If f is homogeneous, this is equivalent to Theorem 1. If f is non-homogeneous, we may write it in the form

$$f(x_1, \cdots x_n) \equiv \phi_k(x_1, \cdots x_n) + \phi_{k-1}(x_1, \cdots x_n) + \cdots + \phi_1(x_1, \cdots x_n) + \phi_0,$$

where each ϕ is a homogeneous polynomial of the degree indicated by its subscript or else is identically zero. We need now merely to apply Theorem 1 to the homogeneous polynomial ϕ_k, which is, of course, not identically zero.

This theorem, and therefore also Theorem 1, which is merely a special case of it, admits the following generalization to the case of a system of functions:

THEOREM 3. *If we have a system of polynomials*

$$f_1(x_1, \cdots x_n),\ f_2(x_1, \cdots x_n), \cdots\cdots f_m(x_1, \cdots x_n),$$

of degrees $k_1, k_2, \cdots k_m$ respectively, there exists a non-singular homogeneous linear transformation which makes these polynomials of degrees $k_1, \cdots k_m$ in each of the variables $x_1', \cdots x_n'$ taken separately.

This theorem may be proved either by the same method used in proving Theorems 1, 2; or by applying Theorem 2 to the product $f_1 f_2 \cdots f_m$.

CHAPTER XV

FACTORS AND COMMON FACTORS OF POLYNOMIALS IN ONE VARIABLE AND OF BINARY FORMS.

65. Fundamental Theorems on the Factoring of Polynomials in One Variable and of Binary Forms. Theorem 2, § 6 may be stated in the following form:

THEOREM 1. *A polynomial of the nth degree in one variable is always reducible when $n > 1$. It can be resolved into the product of n linear factors in one, and essentially in only one, way.*

By means of § 62 we can deduce from this a similar theorem in the case of the binary form

$$a_0 x_1^n + a_1 x_1^{n-1} x_2 + \cdots + a_n x_2^n. \tag{1}$$

Let us first assume that $a_0 \neq 0$. Then the non-homogeneous polynomial

$$a_0 x_1^n + a_1 x_1^{n-1} + \cdots + a_n \tag{2}$$

corresponds to (1), according to the definition of § 62. Factoring (2), we get

$$a_0(x_1 - \alpha_1)(x_1 - \alpha_2) \cdots (x_1 - \alpha_n),$$

or, if we take n constants $\alpha_1'', \alpha_2'', \cdots \alpha_n''$ whose product is a_0,

$$(\alpha_1'' x_1 - \alpha_1')(\alpha_2'' x_1 - \alpha_2') \cdots (\alpha_n'' x_1 - \alpha_n'), \tag{3}$$

where for brevity we have written

$$\alpha_i'' \alpha_i = \alpha_i' \qquad (i = 1, 2, \cdots n).$$

By Theorem 1, § 62, we now infer that the binary form (1) is identically equal to

$$(\alpha_1'' x_1 - \alpha_1' x_2)(\alpha_2'' x_1 - \alpha_2' x_2) \cdots (\alpha_n'' x_1 - \alpha_n' x_2). \tag{4}$$

Moreover, there cannot be any way essentially different from this of factoring (1) into linear factors, for if there were we should, by setting $x_2 = 1$, have a way of factoring (2) into linear factors essentially different from (3). Thus our theorem is proved on the supposition that $a_0 \neq 0$.

Turning now to the case $a_0 = 0$, let us suppose that

$$a_0 = \cdots = a_{k-1} = 0,\ a_k \neq 0,$$

where $k \leq n$. The form (1) then has the form

$$a_k x_1^{n-k} x_2^k + \cdots + a_n x_2^n, \tag{5}$$

which is equal to the product of k factors x_2 and the binary form

$$a_k x_1^{n-k} + \cdots + a_n x_2^{n-k}$$

of degree $n - k$. Since the first coefficient in this form is not zero, it can, as we have just seen, be factored into $n - k$ linear factors. Thus, here also, we see that the binary form can be written in the form (4), the only peculiarity being that in this case k of the constants α'' are zero. We leave it to the reader to show that this factoring can be performed in essentially only one way. This being done, we have the result:

THEOREM 2. *A binary form of the nth degree is always reducible when $n > 1$. It can be resolved into the product of n linear factors in one, and essentially only one, way.*

EXERCISES

1. Prove that every real polynomial in one variable of degree higher than two is reducible in the domain of reals, and can be resolved into irreducible factors in one, and essentially only one, way.

