b_j$ are not divisible by $\psi$ while all the functions $a_0, \cdots a_{i-1}$, $b_0, \cdots b_{j-1}$, are divisible by $\psi$, leads to a contradiction. For this purpose let us consider in the product $f\phi$ the coefficient of $x^{(n-i)+(m-j)}$, which may be written

$$a_0b_{i+j} + \cdots + a_{i-1}b_{j+1} + a_ib_j + a_{i+1}b_{j-1} + \cdots + a_{i+j}b_0,$$

provided we agree that the $a$'s and $b$'s with subscripts greater than $n$ and $m$ respectively shall be identically zero. Since $f\phi$ is by hypothesis divisible by $\psi$, it follows from Theorem 1 that the last written expression must be divisible by $\psi$. This being obviously the case for all the terms which preceed and for all which succeed the term $a_ib_j$, it follows that this term must also be divisible by $\psi$, so that among the linear factors of the function $a_ib_j$ must be found $\psi$. But by Theorem 1, § 65, the function $a_ib_j$ can be resolved into its linear factors in essentially only one way, and one way of so resolving it is to resolve $a_i$ and $b_j$ into their linear factors. Since $\psi$ is *not* one of these factors, we are led to a contradiction, and our theorem is proved.

An important corollary of our theorem is:

COROLLARY. *Let $f(x, y)$ and $\phi(x, y)$ be polynomials in $(x, y)$, and let $\psi(y)$ be a polynomial in $y$ alone. If $\psi$ is a factor of the product of $f\phi$ but is relatively prime to $\phi$, then $\psi$ is a factor of $f$.*

* That is, a linear polynomial.



If $\psi$ is irreducible, this corollary is identical with the theorem. Let us suppose $\psi$ resolved into its irreducible factors none of which are constants, that is, into its factors of the first degree:

$$\psi(y) \equiv \psi_1(y)\,\psi_2(y)\cdots\psi_k(y).$$

Now consider the identity which expresses the fact that $\psi$ is a factor of $f\phi$:

(2) $$f(x, y)\phi(x, y) \equiv \psi_1(y)\psi_2(y)\cdots\psi_k(y)G(x, y).$$

This shows that $\psi_1(y)$ is a factor of $f\phi$ and hence, by Theorem 2, it is a factor either of $f$ or of $\phi$. Since $\psi$ and $\phi$ are relatively prime, $\psi_1$ cannot be a factor of $\phi$. It must then be a factor of $f$:

$$f(x, y) \equiv \psi_1(y)f_1(x, y).$$

Substituting this in (2), and cancelling out $\psi_1$, as we have a right to do since it is not identically zero, we get

(3) $$f_1(x, y)\phi(x, y) \equiv \psi_2(y)\cdots\psi_k(y)G(x, y).$$

From this we infer that $\psi_2$, being a factor of $f_1\phi$, must be a factor of $f_1$:

$$f_1(x, y) \equiv \psi_2(y)f_2(x, y).$$

We substitute this in (3) and cancel out $\psi_2$. Proceeding in this way we get

$$f(x, y) \equiv \psi_1(y)\psi_2(y)\cdots\psi_k(y)f_k(x, y) \equiv \psi(y)f_k(x, y),$$

an identity which proves our corollary.

**EXERCISE**

If $f(x, y)$ and $\phi(x, y)$ are polynomials, then any two sets of polynomials

$$P_1(y),\ Q_1(x, y),\ R_1(x, y),$$
$$P_2(y),\ Q_2(x, y),\ R_2(x, y),$$

will be proportional to each other provided,

(*a*) they satisfy the identities

$$P_1(y)f(x, y) \equiv Q_1(x, y)\phi(x, y) + R_1(x, y),$$
$$P_2(y)f(x, y) \equiv Q_2(x, y)\phi(x, y) + R_2(x, y);$$

(*b*) there is no factor other than a constant common to $P_1$, $Q_1$, and also no factor other than a constant common to $P_2$, $Q_2$;

(*c*) $R_1$ and $R_2$ are both of lower degree in $x$ than $\phi$.

