1

Introduction

1.1 Notation and preliminaries

In this section we introduce some notation and definitions that will be used in this book.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ will denote the sets of natural numbers, integers, rational numbers, real numbers and complex numbers respectively.

If m and n are elements of $\mathbb{Z}$ and if m is a divisor of n, we write $m|n$ or $n \equiv 0 \pmod{m}$. If m is not a divisor of n, we write $m \nmid n$ or $n \not\equiv 0 \pmod{m}$. If p is a prime number and if e is a natural number or zero such that $p^e | n$, $p^{e+1} \nmid n$, we write $p^e \top n$ and we denote this p^e by n_p or $n(p)$. If π is a subset of the set of prime numbers, we define n_π for n an *element of* $\mathbb{Z}$ by $n_\pi = \prod_{p \in \pi} n_p$ and n_π is called the π-component of n. If $n = n_\pi$ or $n = -n_\pi$, n is called a π-number.

If n is an element of $\mathbb{Z}$ greater than 1, then n can be written as a product of powers of primes:

$$n = \prod_{p \text{ prime}} n_p = \prod_{\substack{p \text{ prime} \\ e_p \geq 1}} p^{e_p}.$$

This is called the prime factorization of n and this prime factorization is unique. If n is an element of $\mathbb{Z}$, $|n|$ will denote its absolute value. If m and n are elements of $\mathbb{Z}$ their greatest common divisor (i.e. the greatest positive integer that divides both m and n) is denoted by (m, n). For any pair of integers m and n, (m, n) exists and is uniquely determined. If $|m| = \prod p^{e_p}$ and $|n| = \prod p^{e'_p}$, then $(m, n) = \prod p^{e''_p}$, where e''_p is the smallest of e_p and e'_p (or equal to, say, e_p when e_p and e'_p are equal). If e'''_p denotes the greatest of e_p and e'_p (or, say, e_p when e_p and e'_p are equal), then $\prod p^{e'''_p}$ is the least common multiple of m and n, i.e. the smallest positive integer that is divided by both m and n.

If A is a set and if a is an element of A, we write $a \in A$ (or $A \ni a$).

If B is a subset of A, we write $B \subseteq A$. The corresponding negations are denoted by $a \notin A$ and $B \nsubseteq A$ respectively. If $B \subseteq A$ but $B \neq A$, we write $B \subsetneq A$. If A_i are sets for all i of some index set I, $\bigcup_{i \in I} A_i$ and $\bigcap_{i \in I} A_i$ denote their union and intersection respectively. The symbol $\varnothing$ stands for the empty set. The set of all x that satisfy condition ... is denoted by $\{x | \ldots\}$. The set consisting of the elements $a, b, \ldots$, is denoted by $\{a, b, \ldots\}$. The direct product of the two sets A and B, written as $A \times B$, is defined by

$$A \times B = \{(a, b) | a \in A, b \in B\}.$$

Similarly, the direct product of sets $A_1, \ldots, A_n$ is defined by

$$A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) | a_i \in A_i, 1 \leq i \leq n\}.$$

The number of elements of A is denoted by $|A|$ and the set of all subsets of A is denoted by 2^A.

'For all (or any) elements a of A' is written in abbreviated form as '$\forall a \in A$' and, 'for some element a of A' is written as '$\exists a \in A$'. In the same way '$\forall a, b \in A$' means 'for all elements $a, b \in A$'. If $a, b, \ldots$ are all different, the notation '$a, b, \ldots (\neq)$' will be used.

If P and Q are statements, '$P \Rightarrow Q$' is used to denote the statement: 'If P is valid, then Q is valid'. The negation of this statement is denoted by '$P \not\Rightarrow Q$'. Instead of '$P \Rightarrow Q$ and $Q \Rightarrow P$' we write '$P \Leftrightarrow Q$'. Further '$P \to Q$' is used for 'P is valid, hence Q is valid'.

If f is a map from A into B we write $f : A \to B$ or $A \xrightarrow{f} B$. (We use the same symbol '$\to$' as a logical symbol, but this cannot cause confusion.) The collection of all maps from A into B is denoted by $M(A, B)$.