2. Prove the corresponding theorem for real binary forms.

66. The Greatest Common Divisor of Positive Integers.* We will consider in this section the problem of finding the greatest common divisor of two positive integers a and b, which has the closest

* In this section we use the term *divisor* in the arithmetical sense, not in the algebraic sense defined in § 60. An integer b is said to be a divisor of an integer a if an integer c exists such that $a = bc$.

analogy with the algebraic problem of the next section. The solution of this problem, which was given by Euclid, is as follows:

If we divide a by b* and get a quotient q_0 and a remainder r_1, we may write

$$a = q_0 b + r_1,$$

where, if the division is carried out as far as possible, we have $r_1 < b$.

Then divide b by r getting a quotient q_1 and a remainder r_2 which, if the division is carried out as far as possible, is less than r_1. Proceeding in this way, we get the following system of equations, in which, since the remainders $r_1, r_2, \cdots$ are positive integers which continually decrease, we ultimately come to a point where the division leaves no remainder:

$$\text{(1)} \quad \begin{cases} a = q_0 b + r_1 & r_1 < b, \\ b = q_1 r_1 + r_2 & r_2 < r_1, \\ r_1 = q_2 r_2 + r_3 & r_3 < r_2, \\ \cdots\cdots\cdots & \\ \cdots\cdots\cdots & \\ r_{\rho-2} = q_{\rho-1} r_{\rho-1} + r_\rho & r_\rho < r_{\rho-1}, \\ r_{\rho-1} = q_\rho r_\rho & 0 < r_\rho. \end{cases}$$

From the first of these equations we see that every common factor of a and b is a factor of r_1; from the second, that every common factor of b and r_1 is a factor of r_2; etc.; finally, that every common factor of $r_{\rho-2}$ and $r_{\rho-1}$ is a factor of r_ρ. Hence *every common factor of a and b is a factor of r_ρ.*

On the other hand, we see from the last equation (1) that every factor of r_ρ is a factor of $r_{\rho-1}$; from the next to the last equation, that every common factor of r_ρ and $r_{\rho-1}$ is a factor of $r_{\rho-2}$; etc.; finally, that every common factor of r_2 and r_1 is a factor of b, and that every common factor of r_1 and b is a factor of a. Hence *every factor of r_ρ is a common factor of a and b.*

Since the largest factor of r_ρ is r_ρ itself, we have the result:

THEOREM 1. *In Euclid's algorithm* (1), *the greatest common divisor of a and b is r_ρ.*

In particular, a necessary and sufficient condition that a and b be relatively prime is that $r_\rho = 1$.

* This is possible even if $a < b$, the only peculiarity in this case being that the quotient is zero and the remainder equal to a.

We will next deduce from the equations (1) an important formula by means of which r_ρ is expressed in terms of a, b, and the q's.

From the first equation (1) we have

$$r_1 = a - q_0 b.$$

Substituting this value into the second equation, we get for r_2 the value

$$r_2 = -q_1 a + (q_0 q_1 + 1) b.$$

Substituting the values for r_1 and r_2 just found in the third equation, we get

$$r_3 = (q_1 q_2 + 1) a - (q_0 q_1 q_2 + q_2 + q_0) b.$$

Proceeding in this way, we can express each of the r's, and therefore ultimately r_ρ, in terms of a and b. In order to express conveniently the general formula here, we introduce the following notation:

$$(2) \quad \begin{cases} [\,] = 1 \\ [\alpha_1] = \alpha_1, \\ [\alpha_1, \alpha_2] = \alpha_1 \alpha_2 + 1, \\ [\alpha_1, \alpha_2, \alpha_3] = \alpha_1 \alpha_2 \alpha_3 + \alpha_3 + \alpha_1, \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ [\alpha_1, \cdots \alpha_n] = [\alpha_1, \cdots \alpha_{n-1}]\,\alpha_n + [\alpha_1, \cdots \alpha_{n-2}]. \end{cases}$$

It will be seen that the values of r_1, r_2, r_3 found above are included in the formula

$$(3) \quad r_k = (-1)^{k-1} [q_1, q_2, \cdots q_{k-1}]\, a + (-1)^k [q_0, q_1, q_2, \cdots q_{k-1}] b.$$

By the method of mathematical induction this formula will therefore be established for all values of $k \leqq \rho$ if, assuming that it holds when $k \leqq k_1$, we can show that it holds when $k = k_1 + 1$. This follows at once when, in the formula

$$r_{k_1+1} = r_{k_1-1} - q_{k_1} r_{k_1},$$

we substitute for r_{k_1} and r_{k_1-1} their values from (3) and reduce the resulting expression by means of the definitions (2).

We have therefore established the formula

$$(4) \quad r_\rho = Aa + Bb,$$

where $A = (-1)^{\rho-1} [q_1, q_2, \cdots q_{\rho-1}]$, $B = (-1)^\rho [q_0, q_1, \cdots q_{\rho-1}]$.

