CHAPTER 1

Polynomials

1.1. Divisibility

In this chapter, we very briefly consider some properties of polynomials which we need in the study of algebraic number fields. Suppose that R is a commutative ring with multiplicative identity 1. We denote by $R[t]$ the collection of all polynomials in the variable t and with coefficients in R. It is well known that $R[t]$ itself is a commutative ring with multiplicative identity 1. This ring is called the ring of polynomials over R.

Suppose that $a(t), b(t) \in R[t]$ and $a(t)$ is not identically zero. Then we say that $a(t)$ divides $b(t)$, denoted by $a(t) \mid b(t)$, if there exists $c(t) \in R[t]$ such that $b(t) = a(t)c(t)$; in other words, we have a factorization $b(t) = a(t)c(t)$. In this case, we say that $a(t)$ is a divisor of $b(t)$.

Recall that divisibility in $\mathbb{Z}$ is governed by the magnitude of the integers. In the case of polynomials, this role is now played by the degree of the polynomials. Suppose that the polynomial $a(t) \in R[t]$ is given by $a(t) = a_n t^n + \ldots + a_0$, where $a_0, \ldots, a_n \in R$ and $a_n \neq 0$. Then we say that $a(t)$ is of degree n, denoted by $n = \deg a(t)$.

Theorem 1.1. *Suppose that $a(t), b(t) \in K[t]$, where K is a field, and $a(t)$ is not identically zero. Then there exist $q(t), r(t) \in K[t]$ such that $b(t) = a(t)q(t) + r(t)$, where either $\deg r(t) < \deg a(t)$ or $r(t) = 0$.*

Proof. We first show the existence of such polynomials $q(t), r(t) \in K[t]$. Consider the set

$$S = \{b(t) - a(t)s(t) : s(t) \in K[t]\}.$$

Suppose first that $0 \in S$. Then there exists $q(t) \in K[t]$ such that $b(t) - a(t)q(t) = 0$. In this case, we have $r(t) = b(t) - a(t)q(t) = 0$. On the other hand, if $0 \notin S$, then the degrees of the polynomials in the non-empty set S forms a non-empty subset of the set of all non-negative integers. It then follows from the Principle of induction that there exists a polynomial $r(t) \in S$ of smallest degree, m say. Let $q(t) \in K[t]$ such that $b(t) - a(t)q(t) = r(t)$. Then $\deg r(t) < \deg a(t)$, for otherwise, writing

$$a(t) = a_n t^n + \ldots + a_0 \quad \text{and} \quad r(t) = r_m t^m + \ldots + r_0,$$

where $a_n \neq 0$, $r_m \neq 0$ and $m \geqslant n$, we have

$$r(t) - (r_m a_n^{-1} t^{m-n})a(t) = b(t) - a(t)\left(q(t) + r_m a_n^{-1} t^{m-n}\right) \in K[t].$$

Clearly $\deg(r(t) - (r_m a_n^{-1} t^{m-n})a(t)) < \deg r(t)$, contradicting the minimality of m.

Next, we show that such polynomials $q(t), r(t) \in K[t]$ are unique. Suppose that

$$b(t) = a(t)q_1(t) + r_1(t) = a(t)q_2(t) + r_2(t).$$

Then

$$r_1(t) - r_2(t) = a(t)(q_2(t) - q_1(t)).$$

If $q_1(t) \neq q_2(t)$, then clearly $\deg(a(t)(q_2(t) - q_1(t))) \geqslant \deg a(t)$, while $\deg(r_1(t) - r_2(t)) < \deg a(t)$, a contradiction. It follows that $q_1(t) = q_2(t)$, and so $r_1(t) = r_2(t)$ also. ○

We next establish the existence of greatest common divisors.