(Cf. Theorem 2, § 63.)

**74. The Algorithm of the Greatest Common Divisor for Polynomials in Two Variables.** We will consider the two polynomials in $x$ and $y$,

$$f(x, y) \equiv a_0(y)x^n + a_1(y)x^{n-1} + \cdots + a_n(y),$$
$$\phi(x, y) \equiv b_0(y)x^m + b_1(y)x^{m-1} + \cdots + b_m(y),$$

and assume $a_0 \not\equiv 0$, $b_0 \not\equiv 0$, $n \geqq m > 0$.

Theorem 1 of the last section in combination with the results of § 67 enables us to get all the common factors of $f$ and $\phi$ which involve $y$ only; for such factors must be common factors of all the $a$'s and all the $b$'s.

It remains, then, merely to devise a method of obtaining the common factors of $f$ and $\phi$ which do not themselves contain factors in $y$ alone. We will show how this can be done by means of the algorithm of the greatest common divisor.

Dividing $f$ by $\phi$ (cf. § 63, Theorem 2), we get the identity

$$P_0(y)f(x, y) \equiv Q_0(x, y)\phi(x, y) + R_1(x, y),$$

when $R_1$ is either identically zero, or is of lower degree in $x$ than $\phi$. If $R_1 \not\equiv 0$, divide $\phi$ by $R_1$, getting the identity

$$P_1(y)\phi(x, y) \equiv Q_1(x, y)R_1(x, y) + R_2(x, y),$$

where $R_2$ is either identically zero, or is of lower degree in $x$ than $R_1$. If $R_2 \not\equiv 0$, divide $R_2$ by $R_1$. Proceeding in this way, we get the following system of identities in which the degrees in $x$ of $R_1, R_2, \cdots$ continually decrease, so that after a certain number of steps we reach an $R$, say $R_{\rho+1}$, which is independent of $x$:

$$(1)\quad \begin{cases} P_0(y)f(x, y) \equiv Q_0(x, y)\phi(x, y) + R_1(x, y), \\ P_1(y)\phi(x, y) \equiv Q_1(x, y)R_1(x, y) + R_2(x, y), \\ P_2(y)R_1(x, y) \equiv Q_2(x, y)R_2(x, y) + R_3(x, y), \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ P_{\rho-1}(y)R_{\rho-2}(x, y) \equiv Q_{\rho-1}(x, y)R_{\rho-1}(x, y) + R_\rho(x, y), \\ P_\rho(y)R_{\rho-1}(x, y) \equiv Q_\rho(x, y)R_\rho(x, y) + R_{\rho+1}(y). \end{cases}$$

Theorem 1. *A necessary and sufficient condition that $f$ and $\phi$ have a common factor which involves $x$ is*

$$R_{\rho+1}(y) \equiv 0.$$



In order to prove this theorem we first note that, by the first of the identities (1), any common factor of $f$ and $\phi$ is a factor of $R_1$, hence, by the second of the identities, it is a factor of $R_2$, etc. Finally we see that *every common factor of $f$ and $\phi$ is a factor of all the $R$'s.* But $R_{\rho+1}$ does not contain $x$. Hence if $f$ and $\phi$ have a common factor which contains $x$, $R_{\rho+1}(y) \equiv 0$.

Now suppose conversely that $R_{\rho+1}(y) \equiv 0$, and let

$$(2)\qquad R_\rho(x, y) \equiv S(y)G(x, y),$$

where $G$ has no factor in $y$ alone.* The last identity (1) then tells us that $P_\rho(y)$ is a factor of

$$Q_\rho(x, y)S(y)G(x, y),$$

and since by hypothesis $G$ has no factor in $y$ alone, $P_\rho(y)$ must, by the Corollary of Theorem 2, § 73, be a factor of $Q_\rho S$, that is