If $f : A \to B$ is a map and if a is an element of A, then the image of a under f is denoted by a^f or $f(a)$. For $S \subseteq A$ we define $f(S) (= S^f) = \{f(a) | a \in S\}$ and for $T \subseteq B$ we define $f^{-1}(T) = \{a \in A | f(a) \in T\}$. We call $f(S)$ the image of S under f and we call $f^{-1}(T)$ the inverse image of T under f. If $f(A) = B$, then f is called surjective; if $|f^{-1}(b)| \leq 1 (\forall b \in B)$ then f is called injective. If $f : A \to B$ and $g : B \to C$ are maps then the composition $f \cdot g : A \to C$ is defined by $(f \cdot g)(a) = g(f(a))$ for $a \in A$. The map $f : A \times A \to \{0, 1\}$, defined by

$$f(a, b) = \begin{cases} 0 & \text{if } a \neq b \\ 1 & \text{if } a = b, \end{cases}$$

will be denoted by δ. Instead of $\delta(a, b)$ we will sometimes write $\delta_{a,b}$.

If for $i \in I$, A_i are subsets of A such that

(1) $A = \bigcup_{i \in I} A_i$

(2) $A_i \cap A_j = \varnothing$ if $i \neq j$,

then A is called the direct sum of $\{A_i | i \in I\}$ (as sets). In this case we write $A = \sum_{i \in I} A_i$ (or, if $I = \{1, 2, \ldots\}$, $A = A_1 + A_2 + \ldots$). The summation $A = \sum_{i \in I} A_i$ is also called a decomposition of A (as a set) into disjoint subsets.

A subset E of $A \times A$ is called a relation; instead of $(a, b) \in E$ we usually write $a \underset{E}{\sim} b$ or simply $a \sim b$ and instead of $(a, b) \notin E$, we write $a \not\sim b$. We often denote the relation by $\sim$ rather than by E. An equivalence relation is a relation $\sim$ satisfying:

(i) $a \sim a \quad \forall a \in A$;

(ii) $a \sim b \Rightarrow b \sim a$;

(iii) $a \sim b$ and $b \sim c \Rightarrow a \sim c$.

Putting $C_a = \{x \in A | a \sim x\}$, we have by (ii) and (iii) that if $C_a \neq C_b$, then $C_a \cap C_b = \varnothing$. Therefore, if we pick all the different subsets from the collection $\{C_a | a \in A\}$ and if we denote this collection of subsets by $\{A_i | i \in I\}$, then we have a decomposition of A into disjoint subsets. The A_i are called equivalence classes under $\sim$. If conversely $A = \sum_{i \in I} A_i$ is a decomposition of A into disjoint subsets, then the relation $E = \bigcup_{i \in I} A_i \times A_i \subset A \times A$ is an equivalence relation and the decomposition into disjoint subsets defined by E is just the original decomposition $A = \sum_{i \in I} A_i$. Hence, there is a one-to-one correspondence between decompositions of A into disjoint subsets and equivalence relations on A.

A map $f : B \times A \to A$ is called an operation of B on A. If $(b, a) \in B \times A$, then the element $f(b, a)$ of A is denoted by a^b, ba, $b \cdot a$ and so on and called the image of a by the operation of b. An operation of A on A is called a law of composition on A. If certain laws of composition of A or operations of other sets on A are given, then A is said to carry an algebraic structure or to be an algebraic system.

We assume that the reader is acquainted with the basic concepts and theorems in linear algebra over $\mathbb{C}$. For instance:

(1) Denoting the determinant of a square matrix X by $\det X$,

we have the following result: if A is a (n, m)-matrix, if B is a (m, n)-matrix and if $\det AB \neq 0$ then $n \leq m$.

(2) If $X = (x_{ij})$ is a (n, n)-matrix, then the trace of X is defined by $\operatorname{trace} X = \sum_{i=1}^{n} x_{ii}$. If A and P are both (n, n)-matrices and if P is non-singular (i.e. $\det P \neq 0$), then $\operatorname{trace} A = \operatorname{trace} P^{-1} AP$.

(3) Let A be an (n, n)-matrix. If there exists a non-zero $(n, 1)$-matrix B (i.e. a non-zero column vector) and a complex number α such that $AB = \alpha B$, then α is called an eigenvalue of A, and B is called an eigenvector of A corresponding to the eigenvalue α. An eigenvalue α is a root of the equation of the nth degree with complex coefficients $\det(xE - A) = 0$, where E is the (n, n)-identity matrix, i.e. the matrix which has ones on the diagonal and zeros elsewhere. The nth degree polynomial $\det(xE - A)$ is called the characteristic polynomial of A. The coefficient of x^{n-1} in $\det(xE - A)$ is equal to $-\operatorname{trace} A$ and the constant term is equal to $(-1)^n \det A$.