THEOREM 1.2. *Suppose that K is a field, and that $a(t), b(t) \in K[t]$ are not identically zero. Then there exists $g(t) \in K[t]$, unique up to multiplication by non-zero elements of K, such that*

(i) *there exist polynomials $u(t), v(t) \in K[t]$ such that $g(t) = a(t)u(t) + b(t)v(t)$;*
(ii) *$g(t) \mid a(t)$ and $g(t) \mid b(t)$; and*
(iii) *for every polynomial $h(t) \in K[t]$ such that $h(t) \mid a(t)$ and $h(t) \mid b(t)$, we have $h(t) \mid g(t)$.*

PROOF. Consider the set

$$I = \{a(t)x(t) + b(t)y(t) : x(t), y(t) \in K[t]\}.$$

Suppose that $g(t) \in I$ is not identically zero and is of smallest degree. The conclusion (i) follows trivially.

Next, we show that $g(t)$ divides every polynomial in I. Suppose that

$$z(t) = a(t)x(t) + b(t)y(t)$$

is any polynomial in I. By Theorem 1.1, there exist $q(t), r(t) \in K[t]$ such that $z(t) = g(t)q(t) + r(t)$, where either $\deg r(t) < \deg g(t)$ or $r(t) = 0$. Then

$$r(t) = z(t) - g(t)q(t) = a(t)(x(t) - u(t)q(t)) + b(t)(y(t) - v(t)q(t)) \in I.$$

If $r(t) \neq 0$, then the requirement $\deg r(t) < \deg g(t)$ contradicts the minimality of the degree of $g(t)$. Hence $r(t) = 0$, so that $z(t) = g(t)q(t)$, whence $g(t)$ divides $z(t)$.

Taking $x(t) = 1$ and $y(t) = 0$ gives $g(t) \mid a(t)$. Taking $x(t) = 0$ and $y(t) = 1$ gives $g(t) \mid b(t)$. Also, the conclusion (iii) is a simple consequence of (i).

Finally, note that if $g_1(t)$ and $g_2(t)$ both satisfy the requirements, then each must be a divisor of the other, and therefore must be multiples of each other by non-zero elements in K. $\bigcirc$

The polynomial $g(t) \in K[t]$ in Theorem 1.2 is called a greatest common divisor of the polynomials $a(t)$ and $b(t)$, and denoted by $g(t) = (a(t), b(t))$. Two polynomials $a(t), b(t) \in K[t]$ which are not identically zero are said to be relatively prime, or coprime, if $(a(t), b(t)) \in K$.

REMARK. The set I in the proof of Theorem 1.2 forms a non-zero ideal in the polynomial ring $K[t]$. The first part of our proof merely shows that any non-zero ideal I in a polynomial ring $K[t]$, where K is a field, is generated by a non-zero element of I.

1.2. Irreducibility

Suppose that R is a commutative ring with multiplicative identity 1. A polynomial $u(t) \in R[t]$ is said to be a unit in $R[t]$ if $u(t)$ divides the multiplicative identity 1 of R. A factorization $b(t) = a(t)c(t)$ is said to be proper if neither $a(t)$ nor $c(t)$ is a unit in $R[t]$. A non-constant polynomial $b(t) \in R[t]$ is said to be irreducible if $b(t)$ does not have a proper factorization; in other words, if $b(t) = a(t)c(t)$, where $a(t), c(t) \in R[t]$, then at least one of $a(t)$ or $c(t)$ is a unit.

THEOREM 1.3. *Suppose that K is a field, and that $a(t), b(t) \in K[t]$. Suppose further that $p(t) \in K[t]$ is irreducible. If $p(t) \mid a(t)b(t)$, then $p(t) \mid a(t)$ or $p(t) \mid b(t)$.*

PROOF. Suppose that $p(t) \nmid a(t)$. Since $p(t)$ is irreducible, the only divisors of $p(t)$ are non-zero elements of K or polynomials of the form $cp(t)$, where $c \in K$ is non-zero. Clearly $cp(t) \nmid a(t)$ for any non-zero $c \in K$. Hence we must have $(a(t), p(t)) = 1$. It follows from Theorem 1.2 that there exist $u(t), v(t) \in K[t]$ such that

$$1 = a(t)u(t) + p(t)v(t), \quad \text{so that} \quad b(t) = a(t)b(t)u(t) + p(t)b(t)v(t).$$

Clearly $p(t) \mid b(t)$. $\bigcirc$

We next restrict our attention to the special case when the field K consists of complex numbers.