Since the q's are integers, it is clear that A and B will be integers.

The most important application of the result just obtained is to the case in which a and b are relatively prime. Here $r_\rho = 1$, and we have

$$(5) \quad Aa + Bb = 1.$$

Conversely, if two integers A and B exist which satisfy (5), a and b are relatively prime, as otherwise the left-hand side of (5) would have a factor greater than 1.

THEOREM 2. *A necessary and sufficient condition for a and b to be relatively prime is that there exist two integers A and B such that $Aa + Bb = 1$.*

EXERCISES

1. Prove that $[\alpha_1, \alpha_2, \cdots \alpha_n] = [\alpha_n, \alpha_{n-1}, \cdots \alpha_1]$.

[SUGGESTION. Use the method of mathematical induction.]

2. Prove that the numerical values of the integers A and B found above are respectively less than $\frac{1}{2}b$ and $\frac{1}{2}a$.

[SUGGESTION. Show that $a/b = [q_0, \cdots q_\rho]/[q_1, \cdots q_\rho]$, and that this second fraction is expressed in its lowest terms.]

3. Prove that there can exist only one pair of integers A and B satisfying the relation $Aa + Bb = 1$ and such that A and B are numerically less than $\frac{1}{2}b$ and $\frac{1}{2}a$ respectively.

67. The Greatest Common Divisor of Two Polynomials in One Variable. In place of the integers a and b of the last section, we consider here the two polynomials:

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

By the greatest common divisor of these two polynomials is meant their common factor of greatest degree.* It will turn out in the course of our work that (except in the case in which f and ϕ are both identically zero) this greatest common divisor is completely determinate except for an arbitrary constant factor which may be introduced into it.

* Many English and American text-books use the term *highest* common factor; but as there is not the slightest possibility that the word *greatest*, here, should refer to the *value* of the polynomial, since the polynomial has an infinite number of values for different values of the argument, it seems better to retain the traditional term.

We will assume that neither f nor ϕ is a mere constant, and that the notation has been so introduced that f is of at least as high degree as ϕ; that is, we assume

$$a_0 \neq 0, \quad b_0 \neq 0, \quad n \geqq m > 0.$$

Let us apply Euclid's algorithm to f and ϕ precisely as in § 66 we applied it to a and b. We thus get the system of identities

$$\text{(2)} \qquad \begin{cases} f(x) \equiv Q_0(x)\phi(x) + R_1(x), \\ \phi(x) \equiv Q_1(x)R_1(x) + R_2(x), \\ R_1(x) \equiv Q_2(x)R_2(x) + R_3(x), \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ R_{\rho-1}(x) \equiv Q_\rho(x)R_\rho(x) + R_{\rho+1}. \end{cases}$$

For the sake of uniformity we will write

$$\phi(x) \equiv R_0(x).$$

Then $R_0, R_1, R_2, \cdots$ are polynomials of decreasing degrees, so that after a finite number of steps a remainder is reached which is a constant. This remainder we have indicated by $R_{\rho+1}$.

From this algorithm we infer, as in § 66, that every common factor of f and ϕ is a factor of all the R's, and, on the other hand, that every common factor of two successive R's is a factor of all the preceding R's and therefore of f and ϕ. Accordingly, if f and ϕ have a common factor which is not a constant, this common factor must be a factor of the constant $R_{\rho+1}$, and therefore $R_{\rho+1} = 0$. Conversely, if $R_{\rho+1} = 0$, the polynomial $R_\rho(x)$ is itself a common factor of R_ρ and $R_{\rho+1}$, and therefore of f and ϕ. Hence the two theorems:

THEOREM 1. *A necessary and sufficient condition that two polynomials in one variable f and ϕ, neither of which is a constant, be relatively prime is that in Euclid's algorithm,* (2), $R_{\rho+1} \neq 0$.

THEOREM 2. *If in Euclid's algorithm,* (2), $R_{\rho+1} = 0$, *then $R_\rho(x)$ is the greatest common divisor of f and ϕ.*

By means of this theorem we are in a position to compute the greatest common divisor, not only of two, but of any finite number, of polynomials in one variable. Thus if we want the greatest common divisor of $f(x)$, $\phi(x)$, $\psi(x)$, we should first compute, as above, the greatest common divisor $R_\rho(x)$ of f and ϕ, and then, by the same method, compute the greatest common divisor of $R_\rho(x)$ and $\psi(x)$.

