

CHAPTER THREE

IRREDUCIBILITY AND FACTORIZATION

§1. BASIC DIVISIBILITY THEORY

The set of polynomials over a field  $\mathbf{F}$  is a ring, whose structure shares with the ring of integers many characteristics. A polynomial is *irreducible* iff it cannot be factored as a product of polynomials of strictly lower degree. Otherwise, the polynomial is *reducible*. Every linear polynomial is irreducible, and, when  $\mathbf{F} = \mathbf{C}$ , these are the only ones. When  $\mathbf{F} = \mathbf{R}$ , then the only other irreducibles are quadratics with negative discriminants. However, when  $\mathbf{F} = \mathbf{Q}$ , there are irreducible polynomials of arbitrary degree.

As for the integers, we have a division algorithm, which in this case takes the form that, if  $f(x)$  and  $g(x)$  are two polynomials, then there is a quotient  $q(x)$  and a remainder  $r(x)$  whose degree is less than that of  $g(x)$  for which

$$f(x) = q(x)g(x) + r(x) .$$

A *greatest common divisor* of two polynomials  $f(x)$  and  $g(x)$  is a polynomial of maximum degree that divides both  $f(x)$  and  $g(x)$ . It is determined up to multiplication by a constant, and every common divisor divides the greatest common divisor. These correspond to similar results for the integers and can be established in the same way. One can determine a greatest common divisor by the Euclidean algorithm, and by going through the equations in the algorithm backward arrive at the result that there are polynomials  $u(x)$  and  $v(x)$  for which

$$\gcd(f(x), g(x)) = u(x)f(x) + v(x)g(x) .$$

Two polynomials are *coprime* if their greatest common divisor is 1. If a polynomial  $p(x)$  divides a product  $f(x)g(x)$  and is coprime with one of the factors, then it must divide the other. In particular, an irreducible polynomial that divides a product of polynomials must divide one of the factors. Each polynomial can be written as the product of irreducibles in a unique way up to order of factors and multiplication by constants.

Thus, it is desirable to have a way of determining when a polynomial is irreducible, and, more generally, how to factor it.

Another result for integers that has an analogue for polynomials is the *Chinese Remainder Theorem*: Suppose that  $f_1, f_2, \dots, f_k$  are pairwise coprime polynomials over a field  $\mathbf{F}$  and  $g_1, g_2, \dots, g_k$  are arbitrary polynomials. Then there exists a polynomial  $h(x)$  for which  $h \equiv g_i \pmod{f_i}$  which is uniquely determined up to a multiple of  $f_1 f_2 \dots f_k$ .

IRREDUCIBLE POLYNOMIALS

*Newton's Polygon.* Suppose that  $f(x) = \sum A_i t^i$  is a polynomial with integer coefficients, and that  $p$  is a prime. If we write  $A_i = a_i p^{\alpha_i}$ , where  $a_i$  is not divisible by  $p$ , then we can define the *Newton polygon* for  $f$  with respect to  $p$  as follows: For each  $i$ , plot the point  $(i, \alpha_i)$  in the cartesian plane. The Newton polygon is an open polygon which forms the lower boundary of the convex hull of these points, so that all of these points lie either on or above the polygon. This polygon consists of a finite number of line segments, whose slopes can be listed in increasing order. It may happen that two segments in the Newton polygon are collinear, in which case a slope may be listed more than once. The *Dumas' theorem* states that, if  $f = gh$  is a factorization of a polynomial as a product of polynomials of lower degree over  $\mathbf{Z}$ , then the set of slopes for the Newton polygon of  $f$  is the union of the sets of slopes for the Newton polygons of  $g$  and  $h$ . Moreover, if we weight each slope according to the differences of the abscissae of the endpoints of the segment, then the

sum of the weights for  $g$  and  $h$  is equal to the weight for  $f$ . Since a proof of this appears in Prasolov, I will illustrate the theorem with an example.

Let

$$g(t) = p^4 + p^2t + t^2 + pt^3 + p^3t^4 + p^3t^5 .$$

The points plotted in the cartesian plane (with those actually on and defining the Newton polygon in boldface) are:

$$(\mathbf{0}, \mathbf{4}), (\mathbf{1}, \mathbf{2}), (\mathbf{2}, \mathbf{0}), (\mathbf{3}, \mathbf{1}), (4, 3), (\mathbf{5}, \mathbf{3})$$

with the list of slopes  $\{-2, -2, 1, 1\}$ . Let

$$h(x) = p + p^2t + p^2t^2 + pt^3 + p^4t^4 .$$

The set of points (with those on the Newton polygon in boldface) are:

$$(\mathbf{0}, \mathbf{1}), (1, 2), (2, 2), (\mathbf{3}, \mathbf{1}), (\mathbf{4}, \mathbf{4})$$

with the list of slope  $\{0, 3\}$ .