THEOREM 1.4. *Suppose that $K \subseteq \mathbb{C}$ is a field. Then every irreducible polynomial in $K[t]$ has no repeated roots in $\mathbb{C}$.*

The proof depends on the following observation.

THEOREM 1.5. *Suppose that $K \subseteq \mathbb{C}$ is a field, and the polynomial $a(t) \in K[t]$ is not identically zero. Then $a(t)$ is divisible by the square of a polynomial of positive degree in $K[t]$ if and only if $a(t)$ and $a'(t)$ have a common factor of positive degree in $K[t]$.*

PROOF. Suppose first of all that

$$a(t) = b^2(t)c(t),$$

where $b(t), c(t) \in K[t]$ and $\deg b(t) > 0$. Differentiating formally, we obtain

$$a'(t) = 2b(t)b'(t) + b^2(t)c'(t),$$

so that the polynomials $a(t)$ and $a'(t)$ have $b(t)$ as a common factor.

Suppose now that $a(t)$ is not divisible by the square of any polynomial in $K[t]$ of positive degree. Then for any irreducible factor $b(t)$ of $a(t)$, we have $a(t) = b(t)c(t)$, where $b(t)$ and $c(t)$ are coprime. Differentiating formally, we have

$$a'(t) = b'(t)c(t) + b(t)c'(t).$$

Suppose on the contrary that $a(t)$ and $a'(t)$ have $b(t)$ as a common factor. Then we must have $b(t) \mid b'(t)c(t)$, and so it follows from Theorem 1.3 that $b(t) \mid b'(t)$. This is only possible if $\deg b(t) = 0$, so that $b(t)$ is a constant polynomial. ◯

PROOF OF THEOREM 1.4. Suppose that $a(t) \in K[t]$ is irreducible in $K[t]$. Then $a(t)$ is not divisible by the square of any polynomial of positive degree in $K[t]$, and so it follows from Theorem 1.5 that $a(t)$ and $a'(t)$ are coprime. By Theorem 1.2, there exist $u(t), v(t) \in K[t]$ such that

$$a(t)u(t) + a'(t)v(t) = 1.$$

Clearly $a(t), a'(t), u(t), v(t) \in \mathbb{C}[t]$. This implies that $a(t)$ and $a'(t)$ are coprime over $\mathbb{C}[t]$. It now follows from Theorem 1.5 that $a(t)$ is not divisible by the square of any polynomial of positive degree in $\mathbb{C}[t]$, and so cannot have repeated zeros in $\mathbb{C}$. ◯

1.3. Polynomials with Rational Coefficients

In this section, we study factorization and irreducibility properties in the polynomial ring $\mathbb{Q}[t]$. Our first result shows that if a polynomial with rational integer coefficients can be factorized, then it is possible to write the factors as polynomials with rational integer coefficients.

THEOREM 1.6 (Gauss's lemma). *Suppose that $a(t) \in \mathbb{Z}[t]$. Suppose further that $a(t) = b(t)c(t)$, where $b(t), c(t) \in \mathbb{Q}[t]$. Then there exists a non-zero $\lambda \in \mathbb{Q}$ such that $\lambda b(t), \lambda^{-1}c(t) \in \mathbb{Z}[t]$.*

PROOF. The equation $a(t) = b(t)c(t)$ can be written in the form

$$na(t) = b^*(t)c^*(t), \tag{1.1}$$

where $n \in \mathbb{Z}$ is non-zero, and where the polynomials $b^*(t), c^*(t) \in \mathbb{Z}[t]$ are rational multiples of $b(t), c(t) \in \mathbb{Q}[t]$ respectively. Write

$$b^*(t) = b_r t^r + \ldots + b_0 \quad \text{and} \quad c^*(t) = c_s t^s + \ldots + c_0,$$

where $b_0, \ldots, b_r, c_0 \ldots, c_s \in \mathbb{Z}$, with $b_r \neq 0$ and $c_s \neq 0$. Clearly the integer n divides all the coefficients of $b^*(t)c^*(t)$. Let p be a prime factor of n.