(4) The collection of all polynomials with rational coefficients $\mathbb{Q}[X]$ has many properties that correspond with properties of $\mathbb{Z}$. The role of prime numbers in $\mathbb{Z}$ is played by the irreducible polynomials of $\mathbb{Q}[X]$ (i.e. polynomials that cannot be written as the product of two non-constant polynomials). Since every polynomial can be written as a product of irreducible polynomials (unique to within order and constant factors), the greatest common divisor and the least common multiple are defined and unique to within constant factors.

(5) The nth degree polynomial with complex coefficients

$$x^n + \lambda_1 x^{n-1} + \ldots + \lambda_n = 0$$

has n complex roots.

(6) ...

We finish this section by stating and proving some properties of cyclotomic polynomials, algebraic numbers etc. that we shall have occasion to use.

For two integers m and n, if $(m, n) = 1$ we say that m is prime to n or that m and n are relatively prime.

The Euler-function φ assigns to every positive integer n the number of positive integers less than n that are relatively prime

to n. If $n = p_1^{e_1} \dots p_r^{e_r}$ is the prime-factorization of n, then

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1}).$$

We want to include a proof of this assertion, because it is fundamental.

For $a \in \mathbb{Z}$ the residue class modulo n is defined by $(a)_n = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$. The collection of all residue classes modulo n is denoted by $\mathbb{Z}_n$. For $a, b \in \mathbb{Z}$, dividing both a and b by n we get $a = t_1 n + s_1$ and $b = t_2 n + s_2 (0 \leq s_1, s_2 < n)$. Then $a \equiv b \pmod{n} \Leftrightarrow s_1 = s_2$. The relation $a \sim b$ defined by $a \equiv b \pmod{n}$ is an equivalence relation and the equivalence class determined by a is just $(a)_n$. The following facts are easy to check:

(i) $\forall a \in \mathbb{Z}$ there is an i such that $0 \leq i < n$ and $(a)_n = (i)_n$.

(ii) $(a)_n \neq (b)_n \Rightarrow (a)_n \cap (b)_n = \varnothing$.

(iii) $\mathbb{Z}_n = \{(0)_n, (1)_n, \dots, (n-1)_n\}$.

If $(a, n) = 1$, then $(a)_n$ is called a prime residue class. Since $(a, n) = (b, n)$ whenever $a \equiv b \pmod{n}$, this definition is independent from the choice of the representant a of $(a)_n$. If we represent the collection of all prime residue classes modulo n by $\mathbb{Z}_n^*$, we have by (iii) $\varphi(n) = |\mathbb{Z}_n^*|$. If $n = n_1 n_2$ and if $(n_1, n_2) = 1$, then:

(iv) $(a)_{n_1} \cap (b)_{n_2} \neq \varnothing, \forall a, b \in \mathbb{Z}$. Hence there exists a $c \in \mathbb{Z}$ such that $(c)_{n_1} = (a)_{n_1}$ and $(c)_{n_2} = (b)_{n_2}$.

(v) $(a)_{n_1} \cap (a)_{n_2} = (a)_n$.

(vi) $(a)_{n_1}$ and $(a)_{n_2}$ are prime residue classes $\Leftrightarrow (a)_n$ is a prime residue class.

Proof

(iv) $(n_1, n_2) = 1 \to tn_1 + sn_2 = 1 (\exists t, s \in \mathbb{Z}) \to (a-b)tn_1 + (a-b)sn_2 = a - b \to a + (b-a)tn_1 = b + (a-b)sn_2 \in (a)_{n_1} \cap (b)_{n_2}$.

(v) $a + tn_1 = a + sn_2 \to tn_1 = sn_2 \to n_1 \mid s \to s = rn_1 \to a + sn_2 = a + rn_1 n_2 \in (a)_n$. Therefore $(a)_{n_1} \cap (a)_{n_2} \subseteq (a)_n$ and $(a)_{n_1} \cap (a)_{n_2} \supseteq (a)_n$ is evident.

(vi) Evident.

By (vi) there is a map $f : \mathbb{Z}_n^* \to \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$ defined by $f((a)_n) = ((a)_{n_1}, (a)_{n_2})$. This map is injective by (v) and surjective by (iv).