$$(3)\qquad Q_\rho(x, y)S(y) \equiv P_\rho(y)H(x, y).$$

Substituting first (2) and then (3) in the last identity (1), and cancelling out the factor $P_\rho(y)$ from the resulting identity, as we have a right to do since $P_\rho(y) \not\equiv 0$, we get the result

$$R_{\rho-1}(x, y) \equiv H(x, y)G(x, y).$$

That is, $G$ is a factor not only of $R_\rho$ but also of $R_{\rho-1}$. Accordingly we may write the next to the last identity (1) in the form

$$P_{\rho-1}(y)R_{\rho-2}(x, y) \equiv J(x, y)G(x, y).$$

By the corollary of Theorem 2, § 73, we see that $P_{\rho-1}(y)$ is a factor of $J$, so that $P_{\rho-1}(y)$ can be cancelled out of this last written identity, and we see that $G$ is a factor of $R_{\rho-2}$.

Proceeding in this way, we see that $G$ is a factor of all the $R$'s, and therefore, finally, of $f$ and $\phi$. Moreover, we see from (2) that $G$ is of at least the first degree in $x$, as otherwise $R_\rho$ would not contain $x$, while $R_{\rho+1}$ was assumed to be the first of the $R$'s which did not involve $x$.

Thus our theorem is proved.

Since, as we saw above, every common factor of $f$ and $\phi$ is also a factor of all the $R$'s, it follows from (2) that, if $\psi$ is a common factor of $f$ and $\phi$,

$$G(x, y)S(y) \equiv \psi(x, y)K(x, y).$$

* If $R_\rho$ has no factor in $y$ alone, $S$ reduces to a constant.

If then $\psi$ contains no factor in $y$ alone, $S$ must, by the Corollary of Theorem 2, § 73, be a factor of $K$. Consequently by cancelling out $S$ from the last written identity, we see that $\psi$ is a factor of $G$. That is,

THEOREM 2. *If in Euclid's algorithm $R_{\rho+1} \equiv 0$, the greatest common divisor of $f$ and $\phi$ which contains no factor in $y$ alone is the polynomial $G(x, y)$ obtained by striking from $R_\rho(x, y)$ all factors in $y$ alone.*

We note that if $R_{\rho+1}$ is a constant different from zero, $f$ and $\phi$ are relatively prime; but that the converse of this is not true as the simple example

$$f \equiv 2x^2 + 3y^2, \qquad \phi \equiv x$$

shows.

Going back to the identities (1), we get from the first of these identities, by mere transposition, the value of $R_1$ in terms of $f$ and $\phi$ (and $P_0$, $Q_0$). Substituting this value in the second identity, we get a value for $R_2$ in terms of $f$, $\phi$, and certain $P$'s and $Q$'s. Proceeding in this way, we finally get the formula

$$R_{\rho+1}(y) \equiv F(x, y)f(x, y) + \Phi(x, y)\phi(x, y) \tag{4}$$

where $F$ and $\Phi$ are polynomials in $(x, y)$.

### 75. Factors of Polynomials in Two Variables.

THEOREM 1. *If $f(x, y)$ and $\phi(x, y)$ are any two polynomials in $x$ and $y$, and $\psi(x, y)$ is an irreducible polynomial which is a factor of the product $f\phi$, then $\psi$ is a factor of $f$ or of $\phi$.*

If $\psi$ does not contain both $x$ and $y$, this theorem reduces to Theorem 2, § 73. It remains, then, only to consider the case that $\psi$ involves both variables. In this case, at least one of the polynomials $f$, $\phi$ must be of at least the first degree in $x$. Without loss of generality we may assume this to be $f$. If $\psi$ is a factor of $f$, our theorem is true. Suppose $\psi$ is not a factor of $f$; then, since $\psi$ is irreducible, $f$ and $\psi$ are relatively prime, and if we apply the algorithm of the greatest common divisor to $f$ and $\psi$ (as we did in the last section to $f$ and $\phi$) the first remainder $R_{\rho+1}(y)$ which does not involve $x$ is not identically zero. The identity (4) of the last section now becomes