We first show that either $p \mid b_i$ for every $i = 0, \ldots, r$ or $p \mid c_j$ for every $j = 0, \ldots, s$. Suppose on the contrary that this is not the case. Then there exists m satisfying $0 \leqslant m \leqslant r$ such that $p \nmid b_m$ and

$$p \mid b_i, \quad i = 0, \ldots, m-1.$$

Similarly, there exists q satisfying $0 \leqslant q \leqslant s$ such that $p \nmid c_q$ and

$$p \mid c_j, \quad j = 0, \ldots, q-1.$$

Then the coefficient of t^{m+q} in $b^*(t)c^*(t)$ is equal to

$$b_0 c_{m+q} + \ldots + b_m c_q + \ldots + b_{m+q} c_0,$$

with the convention that this sum only includes those terms for which the coefficients exist. Clearly every term in this expression apart from $b_m c_q$ is divisible by p. It follows that this coefficient is not divisible by p, a contradiction.

We now remove the prime factor p from the expression (1.1) in a suitable way, and repeat this argument with prime factors of n/p, and so on. ◯

Our next result gives a sufficient condition for irreducibility in $\mathbb{Q}[t]$.

THEOREM 1.7 (Eisenstein's criterion). *Suppose that $a(t) \in \mathbb{Z}[t]$, and $a(t) = a_n t^n + \ldots + a_0$, where $a_0, \ldots, a_n \in \mathbb{Z}$. Suppose further that there exists a prime number p such that*

(i) $p \nmid a_n$;
(ii) $p \mid a_i$ *for every* $i = 0, \ldots, n-1$; *and*
(iii) $p^2 \nmid a_0$.

Then $a(t)$ is irreducible in $\mathbb{Q}[t]$.

PROOF. Suppose on the contrary that $a(t)$ is not irreducuble in $\mathbb{Q}[t]$. Then there exist non-constant polynomials $b(t), c(t) \in \mathbb{Q}[t]$ such that $a(t) = b(t)c(t)$. In view of Gauss's lemma, we can further assume that $b(t), c(t) \in \mathbb{Z}[t]$. Write

$$b(t) = b_r t^r + \ldots + b_0 \quad \text{and} \quad c(t) = c_s t^s + \ldots + c_0,$$

where $b_0, \ldots, b_r, c_0 \ldots, c_s \in \mathbb{Z}$, with $b_r \neq 0$, $c_s \neq 0$, $r + s = n$ and $r, s \geqslant 1$. Note that $a_0 = b_0 c_0$. It follows from (ii) and (iii) that p divides exactly one of b_0 and c_0. Without loss of generality, suppose that $p \mid b_0$ and $p \nmid c_0$. It now follows from (i) that there exists m satisfying $1 \leqslant m \leqslant r$ such that $p \nmid b_m$ and

$$p \mid b_i, \quad i = 1, \ldots, m-1.$$

Then the coefficient of t^m in $a(t) = b(t)c(t)$ is equal to

$$a_m = b_0 c_m + \ldots + b_m c_0,$$

where $m \leqslant r < n$ and with the convention that this sum only includes those terms for which the coefficients exist. Clearly $p \nmid a_m$, contradicting (ii). ◯

1.4. Symmetric Polynomials

In this last section, we consider polynomials of more than one variable. Suppose that R is a commutative ring with multiplicative identity 1. We denote by $R[t_1, \ldots, t_n]$ the collection of all polynomials in the variables $t_1, \ldots, t_n$ and with coefficients in R. As before, $R[t_1, \ldots, t_n]$ itself is a commutative ring with multiplicative identity 1.