From the identities (2) we can compute the value of each of the remainders in terms of f, ϕ, and the quotients Q. The formulæ here are precisely like those of § 66, and give for $R_{\rho+1}$ the value

$$\text{(3)} \qquad \begin{aligned} R_{\rho+1} \equiv (-1)^\rho [Q_1(x), Q_2(x), \cdots Q_\rho(x)]f(x) \\ + (-1)^{\rho+1} [Q_0(x), Q_1(x), \cdots Q_\rho(x)]\phi(x). \end{aligned}$$

Suppose, now, that f and ϕ are relatively prime. We may then divide (3) by $R_{\rho+1}$ and get

$$\text{(4)} \qquad F(x)f(x) + \Phi(x)\phi(x) \equiv 1,$$

where

$$\text{(5)} \qquad \begin{cases} F(x) \equiv \dfrac{(-1)^\rho}{R_{\rho+1}} [Q_1(x), Q_2(x), \cdots Q_\rho(x)], \\ \Phi(x) \equiv \dfrac{(-1)^{\rho+1}}{R_{\rho+1}} [Q_0(x), Q_1(x), \cdots Q_\rho(x)]. \end{cases}$$

From the definitions (2), § 66, we see that F and Φ are polynomials in x. The existence of two polynomials F and Φ which satisfy (4) is therefore a necessary condition that f and ϕ be relatively prime. It is also a sufficient condition; for from (4) we see that every common factor of f and ϕ must be a factor of 1, that is, must be a constant. Thus we have proved the theorem:

THEOREM 3. *A necessary and sufficient condition that the polynomials $f(x)$ and $\phi(x)$ be relatively prime is that two polynomials $F(x)$ and $\Phi(x)$ exist which satisfy* (4).*

We can make this statement a little more precise by noting the degrees of F and Φ as given by (5). For this purpose let us first notice that if $\alpha_1, \cdots \alpha_n$ are polynomials of degrees $k_1, \cdots k_n$ respectively, $[\alpha_1, \cdots \alpha_n]$ will, by (2), § 66, not be of degree greater than $k_1 + \cdots + k_n$. Now let the degree of $R_i(x)$ be m_i, and, as above, the degrees of f and ϕ, n and m respectively. Then (cf. (2)) the degrees of $Q_0, Q_1, Q_2, \cdots$ will be $n-m, m-m_1, m_1-m_2, \cdots$ respectively. Accordingly, by (5), the degrees of F and Φ are respectively not greater than

$$(m-m_1) + (m_1-m_2) + \cdots + (m_{\rho-1}-m_\rho) = m - m_\rho,$$

and $(n-m) + (m-m_1) + (m_1-m_2) + \cdots + (m_{\rho-1}-m_\rho) = n - m_\rho$.

Hence, since $m_\rho > 0$, F is of degree less than m, and Φ of degree less than n.

* The proof we have given of this theorem applies only when neither f nor ϕ is a constant. The truth of the theorem is at once obvious if f or ϕ is a constant.

Conversely, we will now show that if F_1 is a polynomial of degree less than m, and Φ_1 a polynomial of degree less than n, and if

$$F_1(x)f(x)+\Phi_1(x)\phi(x)\equiv 1, \tag{6}$$

then $$F_1(x)\equiv F(x), \quad \Phi_1(x)\equiv \Phi(x).$$

To prove this, subtract (6) from (4), getting

$$(F-F_1)f\equiv(\Phi_1-\Phi)\phi.$$

If we resolve the two sides of this identity into their linear factors, we see that, since f and ϕ are relatively prime, f must be a factor of $\Phi_1-\Phi$ and ϕ a factor of $F-F_1$. This, however, is possible only if $\Phi_1-\Phi$ and $F-F_1$ vanish identically, as otherwise they would be of lower degree than f and ϕ respectively. We have thus proved the theorem :

THEOREM 4. *If $f(x)$ and $\phi(x)$ are relatively prime, and neither is a constant, there exists one, and only one, pair of polynomials $F(x)$ $\Phi(x)$, whose degrees are respectively less than the degrees of ϕ and f, and which satisfy the identity* (4).

Before proceeding to the general applications of the principles here developed which will be found in the next section, the reader will do well to familiarize himself somewhat with the ideas involved by considering the special case of two polynomials of the second degree:

$$f(x)\equiv a_0x^2+a_1x+a_2 \qquad a_0\neq 0,$$
$$\phi(x)\equiv b_0x^2+b_1x+b_2 \qquad b_0\neq 0.$$

If the condition that these two polynomials be relatively prime be worked out by a direct application of Euclid's algorithm, it will be found necessary to consider separately the cases in which $a_1b_0-a_0b_1$ is or is not zero. By collating these results it will be found that in all cases the desired condition is:

$$(a_2b_0-a_0b_2)^2+(a_1b_0-a_0b_1)(a_1b_2-a_2b_1)\neq 0.$$

This condition may be found more neatly and quickly by obtaining the condition that two polynomials of the form

$$F(x)\equiv p_0x+p_1,$$
$$\Phi(x)\equiv q_0x+q_1$$

exist which satisfy the identity (4).