Therefore $|\mathbb{Z}_n^*| = |\mathbb{Z}_{n_1}^*| \times |\mathbb{Z}_{n_2}^*|$, i.e. $\varphi(n) = \varphi(n_1)\cdot\varphi(n_2)$ and hence $\varphi(n) = \varphi(p_1^{e_1}) \ldots \varphi(p_r^{e_r})$. The numbers less than p^r that are not relatively prime to p^r are $p, 2p, \ldots, p^{r-1}\cdot p$, hence $\varphi(p^r) = p^r - p^{r-1}$ and we have

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1}). \qquad \blacksquare$$

The complex roots of the equation $X^n - 1 = 0$ are called the nth roots of unity. These roots correspond with the n points of the unit circle in the Gaussian plane that starting from the point corresponding with 1 divide the unit circle in n equal arcs. $\omega = e^{2\pi i/n} = \cos 2\pi/n + i \sin 2\pi/n$ is one of the nth roots of unity and since $\omega, \omega^2, \ldots, \omega^n = 1$ are all different nth roots of unity, we conclude that every nth root of unity is included in this set. An nth root of unity with the property that its nth power is the first power to become 1 is called a primitive nth root of unity. Since $\omega^m = 1 \Leftrightarrow m \equiv 0 \pmod{n}$ we conclude:

$$\omega^{md} = 1 \Leftrightarrow md \equiv 0 \pmod{n} \Leftrightarrow d \equiv 0 \pmod{n/(n,m)}.$$

Hence

$$\omega^m \text{ is a primitive } n\text{th root of unity} \Leftrightarrow (n,m) = 1.$$

Therefore the number of primitive nth roots of unity is equal to $\varphi(n)$. If d is an integer such that $d|n$ and $1 \le d < n$, then $X^d - 1$ is a factor of $X^n - 1$. Hence, the least common multiple $f(X)$ (with leading coefficient 1) of $\{X^d - 1 \,|\, d|n \text{ and } 1 \le d < n\}$ is also a factor of $X^n - 1$; i.e. $X^n - 1 = f(X)\cdot\Phi_n(X)$ for some polynomial $\Phi_n(X)$. The polynomial $\Phi_n(X)$ is called the nth cyclotomic polynomial; it has integer coefficients and its leading coefficient is equal to 1. It is easy to verify that $\Phi_n(X)$ can be written as:

$$\Phi_n(X) = \prod_{\substack{\omega_i \text{ primitive } n\text{th} \\ \text{root of 1}}} (X - \omega_i).$$

A complex number α is called algebraic if it satisfies an equation with rational coefficients:

$$a_0 x^r + \ldots + a_r = 0 \quad (a_0, \ldots, a_r \in \mathbb{Q})$$

If α satisfies an equation with $a_0 = 1, a_1, \ldots, a_r \in \mathbb{Z}$, then α is called an algebraic integer. Of course, rational numbers are algebraic and integers are algebraic integers. We have the following lemma.

Lemma 1.1.1 *If the rational number α is an algebraic integer, then α is an integer.*

Proof Suppose $\alpha \notin \mathbb{Z}$, then α can be written as: $\alpha = m/n$ with $(n, m) = 1$ and $n > 1$. Since α is an algebraic integer by assumption there is a polynomial $f(X) = X^r + a_1 X^{r-1} + \ldots + a_r (a_1, \ldots, a_r \in \mathbb{Z})$ such that $f(\alpha) = 0$. Hence

$$m^r + a_1 m^{r-1} n + \ldots + a_{r-1} m n^{n-1} + a_r n^r = 0,$$

but this contradicts the assumption $(n, m) = 1$. ■

Lemma 1.1.2 *Let $y_1, \ldots, y_N, z \in \mathbb{C}$ such that at least one of the $y_1, \ldots, y_N$ is not equal to zero. If there exist rational numbers $a_{ij} (1 \leq i, j \leq N)$ such that*

$$z y_i = \sum_{j=1}^{N} a_{ij} y_j \quad (1 \leq i \leq N), \tag{1.1.1}$$

then z is algebraic. If all the a_{ij} are integers, then z is an algebraic integer.