A polynomial $a(t_1, \ldots, t_n) \in R[t_1, \ldots, t_n]$ is said to be symmetric if

$$a(t_1, \ldots, t_n) = a(t_{\sigma(1)}, \ldots, t_{\sigma(n)})$$

for all permutations σ on the set $\{1, \ldots, n\}$. In particular, the elementary symmetric polynomials are given by

$$\begin{aligned} s_1(t_1, \ldots, t_n) &= t_1 + t_2 + \ldots + t_n, \\ s_2(t_1, \ldots, t_n) &= t_1 t_2 + t_1 t_3 + \ldots + t_1 t_n + t_2 t_3 + \ldots + t_{n-1} t_n, \\ &\vdots \\ s_n(t_1, \ldots, t_n) &= t_1 \ldots t_n. \end{aligned}$$

EXAMPLE. Consider a polynomial $f(t) \in K[t]$, where $K \subseteq \mathbb{C}$ is a field. Resolving $f(t)$ into linear factors over $\mathbb{C}$, we have

$$f(t) = a(t - \alpha_1) \ldots (t - \alpha_n) = a(t^n - s_1 t^{n-1} + \ldots + (-1)^n s_n),$$

where $s_i = s_i(\alpha_1, \ldots, \alpha_n)$ for every $i = 1, \ldots, n$.

Elementary symmetric polynomials are of particular interest as a consequence of the following important result.

THEOREM 1.8. *Let R be a commutative ring with multiplicative identity* 1. *Then every symmetric polynomial in $R[t_1, \ldots, t_n]$ can be expressed as a polynomial in $R[s_1, \ldots, s_n]$, where $s_i = s_i(t_1, \ldots, t_n)$ for every $i = 1, \ldots, n$.*

PROOF. We first define the following "lexicographic" order on the monomials $t_1^{\beta_1} \dots t_n^{\beta_n}$ by saying that $t_1^{\beta_1} \dots t_n^{\beta_n}$ precedes $t_1^{\gamma_1} \dots t_n^{\gamma_n}$ if the first non-vanishing $\beta_i - \gamma_i$, where $i = 1, \dots, n$, is positive. For every symmetric polynomial $a(t_1, \dots, t_n)$ in $R[t_1, \dots, t_n]$, we order its terms lexicographically. If $ct_1^{\beta_1} \dots t_n^{\beta_n}$ is one of the terms of $a(t_1, \dots, t_n)$, then there are similar monomials with the exponents $\beta_1, \dots, \beta_n$ permuted. It is then not too difficult to see that the leading term in lexicographic order of $a(t_1, \dots, t_n)$ is one of the form $ct_1^{\beta_1} \dots t_n^{\beta_n}$, where $\beta_1 \geqslant \dots \geqslant \beta_n$. On the other hand, the leading term of

$$s_1^{k_1} \dots s_n^{k_n} = (t_1 + \dots + t_n)^{k_1} \dots (t_1 \dots t_n)^{k_n}$$

is

$$t_1^{k_1 + \dots + k_n} t_2^{k_2 + \dots + k_n} \dots t_n^{k_n}.$$

It follows that choosing $k_1 = \beta_1 - \beta_2, \dots, k_{n-1} = \beta_{n-1} - \beta_n$ and $k_n = \beta_n$, we conclude that the leading term of

$$a(t_1, \dots, t_n) - cs_1^{\beta_1 - \beta_2} \dots s_{n-1}^{\beta_{n-1} - \beta_n} s_n^{\beta_n} \tag{1.2}$$

in lexicographic order comes after $ct_1^{\beta_1} \dots t_n^{\beta_n}$. There are only finitely many monomials in lexicographic order in $a(t_1, \dots, t_n)$. Repeating our argument on (1.2) and so on, noting that (1.2) is symmetric, we can clearly reduce $a(t_1, \dots, t_n)$ to a polynomial in $R[s_1, \dots, s_n]$. ◯