$$R_{\rho+1}(y) \equiv F(x, y)f(x, y) + \Psi(x, y)\psi(x, y). \tag{1}$$



If we multiply this by $\phi(x, y)$, the second member becomes a polynomial which has $\psi$ as a factor, since, by hypothesis, $f\phi$ has $\psi$ as a factor. We may therefore write

$$R_{\rho+1}(y)\phi(x, y) \equiv \psi(x, y)\chi(x, y). \tag{2}$$

Now no factor other than a constant of $R_{\rho+1}$ can be a factor of $\psi$, since $\psi$ is irreducible. Consequently, by the Corollary of Theorem 2, § 73, $R_{\rho+1}$ is a factor of $\chi(x, y)$. Cancelling out $R_{\rho+1}$ from (2), as we have a right to do since it does not vanish identically, we get an identity of the form

$$\phi(x, y) \equiv \psi(x, y)\chi_1(x, y);$$

that is, $\psi$ is a factor of $\phi$, and our theorem is proved.

By applying this theorem a number of times, we get the

COROLLARY. *If the product of any number of polynomials in two variables,*

$$f_1(x, y)f_2(x, y) \cdots f_k(x, y),$$

*is divisible by an irreducible polynomial $\psi(x, y)$, then $\psi$ is a factor of at least one of the $f$'s.*

We come now to the fundamental theorem of the whole subject of divisibility of polynomials in two variables.

THEOREM 2. *A polynomial in two variables which is not identically zero can be resolved into the product of irreducible factors no one of which is a constant in one, and essentially in only one, way.*

That a polynomial $f(x, y)$ can be resolved into the product of irreducible factors no one of which is a constant in at least one way may be seen as follows. If $f$ is irreducible, no factoring is possible or necessary. If $f$ is reducible, we have

$$f(x, y) \equiv f_1(x, y)f_2(x, y),$$

where neither $f_1$ nor $f_2$ is a constant. If $f_1$ and $f_2$ are both irreducible, we have a resolution of $f$ of the form demanded. If not, resolve such of these polynomials $f_1$ and $f_2$ as are reducible into the product of two factors neither of which is a constant. We thus get $f$ expressed as the product of three or four factors. This is the resolution of $f$ demanded if all the factors are irreducible. If not, resolve such as are reducible into the product of two factors, etc. This process must stop after a finite number of steps, for each time we factor

a polynomial into two factors, the degrees of the factors are lower than the degree of the original polynomial. We shall thus ultimately resolve $f$ by this process into the product of irreducible factors, no one of which is a constant.

Suppose now that $f$ can be resolved in two ways into the product of irreducible factors none of which are constants,

$$f(x, y) \equiv f_1(x, y) f_2(x, y) \cdots f_k(x, y)$$
$$\equiv \phi_1(x, y) \phi_2(x, y) \cdots \phi_l(x, y).$$

Since $\phi_1$ is a factor of $f$, it must, by the Corollary of Theorem 1, be a factor of one of the polynomials $f_1, f_2, \cdots f_k$. Suppose the $f$'s so arranged that it is a factor of $f_1$. Then, since $f_1$ is irreducible, $f_1$ and $\phi_1$ can differ only by a constant factor, and since $\phi_1 \not\equiv 0$, we may cancel it from the identity above, getting

$$c_1 f_2 f_3 \cdots f_k \equiv \phi_2 \phi_3 \cdots \phi_l.$$

In the same way we see from this identity that $f_2$ and one of the $\phi$'s, say $\phi_2$, differ only by a constant factor. Cancelling $\phi_2$, we get

$$c_1 c_2 f_3 \cdots f_k \equiv \phi_3 \cdots \phi_l.$$

Proceeding in this way, we should use up the $\phi$'s before the $f$'s if $l < k$, the $f$'s before the $\phi$'s if $l > k$. Neither of these cases is possible, for we should then have ultimately a constant on one side of the identity, and a polynomial different from a constant on the other. Thus we must have $k = l$. Moreover we see that the $f$'s can be arranged in such an order that each $f$ is proportional to the corresponding $\phi$, and this is what we mean (cf. Definition 7, § 60) by saying that the two methods of factoring are not essentially different.