Proof The equations (1.1.1) say that z is an eigenvalue of the matrix $A = (a_{ij})$, hence z is a root of the characteristic polynomial

$$f(x) = \det(xE - A) = x^N + \alpha_1 x^{N-1} + \ldots + \alpha_{N-1} x + \alpha_N.$$

Since the coefficients α_i are linear combinations of monomials of the a_{ij} with coefficients ± 1, the proof is finished. ■

Lemma 1.1.3 *The products and sums of algebraic integers are algebraic integers.*

Proof Let α and β be algebraic integers, satisfying the equations $x^n + \lambda_1 x^{n-1} + \ldots + \lambda_n = 0 (\lambda_1, \ldots, \lambda_n \in \mathbb{Z})$ and $x^m + \mu_1 x^{m-1} + \ldots + \mu_m = 0 (\mu_1, \ldots, \mu_m \in \mathbb{Z})$ respectively. Putting $y_{i,j} = \alpha^i \beta^j (0 \leq i \leq n-1,$

$0 \leq j \leq m-1$), we have:

$$(\alpha+\beta)y_{ij} = \begin{cases} y_{i+1,j} + y_{i,j+1} & (i \leq n-2, j \leq m-2) \\ -\sum_{k=1}^{n} \lambda_k y_{n-k,j} + y_{n-1,j+1} & (i = n-1, j \leq m-2) \\ y_{i+1,m-1} - \sum_{k=1}^{m} \mu_k y_{i,m-k} & (i \leq n-2, j = m-1) \\ -\sum_{k=1}^{n} \lambda_k y_{n-k,m-1} - \sum_{k=1}^{m} \mu_k y_{n-1,m-k} & (i = n-1, j = m-1). \end{cases}$$

Therefore $\alpha+\beta$ is an algebraic integer by lemma 1.1.2. The proof for $\alpha \cdot \beta$ is similar. ■

If we expand the product $(X-x_1)\ldots(X-x_n)$, we get

$$(X-x_1)\ldots(X-x_n) = X^n - E_1 X^{n-1} + \ldots + (-1)^n E_n$$

where

$$E_1 = \sum_{i=1}^{n} x_i,\ E_2 = \sum_{i<j} x_i x_j, \ldots, E_r = \sum_{i_1<\ldots<i_r} x_{i_1}\ldots x_{i_r}, \ldots,$$

$$E_n = x_1 x_2 \ldots x_n.$$

$E_1, \ldots, E_n$ are invariant under all permutations of $x_1, \ldots, x_n$ and are called the elementary symmetric polynomials. Generally, a polynomial with complex coefficients $f(x_1, \ldots, x_n)$ that is invariant under all permutations of $x_1, \ldots, x_n$ is called a symmetric polynomial.

Lemma 1.1.4 *For every symmetric polynomial $f(x_1, \ldots, x_n)$ there exists a polynomial $g(y_1, \ldots, y_n)$ such that $f(x_1, \ldots, x_n) = g(E_1, \ldots, E_n)$ and such that the coefficients of $g(y_1, \ldots, y_n)$ are polynomial expressions with integer coefficients of the coefficients of $f(x_1, \ldots, x_n)$.*

Proof The degree of a monomial $\lambda x_1^{r_1}\ldots x_n^{r_n} (\lambda \in \mathbb{C}, \lambda \neq 0)$ is defined to be $\sum_{i=1}^{n} r_i$. Let $f_r(x_1, \ldots, x_n)$ represent the sum of all monomials with degree r occurring in $f(x_1, \ldots, x_r)$. Then f can be represented as $f = \sum_r f_r(x_1, \ldots, x_n)$ and each $f_r(x_1, \ldots, x_n)$ is symmetric. Hence, it suffices to prove the lemma for the case

$f(x_1, \ldots, x_n) = f_r(x_1, \ldots, x_n)$ (in this case f is called a homogeneous polynomial of degree r). Let $M = M(x_1, \ldots, x_n)$ be one of the monomials occurring in $f(x_1, \ldots, x_n)$. Then all monomials obtained from M by a permutation of $(x_1, \ldots, x_n)$ occur in $f(x_1, \ldots, x_n)$ and their sum $f_0(x_1, \ldots, x_n)$ is symmetric. Therefore it suffices to prove the lemma for the case $f(x_1, \ldots, x_n) = f_0(x_1, \ldots, x_n)$. Among the monomials occurring in f there is a monomial M that can be written as

$$M(x_1, \ldots, x_n) = \lambda_0 (x_1 \ldots x_l)^a (x_{l+1} \ldots x_m)^b \ldots (x_{p+1} \ldots x_{p+q})^t$$
$$\lambda_0 \in \mathbb{C}, a > b > \ldots > t.$$