It is this last method which we shall apply to the general case in the next section.

68. The Resultant of Two Polynomials in One Variable. Let

$$f(x)\equiv a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n \qquad a_0\neq 0,\ n>0,$$
$$\phi(x)\equiv b_0x^m+b_1x^{m-1}+\cdots+b_{m-1}x+b_m \qquad b_0\neq 0,\ m>0.$$

The condition that these polynomials be relatively prime consists as we see from Theorem 4, § 67, in the existence of constants p_0, p_1, $\cdots$ p_{m-1}, q_0, q_1, $\cdots$ q_{n-1} such that

$$(p_0x^{m-1}+p_1x^{m-2}+\cdots+p_{m-1})(a_0x^n+a_1x^{n-1}+\cdots+a_n)$$
$$+(q_0x^{n-1}+q_1x^{n-2}+\cdots+q_{n-1})(b_0x^m+b_1x^{m-1}+\cdots+b_m)\equiv 1.$$

Equating coefficients of like powers of x, we see that the following system of equations is equivalent to the last written identity:

$$\left|\begin{array}{lll}
a_0p_0 & +b_0q_0 & =0,\\
a_1p_0+a_0p_1 & +b_1q_0+b_0q_1 & =0,\\
\cdots\cdots & \cdots\cdots & \cdots\\
a_mp_0+a_{m-1}p_1+\cdots+a_1p_{m-1} & +b_mq_0+b_{m-1}q_1+\cdots+b_0q_m & =0,\\
a_{m+1}p_0+a_mp_1+\cdots+a_2p_{m-1} & +b_mq_1+\cdots\cdots+b_0q_{m+1} & =0,\\
\cdots\cdots & \cdots\cdots & \cdots\\
a_np_0+a_{n-1}p_1+\cdots+a_{n-m+1}p_{m-1} & +b_mq_{n-m}+\cdots\cdots+b_1q_{n-1} & =0,\\
a_np_1+\cdots+a_{n-m+2}p_{m-1} & +b_mq_{n-m+1}+\cdots+b_2q_{n-1} & =0,\\
\cdots\cdots & \cdots\cdots & \cdots\\
a_np_{m-1} & +b_mq_{n-1} & =1
\end{array}\right. \tag{1}$$

In writing these equations we have assumed for the sake of definiteness that $n\geqq m$, though the change would be immaterial if this were not the case. This is a system of $m+n$ linear equations in the $m+n$ unknowns p_0, $\cdots$ p_{m-1}, q_0, $\cdots$ q_{n-1}, whose determinant, after an interchange of rows and columns and a shifting of the rows, is

$$R\binom{a_0,\cdots a_n}{b_0,\cdots b_m}=\begin{vmatrix}
a_0 & \cdots & a_n & 0 & \cdots & 0\\
0 & a_0 & \cdots & a_n & 0 & \cdots & 0\\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\
0 & \cdots & 0 & a_0 & \cdots & a_n\\
0 & \cdots & 0 & b_0 & \cdots & b_m\\
0 & \cdots & 0 & b_0 & \cdots & b_m & 0\\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\
b_0 & \cdots & b_m & 0 & \cdots & 0
\end{vmatrix},$$

a determinant which, it should be noticed, has $m+n$ rows and columns

If $R \neq 0$, the set of equations (1) has one and only one solution, and f and ϕ are relatively prime. If $R = 0$, two cases seem at first sight possible (cf. § 16): either the system of equations has no solution, or it has an infinite number of solutions. This latter alternative cannot, however, really arise, for we have seen in Theorem 4, § 67, that not more than one pair of polynomials F and Φ can exist which satisfy formula (4) of that section and whose degrees do not exceed $m-1$ and $n-1$ respectively. Accordingly, if $R = 0$, the set of equations has *no* solution and f and ϕ have a common factor.

R is called the *resultant* of f and ϕ.*

The term *resultant* has thus been defined only on the supposition that f and ϕ are both of at least the first degree. It is desirable to extend this definition to the case in which one or both of these polynomials is a constant. Except in the extreme case $m = n = 0$, we will continue to use the determinant R as the definition of the resultant. Thus when $m = 0$, $n > 0$ we have

$$R\begin{pmatrix} a_0, \cdots a_n \\ b_0 \end{pmatrix} = (-1)^{\frac{n(n-1)}{2}} b_0^n.$$

If $b_0 \neq 0$ we have $R \neq 0$, and moreover in this case f and ϕ are relatively prime since the constant ϕ has no factors other than constants. If, however, $b_0 = 0$, we have $R = 0$, and every factor of f is a factor of ϕ, since ϕ is now identically zero.