Thus our theorem is proved.

THEOREM 3. *If two polynomials $f$ and $\phi$ in $(x, y)$ are relatively prime, there are only a finite number of pairs of values of $(x, y)$ for which $f$ and $\phi$ both vanish.**

For if $f$ and $\phi$ both vanished at the points

$$(x_1, y_1), (x_2, y_2), \cdots, \tag{3}$$

and if these points were infinite in number, there would be among them either an infinite number of distinct $x$'s or an infinite number of distinct $y$'s. By a suitable choice of notation we may suppose that there are an infinite number of distinct $y$'s. Then it is clear that $f$ and $\phi$ must be of at least the first degree in $x$, since a polynomial in $y$ alone which does not vanish identically cannot vanish for an infinite number of values of $y$. We may then apply to $f$ and $\phi$ the algorithm of the greatest common divisor as in § 74, thus getting (cf. (4), § 74) an identity of the form

$$F(x, y) f(x, y) + \Phi(x, y) \phi(x, y) \equiv R_{\rho+1}(y) \not\equiv 0. \tag{4}$$

Since the first member of (4) vanishes at all the points (3), $R_{\rho+1}(y)$ would vanish for an infinite number of distinct values of $y$, and this is impossible.

An important corollary of the theorem just proved is that if $f$ and $\phi$ are two irreducible polynomials in $(x, y)$, and if the equations $f = 0$ and $\phi = 0$ have the same locus, then $f$ and $\phi$ differ merely by a constant factor. This would, however, no longer be necessarily true if $f$ and $\phi$ were not irreducible, as the example,

$$f \equiv xy^2, \quad \phi \equiv x^2 y,$$

shows; for the two curves $f = 0$ and $\phi = 0$ are here identical, since the curve in each case consists of the two coördinate axes, and yet $f$ and $\phi$ are not proportional. By means of the following convention, however, the statement made above becomes true in all cases:

Let $f$ be resolved into its irreducible factors,

$$f \equiv f_1^{a_1} f_2^{a_2} \cdots f_k^{a_k},$$

where $f_1, \cdots f_k$ are irreducible polynomials in $(x, y)$, no two of which are proportional to each other. The curve $f = 0$ then consists of the $k$ pieces,

$$f_1 = 0, f_2 = 0, \cdots f_k = 0.$$

To each of these pieces we attach the corresponding positive integer $a_i$ which we call the *multiplicity* of this piece; and we then regard two curves given by algebraic equations as identical only when they consist of the same irreducible pieces, and each of these pieces has the same multiplicity in both cases. With this convention we may say:

COROLLARY. *If $f$ and $\phi$ are polynomials in $(x, y)$ neither of which is identically zero, a necessary and sufficient condition that the two curves $f = 0$, $\phi = 0$ be identical is that the polynomials $f$ and $\phi$ differ only by a constant factor.*

* Stated geometrically, this theorem tells us that two algebraic plane curves $f(x, y) = 0$, $\phi(x, y) = 0$ can intersect in an infinite number of points only when they have an entire algebraic curve in common.

### EXERCISES

1. Let $f(x)$, $\phi(x)$, $\psi(x)$ be polynomials in $x$ whose coefficients lie in a certain domain of rationality. Then if $\psi$ is irreducible in this domain and is a factor of the product $f\phi$, prove that $\psi$ is a factor of $f$ or of $\phi$.

2. Let $f(x)$ be a polynomial in $x$, which is not identically zero, and whose coefficients lie in a certain domain of rationality. Prove that $f$ can be resolved into a product of polynomials whose coefficients lie in this domain, which are irreducible in this domain, and no one of which is a constant, in one and essentially in only one way.

3. Extend the results of this section to polynomials in two variables whose coefficients lie in a certain domain of rationality.