The product  $f(x) = g(x)h(x)$  of these polynomials is

$$f(x) = p^5 + p^3(1 + p^3)t + p(1 + p^2 + p^5)t^2 + p^2(2 + p^2 + p^5)t^3 + p^2(1 + 2p + p^2 + p^6)t^4 \\ + p(1 + p^2 + p^3 + p^4 + p^5)t^5 + p^2(1 + p^2 + 2p^3)t^6 + p^4(1 + 2p)t^7 + p^4(1 + p^3)t^8 + p^7t^9 .$$

The corresponding set of points is

$$(\mathbf{0}, \mathbf{5}), (\mathbf{1}, \mathbf{3}), (\mathbf{2}, \mathbf{1}), (3, 2), (4, 2), (\mathbf{5}, \mathbf{1}), (\mathbf{6}, \mathbf{2}), (7, 4), (\mathbf{8}, \mathbf{4}), (\mathbf{9}, \mathbf{7})$$

with slope list  $\{-2, -2, 0, 1, 1, 3\}$ .

To understand why the Dumas result holds, consider a particular edge of the Newton polygon for  $f(t)$ , the pair of edges containing the three collinear points  $(5, 1), (6, 2), (8, 4)$ . These lie on the line  $y - x = -4$  and this is the smallest value of  $y - x$  assumed at any of the points on or above the polygon. Let us call these values of  $y - x$  the *weight* of  $y - x$  at the points in question.

For the points corresponding to  $g(t)$ , this function  $y - x$  is minimized at the points  $(2, 0), (3, 1), (5, 3)$ , and for the points corresponding to  $h(x)$ , it is minimized at  $(3, 1)$ . Consider the points  $(2, 0)$  and  $(3, 1)$  whose abscissae are minimum in the two sets of points. These correspond to terms in  $x^2$  and  $x^3$  in  $g$  and  $h$ , respectively, which in the product contribute to the term in  $f$  in  $x^5$ , corresponding to the point  $(5, 1)$ .

The  $f$ -term in  $x^5$  is the sum of products of five pairs of terms terms in  $g$  and  $h$  corresponding to the pairs of points:

$$[(1, 2), (4, 4)], [(2, 0), (3, 1)], [(3, 1), (2, 2)], [(4, 3), (1, 2)], [(5, 3), (0, 1)] .$$

The weights of  $y - x$  at the products of these five terms are respectively

$$(4 + 2) - (4 + 1) = 1, (1 + 0) - (3 + 2) = -4, (1 + 2) - (3 + 2) = -2, (3 + 2) - (4 + 1) = 0, (3 + 1) - (5 + 0) = -1$$

and we find that the weight at  $(5, 1)$  is the sum of the weights are  $(2, 0)$  and  $(3, 1)$ .

Now look at the points  $(5, 3)$  and  $(3, 1)$  whose abscissae are maximized in the minimizing sets of  $y - x$ . In the product of  $g(x)$  and  $h(x)$ , their terms combine to give a term in  $x^8$  in the expansion of  $f(x)$ , corresponding to the point  $(8, 4)$ . The combined weights of all the point pairs for the pairwise products contributing to this term is at least  $-4$  and is exactly  $-4$  for the pair of points  $[(5, 3), (3, 1)]$ . We find that

$$4 - 8 = (3 + 1) - (5 + 3) = (3 - 5) + (1 - 3) .$$

Note that the weight assigned to the slope  $-1$  for  $f$  is equal to  $8 - 5 = (5 - 2) + (3 - 3) = 3$ .

As a corollary, we have that, for some prime, the Newton polygon consists of precisely one segment, then it must be irreducible. In particular, we have the *Eisenstein irreducibility criterion*: If  $f(x) = a_n x^n + \cdots + a_1 x + a_0$  is a polynomial over  $\mathbf{Z}$  and  $p$  is a prime that does not divide  $a_n$ , but divides all the other coefficients, and  $p^2$  does not divide  $a_0$ , then  $f(x)$  is irreducible over  $\mathbf{Z}$ .

An example of an irreducibility result of a different character is *Perron's criterion*: Suppose that  $f(x) = x^n + \cdots + a_1 x + a_0$  is a polynomial over  $\mathbf{Z}$  for which  $a_0 \neq 0$  and

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0| .$$

Then  $f$  is irreducible.

We use Rouché's theorem to show that  $f$  has precisely one root in the exterior of the closed unit disc  $D$ . This is true of the polynomial  $x^n + a_{n-1}x^{n-1}$  since  $|a_{n-1}| > 1$ . Observe that, when  $|z| = 1$ ,

$$|f(x) - g(x)| \leq |a_{n-2}| + \cdots + |a_0| < |a_1| - 1 \leq |g(x)| .$$

Finally, we have *Hilbert's Irreducibility Theorem*: If  $f(t, x)$  is an irreducible polynomial over  $\mathbf{Q}$ , then there are infinitely many rational values of  $t$  for which the polynomial  $f_t(x) \equiv f(t, x)$  is irreducible over  $\mathbf{Q}$ .