Similarly when $n = 0$, $m > 0$, we have

$$R\begin{pmatrix} a_0 \\ b_0, \cdots b_m \end{pmatrix} = a_0^m,$$

and we see that a necessary and sufficient condition that f and ϕ be relatively prime is that $R \neq 0$.

Finally, when $n = m = 0$, we define the symbol $R\begin{pmatrix} a_0 \\ b_0 \end{pmatrix}$, which we still use to denote the resultant, by the formula

$$R\begin{pmatrix} a_0 \\ b_0 \end{pmatrix} = \begin{cases} 1 & \text{when } a_0 \text{ and } b_0 \text{ are not both zero,} \\ 0 & \text{when } a_0 = b_0 = 0. \end{cases}$$

We may now say with entire generality:

THEOREM. *A necessary and sufficient condition for two polynomials in one variable to be relatively prime is that their resultant do not vanish.*

For another method of approach to the resultant, cf. Exercise 4 at the end of § 76.

* It should be noticed that the resultant of ϕ and f may be the negative of the resultant of f and ϕ. This change of sign is of no consequence for most purposes.

69. The Greatest Common Divisor in Determinant Form.

DEFINITION. *By the ith subresultant R_i of two polynomials in one variable is understood the determinant obtained by striking out the first i and the last i rows and also the first i and the last i columns from the resultant of these polynomials.*

Thus if the polynomials are of degrees 5 and 3 respectively, the resultant R is a determinant of the eighth order, R_1 of the sixth, R_2 of the fourth, and R_3 of the second, as indicated below:

$$R = \begin{vmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ 0 & 0 & 0 & 0 & b_0 & b_1 & b_2 & b_3 \\ 0 & 0 & 0 & b_0 & b_1 & b_2 & b_3 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 & b_3 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & b_3 & 0 & 0 & 0 \\ b_0 & b_1 & b_2 & b_3 & 0 & 0 & 0 & 0 \end{vmatrix}$$

(R_1: the 7-row block; R_2: the 6-row block; R_3: the 4-row block)

We now state the following results, leaving their proof to the reader:

LEMMA. *If $f_1(x)$ and $\phi_1(x)$ are polynomials, and*

$$f(x) \equiv (x-\alpha) f_1(x), \qquad \phi(x) \equiv (x-\alpha)\phi_1(x),$$

the resultant of f_1 and ϕ_1 and their successive subresultants are equal respectively to the successive subresultants of f and ϕ.

THEOREM 1. *The degree of the greatest common divisor of $f(x)$ and $\phi(x)$ is equal to the subscript of the first of the subresultants $R_0 = R$, R_1, R_2, $\cdots$ which does not vanish.*

THEOREM 2. *If i is the degree of the greatest common divisor of two polynomials $f(x)$ and $\phi(x)$, then this greatest common divisor may be obtained from the ith subresultant of f and ϕ by replacing the last*

element in the last row of coefficients of f by $f(x)$, the element just above this by $xf(x)$, the element above this by $x^2f(x)$, etc.; and replacing the last element in the first row of coefficients of ϕ by $\phi(x)$, the element below this by $x\phi(x)$, etc.

If, for instance, the degrees of f and ϕ are 5 and 3 respectively, and $i = 1$, the greatest common divisor is

$$\begin{vmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & xf(x) \\ 0 & a_0 & a_1 & a_2 & a_3 & f(x) \\ 0 & 0 & 0 & b_0 & b_1 & \phi(x) \\ 0 & 0 & b_0 & b_1 & b_2 & x\phi(x) \\ 0 & b_0 & b_1 & b_2 & b_3 & x^2\phi(x) \\ b_0 & b_1 & b_2 & b_3 & 0 & x^3\phi(x) \end{vmatrix}.$$

70. Common Roots of Equations. Elimination. Consider the equations

$$f(x) \equiv a_0x^n + a_1x^{n-1} + \cdots + a_n = 0 \qquad a_0 \neq 0,$$
$$\phi(x) \equiv b_0x^m + b_1x^{m-1} + \cdots + b_m = 0 \qquad b_0 \neq 0,$$

whose roots are $\alpha_1, \alpha_2, \cdots \alpha_n$ and $\beta_1, \beta_2, \cdots \beta_m$, respectively; and suppose $f(x)$ and $\phi(x)$ resolved into their linear factors:

$$f(x) \equiv a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$
$$\phi(x) \equiv b_0(x-\beta_1)(x-\beta_2)\cdots(x-\beta_m).$$

Since, by Theorem 1, § 65, these sets of factors are unique, it is evident that the equations $f(x) = 0$ and $\phi(x) = 0$ will have a common root when, and only when, $f(x)$ and $\phi(x)$ have a common factor, that is, when, and only when, the resultant R of f and ϕ is zero.