**76. Factors of Polynomials in Three or More Variables.** The results so far obtained in this chapter may be extended to polynomials in three variables without, in the main, essentially modifying the methods already used. We proceed therefore to state the theorems in the order in which they should be proved, leaving the proofs of most of them to the reader. The extension to the case of $n$ variables then presents no difficulty, and is left entirely to the reader (cf. Exercise 1).

Let $f(x, y, z)$ be any polynomial in three variables, and suppose it arranged according to powers of $x$,

$$f(x, y, z) \equiv a_0(y, z)x^n + a_1(y, z)x^{n-1} + \cdots + a_n(y, z),$$

the $a$'s being polynomials in $(y, z)$.

Corresponding to Theorems 1, 2 of § 73 we have

THEOREM 1. *A necessary and sufficient condition that a polynomial in $(y, z)$ be a factor of $f$ is that it be a factor of all the $a$'s.*

THEOREM 2. *If $f(x, y, z)$ and $\phi(x, y, z)$ are any two polynomials in $(x, y, z)$ and $\psi(y, z)$ is an irreducible polynomial in $(y, z)$ only which is a factor of the product $f\phi$, then $\psi$ is a factor of $f$ or of $\phi$.*

COROLLARY. *Let $f(x, y, z)$ and $\phi(x, y, z)$ be polynomials in $(x, y, z)$, and let $\psi(y, z)$ be a polynomial in $(y, z)$ alone. If $\psi$ is a factor of the product of $f\phi$, but is relatively prime to $\phi$, then it is a factor of $f$.*

To find the greatest common divisor of two polynomials in three variables we proceed exactly as in the case of two variables, getting



a set of identities similar to (1), § 74, the $P$'s and $R_{\rho+1}$ being now functions of $(y, z)$, while the other $R$'s and the $Q$'s are functions of $(x, y, z)$. Corresponding to Theorems 1, 2 of § 74 we now have

THEOREM 3. *A necessary and sufficient condition that $f(x, y, z)$, and $\phi(x, y, z)$ have a common factor which involves $x$ is that $R_{\rho+1}(y, z) \equiv 0$.*

THEOREM 4. *If $R_{\rho+1}(y, z) \equiv 0$, the greatest common divisor of $f(x, y, z)$ and $\phi(x, y, z)$ which contains no factor in $(y, z)$ alone is the polynomial $G(x, y, z)$ obtained by striking out from $R_\rho(x, y, z)$ all factors in $(y, z)$ alone.*

From the algorithm of the greatest common divisor for the two polynomials $f(x, y, z)$, $\phi(x, y, z)$ we also deduce the identity

$$(1) \qquad R_{\rho+1}(y, z) \equiv F(x, y, z)f(x, y, z) + \Phi(x, y, z)\phi(x, y, z),$$

similar to (4), § 74.

Corresponding to Theorems 1, 2 of § 75 we have

THEOREM 5. *If $f(x, y, z)$ and $\phi(x, y, z)$ are any two polynomials and $\psi(x, y, z)$ is an irreducible polynomial which is a factor of the product $f\phi$, then $\psi$ is a factor of $f$ or of $\phi$.*

COROLLARY. *If the product of any number of polynomials*

$$f_1(x, y, z)f_2(x, y, z) \cdots f_k(x, y, z),$$

*is divisible by an irreducible polynomial $\psi(x, y, z)$, then $\psi$ is a factor of at least one of the $f$'s.*

THEOREM 6. *A polynomial in three variables which is not identically zero can be resolved into the product of irreducible factors no one of which is a constant in one, and essentially in only one, way.*

When we come to Theorem 3, § 75, however, we find that it does not admit of immediate extension to the case of three variables; for $R_{\rho+1}(y)$, which came into the proof of that theorem, becomes now $R_{\rho+1}(y, z)$, and we can no longer say that this does not vanish at an infinite number of points $(y, z)$. Not only is the proof thus seen to fail, but the obvious extension of the theorem itself is seen to be false when we recall that two surfaces intersect, in general, in a curve.