Now we order the triples (r, a, l) in the following way: $(r, a, l) > (r_1, a_1, l_1)$ if (i) $r > r_1$ or (ii) $r = r_1$ and $a > a_1$ or (iii) $r = r_1$ and $a = a_1$ and $l > l_1$ and we proceed by induction. If $r = 1$, then $f(x_1, \ldots, x_n) = \lambda_0 E_1$ which verifies our assertion, so suppose $r > 1$. If all the $x_1, \ldots, x_n$ occur in $M(x_1, \ldots, x_n)$, then $f(x_1, \ldots, x_n) = E_n \cdot f_1(x_1, \ldots, x_n)$ for some f_1 and we can apply the induction hypothesis to f_1. So we may assume $p + q < n$. If $a = 1$ then $f(x_1, \ldots, x_n) = \lambda_0 E_r$, hence we may take $a > 1$. Let

$$M_2(x_1, \ldots, x_n) = \lambda_0 (x_1 \ldots x_l)^{a-1} (x_{l+1} \ldots x_m)^b \ldots (x_{p+1} \ldots x_{p+q})^t$$

and let $f_2(x_1, \ldots, x_n)$ be the sum of all the monomials obtained from M_2 by permutations of $x_1, \ldots, x_n$. Then:

$$E_l \cdot f_2 = (\sum x_1 \ldots x_l) \sum \lambda_0 (x_1 \ldots x_l)^{a-1} (x_{l+1} \ldots x_m)^b \ldots (x_{p+1} \ldots x_{p+q})^t$$
$$= f(x_1 \ldots x_n) + f_3(x_1 \ldots x_n) \quad \text{for some } f_3(x_1 \ldots x_n).$$

Since the theorem is true for f_2 and f_3 by the induction hypothesis, it is also true for f. ■

Lemma 1.1.5 (Gauss) *Let f be a polynomial with integer coefficients. If f is reducible over $\mathbb{Q}$, then f is reducible over $\mathbb{Z}$, i.e. if there exist non-constant polynomials $\tilde{g}$ and $\tilde{h}$ with rational coefficients, such that $f = \tilde{g} \cdot \tilde{h}$, then there exist non-constant polynomials g and h with integer coefficients such that $f = gh$.*

Proof We may assume that the greatest common divisor of the coefficients of f is equal to 1 (polynomials over $\mathbb{Z}$ with this

property are called primitive). Writing the coefficients of $\tilde{g}$ and $\tilde{h}$ as fractions and multiplying both sides of the equality $f = \tilde{g} \cdot \tilde{h}$ by the product of the denominators of the coefficients of $\tilde{g}$ and $\tilde{h}$, we arrive at an equality: $af(x) = bg(x) \cdot h(x)$, where a and b are integers and g and h are primitive polynomials. It suffices to prove that $|a| = |b|$, i.e. that $g(x)h(x)$ is primitive. Assume $g(x)h(x)$ is not primitive, and let p be a prime divisor of the greatest common divisor of the coefficients of $g(x)h(x)$. Putting $g(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0$, there exists an i_0 such that $a_{i_0} \not\equiv 0 \pmod{p}$, $a_i \equiv 0 \pmod{p}$, $\forall i < i_0$. Similarly, putting $h(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_0$, there exists a j_0 such that $b_{j_0} \not\equiv 0 \pmod{p}$, $a_j \equiv 0 \pmod{p}$, $\forall j < j_0$. The coefficient of $x^{i_0 + j_0}$ in $g(x) \cdot h(x)$ is equal to:

$$\sum_{i+j=i_0+j_0} a_i b_j = a_{i_0} b_{j_0} + \sum_{\substack{i < i_0 \text{ or } j < j_0 \\ i+j=i_0+j_0}} a_i b_j \not\equiv 0 \pmod{p}. \quad \text{Contradiction.}$$

■

1.2 Groups

In this section, we introduce some basic definitions and theorems about groups.

1.2.1 Groups, subgroups and cosets

Let G be a set and let f be a law of composition on G. Instead of $f(a, b)$ we will write ab and we will call ab the product of a and b. The set G together with this operation is called a group if the following conditions are satisfied:

(i) if a, b and c are arbitrary elements of G, then $(ab)c = a(bc)$ (associativity);

(ii) there exists an element $e \in G$ such that $ea = ae = a$ for all elements $a \in G$ (existence of identity); and

(iii) for every element $a \in G$ there exists an element $b \in G$ such that $ab = ba = e$ (existence of inverse).

The element e of condition (ii) is uniquely determined. (For suppose $e' \in G$ also satisfies condition (ii), then $e' = ee' = e$.) This uniquely determined element e is called the identity (or unit) of G and is denoted by 1. The element b of condition (iii) is uniquely determined