To eliminate x between two equations $f(x) = 0$ and $\phi(x) = 0$, is often taken in elementary algebra to mean: to find a relation between the coefficients of f and ϕ which must hold if the two equations are both satisfied; that is, to find a *necessary* condition for the two equations to have a common root. For most purposes, however, when we eliminate we want a relation between the coefficients which not only holds when the two equations have a common root, but such that, conversely, when it holds the equations will have a common root. From this broader point of view, to eliminate x between two equations $f(x) = 0$ and $\phi(x) = 0$ means simply to find a *necessary and sufficient* condition that these equations have a common root. Hence the result of this elimination is $R = 0$. Let us, however, look at this question from a little different point of view.

In the equations

$$(1) \qquad a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0 \qquad a_0 \neq 0,$$
$$(2) \qquad b_0x^3 + b_1x^2 + b_2x + b_3 = 0 \qquad b_0 \neq 0,$$

let us consider the different powers of x as so many distinct unknowns. We have, then, two non-homogeneous, linear equations in the five unknowns x, x^2, x^3, x^4, x^5. Multiplying (1) through by x and then by x^2, and (2) by x, x^2, x^3, x^4, in turn, we have

$$\begin{aligned} a_0x^7 + a_1x^6 + a_2x^5 + a_3x^4 + a_4x^3 + a_5x^2 &= 0, \\ a_0x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_4x^2 + a_5x &= 0, \\ a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 &= 0, \\ b_0x^3 + b_1x^2 + b_2x + b_3 &= 0, \\ b_0x^4 + b_1x^3 + b_2x^2 + b_3x &= 0, \\ b_0x^5 + b_1x^4 + b_2x^3 + b_3x^2 &= 0, \\ b_0x^6 + b_1x^5 + b_2x^4 + b_3x^3 &= 0, \\ b_0x^7 + b_1x^6 + b_2x^5 + b_3x^4 &= 0, \end{aligned}$$

a system of eight non-homogeneous, linear equations in seven unknowns.

If a value of x satisfies both (1) and (2), it will evidently satisfy all the above equations. These equations are therefore consistent, so that by Theorem 1, § 16, we have.

$$\begin{vmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ 0 & 0 & 0 & 0 & b_0 & b_1 & b_2 & b_3 \\ 0 & 0 & 0 & b_0 & b_1 & b_2 & b_3 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 & b_3 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & b_3 & 0 & 0 & 0 \\ b_0 & b_1 & b_2 & b_3 & 0 & 0 & 0 & 0 \end{vmatrix} = 0.$$

Hence the vanishing of this determinant is a *necessary* condition for (1) and (2) to have a common root.

This device is known as *Sylvester's Dialytic Method of Elimination.**

* For the sake of simplicity we have taken the special case where $n = 5$ and $m = 3$. The method, however, is perfectly general.

The above determinant is seen to be exactly the same as the resultant R of (1) and (2), so that Sylvester's method leads to the same condition for two equations to have a common root as that found above, namely $R=0$. It does not prove, however, that this condition is sufficient, but merely that it is necessary. Thus Sylvester's method, while brief, is very imperfect.

The number of roots common to two equations, $f(x)=0$ and $\phi(x)=0$, and also an equation for computing the common roots, may be obtained at once from § 69.

71. The Cases $a_0=0$ and $b_0=0$. It is important for us to note that according to the definitions we have given, the determinant $R\begin{pmatrix} a_0, \cdots a_n \\ b_0, \cdots b_m \end{pmatrix}$ will be the resultant of the two polynomials

$$f(x)\equiv a_0x^n+a_1x^{n-1}+\cdots+a_n,$$
$$\phi(x)\equiv b_0x^m+b_1x^{m-1}+\cdots+b_m,$$

only when f and ϕ are precisely of degrees n and m respectively, that is, only when $a_0\neq 0$, $b_0\neq 0$. Thus, for instance, the resultant of the polynomials

$$f(x)\equiv a_1x^{n-1}+a_2x^{n-2}+\cdots+a_n,$$
$$\phi(x)\equiv b_0x^m+b_1x^{m-1}+\cdots+b_m,$$

is not the $(m+n)$-rowed determinant $R\begin{pmatrix} 0, a_1, \cdots a_n \\ b_0, \cdots b_m \end{pmatrix}$ but, if $a_1\neq 0$, $b_0\neq 0$, the $(m+n-1)$-rowed determinant $R\begin{pmatrix} a_1, \cdots a_n \\ b_0, \cdots b_m \end{pmatrix}$ or, if a_1 or b_0 is zero, a determinant of still lower order.*