This theorem may, however, be replaced by the following one:

THEOREM 7. *If $f(x, y, z)$ and $\phi(x, y, z)$ are any two polynomials in three variables of which $\phi$ is irreducible, and if $f$ vanishes at all points $(x, y, z)$ at which $\phi$ vanishes, then $\phi$ is a factor of $f$.*

In proving this theorem we may, without loss of generality, assume that $\phi$ actually contains one of the variables, say $x$; for if $\phi$ contains none of the variables $x$, $y$, $z$, the theorem is trivial and obviously true.

Suppose $\phi$ were not a factor of $f$. Then, since $\phi$ is irreducible, $f$ and $\phi$ are relatively prime. Hence, in the identity (1) above, $R_{\rho+1}(y, z) \not\equiv 0$. Let us write

$$(2) \qquad \phi(x, y, z) \equiv b_0(y, z)x^m + b_1(y, z)x^{m-1} + \cdots + b_m(y, z) \qquad (m \geq 1),$$

where, without loss of generality, we may assume $b_0(y, z) \not\equiv 0$. Then

$$(3) \qquad R_{\rho+1}(y, z)b_0(y, z) \not\equiv 0.$$

Accordingly we can find a point $(y_1, z_1)$ such that

$$(4) \qquad R_{\rho+1}(y_1, z_1) \neq 0, \qquad b_0(y_1, z_1) \neq 0.$$

Consequently $\phi(x, y_1, z_1)$ is a polynomial in $x$ alone which is of at least the first degree, and which therefore (Theorem 1, § 6) vanishes for some value $x_1$ of $x$. That is

$$\phi(x_1, y_1, z_1) = 0.$$

Accordingly, by hypothesis,

$$f(x_1, y_1, z_1) = 0.$$

Referring now to the identity (1), we see that

$$R_{\rho+1}(y_1, z_1) = 0.$$

This, however, is in contradiction with (4). Thus our theorem is proved.

If to each part of a reducible algebraic surface we attach a *multiplicity* in precisely the same way as was explained in the last section for plane curves, we infer at once the

COROLLARY. *If $f$ and $\phi$ are polynomials in $(x, y, z)$ neither of which is identically zero, a necessary and sufficient condition that the two surfaces*

$$f = 0, \ \phi = 0$$

*be identical is that the polynomials $f$ and $\phi$ differ only by a constant factor.*

Theorem 7 admits also the following generalization:

THEOREM 8. *If $f(x, y, z)$ and $\phi(x, y, z)$ are any two polynomials in three variables which both vanish at the point $(x_0, y_0, z_0)$ and of which $\phi$ is irreducible, and if in the neighborhood $N$ of $(x_0, y_0, z_0)$ $f$ vanishes at all points at which $\phi$ vanishes, then $\phi$ is a factor of $f$.*



We assume, as before, that $\phi$ contains $x$ and can therefore be written in the form (2). Let us first consider the case in which $b_0(y_0, z_0) \neq 0$. Here the proof is very similar to the proof of Theorem 7.

We obtain relation (3) precisely as above, and from it we infer that a point $(y_1, z_1)$ *in as small a neighborhood $M$ of $(y_0, z_0)$ as we please* can be found at which the relations (4) are true.

Now consider the equation

$$(5) \qquad \phi(x, y_1, z_1) = 0.$$

By writing $\phi$ in the form (2), we see that by taking the neighborhood $M$ of $(y_0, z_0)$ sufficiently small, we can make the coefficients of (5) differ from the coefficients of

$$(6) \qquad \phi(x, y_0, z_0) = 0$$

by as little as we please (cf. Theorem 3, § 5). Now $x_0$ is by hypothesis a root of equation (6). Consequently by taking $M$ sufficiently small, we can cause (5) to have at least one root $x_1$ which differs from $x_0$ by as little as we please (cf. Theorem 4, § 6). Thus we see that a point $(x_1, y_1, z_1)$ in the given neighborhood $N$ of $(x_0, y_0, z_0)$ can be found at which

$$\phi(x_1, y_1, z_1) = 0.$$

Accordingly, by hypothesis,

$$f(x_1, y_1, z_1) = 0.$$

From the identity (1) we have then

$$R_{\rho+1}(y_1, z_1) = 0,$$

which is in contradiction with (4). Thus our theorem is proved on the supposition that $b_0(y_0, z_0) \neq 0$.*