### §3. FACTORIZATION OF POLYNOMIALS OVER THE INTEGERS

One simple way to attempt to get at a factor of a polynomial  $f(x)$  is to determine the greatest common divisor of it and its derivative. If this common divisor is 1, then every irreducible factor of  $f(x)$  appears only to the first degree. If this common divisor has positive degree, then we have a divisor of the polynomial. The quotient with respect to this divisor will be a product of irreducibles, all raised to the exponent 1.

There is a test that can show whether two polynomials have a divisor in common. Suppose that  $f(x)$  is a polynomial of degree  $n$  and that  $g(x)$  is a polynomial of degree  $m$ . Then  $f$  and  $g$  have a nontrivial common divisor  $h$  if and only if there are polynomials  $p$  and  $q$  of degrees not exceeding  $n - 1$  and  $m - 1$  respectively, for which  $f = hp$  and  $g = hq$ . If this happens, then  $fq = gp$ .

On the other hand, suppose that  $fq = gp$  for some polynomials  $p$  and  $q$  for which the degrees of  $p$  and  $q$  do not exceed  $n - 1$  and  $m - 1$  respectively. Then  $f$  and  $g$  cannot be coprime. For otherwise,  $f$ , dividing the product  $gp$ , would have to divide  $p$ , which is impossible.

Finding such a pair  $p, q$  of polynomials entails setting up a set of linear equations for its coefficients in terms of the coefficients of  $f$  and  $g$ . To see how this works, suppose, for example, that

$$\begin{aligned} f(x) &= a_3 x^3 + a_2 x^2 + a_1 x + a_0 , \\ g(x) &= b_2 x^2 + b_1 x + b_0 , \\ p(x) &= u_2 x^2 + u_1 x + u_0 , \\ q(x) &= v_1 x + v_0 . \end{aligned}$$

Comparing the coefficients on either side of the equation  $f(x)q(x) = g(x)p(x)$  leads to the linear system

$$\begin{aligned} a_3 v_1 &= b_2 u_2 \\ a_2 v_1 + a_2 v_0 &= b_1 u_2 + b_2 u_1 \\ a_1 v_1 + a_2 v_0 &= b_0 u_2 + b_1 u_1 + b_0 u_0 \\ a_1 v_0 + a_0 v_1 &= b_0 u_1 + b_1 u_0 \end{aligned}$$

$$a_0v_0 = b_0u_0 ,$$

whose associated matrix of coefficients is

$$\begin{pmatrix} a_3 & 0 & -b_2 & 0 & 0 \\ a_2 & a_3 & -b_1 & -b_2 & 0 \\ a_1 & a_2 & -b_0 & -b_1 & -b_2 \\ a_0 & a_1 & 0 & -b_0 & -b_1 \\ 0 & a_0 & 0 & 0 & -b_0 \end{pmatrix}$$

A pair  $(p, q)$  of polynomials exists if and only if the determinant of the matrix, or equivalently of the matrix

$$\begin{pmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 & 0 \\ 0 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & b_2 & b_1 & b_0 \end{pmatrix}$$

vanishes. This determinant is called the *Sylvester resultant* of the polynomials  $f$  and  $g$ .

If a polynomial over  $\mathbf{Z}$  is reducible, then if we reduce its coefficients modulo a prime  $p$ , with a finitely many exceptions where the prime figures in the factors of the coefficients, it will still factor. Accordingly, the task of factoring a polynomial can be carried out modulo  $p$  for primes  $p$ , and then the architecture of the factorizations examined to suggest possible factorizations over the integers.

A standard algorithm for the modulo  $p$  factorization is due to Berlekamp. We have the following results for a monic polynomial  $f(x)$  of degree  $n$ .

Suppose  $h$  is such that  $h^p - h$  is divisible by  $f$  modulo  $p$ ; then

$$f(x) = \prod_a \{ \gcd (f(x), h(x) - a) : a \in \mathbf{Z}_p \} .$$

To prove this, we note that, modulo  $p$ , the polynomials  $h(x) - a$  constitute a coprime set as  $a$  varies over  $\mathbf{Z}_p$ , so that the polynomial

$$F(x) = \prod \gcd (f(x), h(x) - a)$$

is a product of pairwise coprime polynomials and so a divisor of  $f(x)$ . However, it is given that  $f(x)$  divides

$$h(x)^p - h(x) = \prod_a (h(x) - a) .$$

Suppose that  $h(x) - a = u_a(x)v_a(x)$ , where  $u_a(x)$  is the greatest common divisor of  $f(x)$  and  $h(x) - a$ , and  $f(x)$  and  $v_a(x)$  are coprime. Then  $f(x)$  divides

$$\prod_a u_a(x) \text{prod}_a v_a(x) .$$

Since the second product is coprime with  $f(x)$  and the first product is equal to  $F(x)$ , it follows that  $f(x)$  divides  $F(x)$ . Hence,  $f(x) = F(x)$ .

## References

1. Victor V. Prasolov, *Polynomials* Springer Chapter 2 (pages 47-76)