Let us indicate by R the $(m+n)$-rowed determinant $R\begin{pmatrix} a_0, \cdots a_n \\ b_0, \cdots b_m \end{pmatrix}$ and by r the resultant of f and ϕ, and consider the case $a_0=0$, $a_1\neq 0$, $b_0\neq 0$. Since every element of the first column of R except the last is zero, we may write

$$R=(-1)^{m+n-1}b_0r.$$

In a similar way we see that if the degree of f is $n-i$, and $b_0\neq 0$, we may write

$$R=\pm b_0^i r,$$

and if the degree of ϕ is $m-i$, and $a_0\neq 0$, we have

$$R=a_0^i r.$$

Accordingly, except when $a_0=b_0=0$, R differs from r only by a non-vanishing factor.

* As an illustration take the two polynomials $f(x)\equiv(\alpha+\beta)x^2+x-\beta$ and $\phi(x)\equiv\alpha x+1$. If $\alpha+\beta\neq 0$ and $\alpha\neq 0$, the resultant here is $(\alpha^2-1)\beta$. But if $\alpha=-\beta\neq 0$, the resultant is $1-\alpha^2$.

THEOREM. *Although* $R\begin{pmatrix} a_0, \cdots a_n \\ b_0, \cdots b_m \end{pmatrix}$ *is the resultant of* f *and* ϕ *only when* $a_0\neq 0$ *and* $b_0\neq 0$ *(or when* $m=0$ *or* $n=0$*), nevertheless its vanishing still forms a necessary and sufficient condition that* f *and* ϕ *have a common factor even when* $a_0=0$ *or* $b_0=0$*, provided merely that both* a_0 *and* b_0 *are not zero.*

That this last restriction can not be removed is at once evident; for, if $a_0=b_0=0$, every element in the first column of the determinant is zero, and hence the determinant vanishes irrespective of whether f and ϕ have a common factor or not.* All that we can say, if we do not wish to make this exception, is, therefore, that in all cases the vanishing of R forms a *necessary* condition that f and ϕ have a common factor.

72. The Resultant of Two Binary Forms. Let us now consider the binary forms

$$f(x_1, x_2)\equiv a_0x_1^n+a_1x_1^{n-1}x_2+\cdots+a_nx_2^n \qquad (n\geqq 1)$$
$$\phi(x_1, x_2)\equiv b_0x_1^m+b_1x_1^{m-1}x_2+\cdots+b_mx_2^m \qquad (m\geqq 1).$$

By the side of these forms we write the polynomials in one variable

$$F(x)\equiv a_0x^n+a_1x^{n-1}+\cdots+a_n,$$
$$\Phi(x)\equiv b_0x^m+b_1x^{m-1}+\cdots+b_m.$$

The determinant $R\begin{pmatrix} a_0, \cdots a_n \\ b_0, \cdots b_m \end{pmatrix}$

will be the resultant of F and Φ only when neither a_0 nor b_0 is zero. We will, however, call it the resultant of the binary forms f and ϕ in all cases.

* By looking at the question from the side of the theory of common roots of two equations (cf. § 70), and by introducing the conception of *infinite roots*, we may avoid even this last exception. An equation

$$a_0x^n+a_1x^{n-1}+\cdots+a_n=0$$

has n roots, distinct or coincident, provided $a_0\neq 0$. If we allow a_0 to approach the value zero, one or more of these roots becomes in absolute value larger and larger, as is seen by the transformation $x'=1/x$. Hence it is natural to say that if $a_0=0$ the equation has an infinite root. If then we consider two equations each of which has an infinite root as having a common root, we may say:

A necessary and sufficient condition that the equations

$$a_0x^n+a_1x^{n-1}+\cdots+a_n=0 \qquad n>0,$$
$$b_0x^m+b_1x^{m-1}+\cdots+b_m=0 \qquad m>0,$$

have a common root is in all cases the vanishing of $R\begin{pmatrix} a_0, \cdots a_n \\ b_0, \cdots b_m \end{pmatrix}$.

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 Φ correspond to the forms f and ϕ according to the definition of § 62. Accordingly, by Theorem 2 of that section a necessary and sufficient condition that f and ϕ 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 ϕ have the common factor x_2, and the resultant of f and ϕ 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

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

Φ corresponds to ϕ_1. Now we know in this case (cf. § 71) that $R \neq 0$ is a necessary and sufficient condition that F and Φ be relatively prime. Accordingly, by Theorem 2, § 62, it is also a necessary and sufficient condition that f and ϕ_1 be relatively prime. But since x_2 is not a factor of f, the two forms f and ϕ will be relatively prime when and only when f and ϕ_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.