* The proof just given will, in fact, apply to the case in which not all the $b$'s in (2) vanish at the point $(y_0, z_0)$, if we use the extension of Theorem 4, § 6, which is there mentioned in a footnote. It is only the extreme case in which all the $b$'s vanish at this point which requires the special treatment which we now proceed to give. The reader is advised to consider the geometrical meaning of this extreme case.

In order to treat the case in which $b_0(y_0, z_0) = 0$, let us denote by $k$ the degree of $\phi(x, y, z)$, and let us subject this polynomial to a non-singular linear transformation

$$(7) \qquad \begin{cases} x = \alpha_1 x' + \beta_1 y' + \gamma_1 z' \\ y = \alpha_2 x' + \beta_2 y' + \gamma_2 z' \\ z = \alpha_3 x' + \beta_3 y' + \gamma_3 z' \end{cases}$$

which makes the degree of $\phi$ in $x$ equal to the total degree $k$ of $\phi$ (cf. Theorem 2, § 64).

Suppose that this transformation carries over the point $(x_0, y_0, z_0)$ into the point $(x_0', y_0', z_0')$. Then it is possible, since (7) is non-singular, to take such a small neighborhood $N'$ of $(x_0', y_0', z_0')$ that all points in this neighborhood correspond to points in the given neighborhood $N$ of $(x_0, y_0, z_0)$.

Moreover, by means of (7), $\phi$ has gone over into

$$(8) \qquad \phi'(x', y', z') \equiv b_0' x'^k + b_1'(y', z') x'^{k-1} + \cdots + b_k'(y', z'),$$

where $b_0'$ is a constant different from zero. Let us denote by $f'(x', y', z')$ the polynomial into which $f$ is transformed. Then it is clear that, since, in the neighborhood $N$, $f$ vanishes whenever $\phi$ does, in the neighborhood $N'$ (which corresponds to a *part* of $N$), $f'$ vanishes whenever $\phi'$ does. Accordingly we can apply the part of the theorem already proved to the two polynomials $f'$ and $\phi'$, since the first coefficient of $\phi'$ in the form (8), being a constant different from zero, does not vanish at $(y_0', z_0')$. We infer that $\phi'$ is a factor of $f'$,

$$f'(x', y', z') \equiv \phi'(x', y', z')\, \psi'(x', y', z').$$

If here we replace $x'$, $y'$, $z'$ by their values in terms of $x$, $y$, $z$ from (7), we see that $\phi$ is a factor of $f$; and our theorem is proved.

### EXERCISES

1. State and prove the eight theorems of this section for the case of polynomials in $n$ variables.

2. Extend the result of the exercise at the the end of § 73 to the case of polynomials in $n$ variables.

3. Extend the results of the two preceding exercises to the case in which we consider only polynomials whose coefficients lie in a certain domain of rationality.



4. The resultant of two polynomials in one variable

$$f(x) \equiv a_0 x^n + a_1 x^{n-1} + \cdots + a_n,$$
$$\phi(x) \equiv b_0 x^m + b_1 x^{m-1} + \cdots + b_m,$$

is sometimes defined as the polynomial $R$ in the $a$'s and $b$'s of lowest degree which satisfies an identity of the form

$$Ff + \Phi\phi \equiv R,$$

where $F$ and $\Phi$ are polynomials in $(a_0, \cdots a_n; b_0, \cdots b_m; x)$, and the identity is an identity in all these arguments. Prove that the resultant as thus defined differs only by a constant factor different from zero from the resultant as we defined it in § 68.