Chapter 1

Introduction

1. About the course

Finite mathematics is a very broad and heterogeneous area of mathematics, studying finite sets and configurations. The typical general problems it considers are the existence of such configurations with certain properties, their number and characterisation.

Finite mathematics is related to almost all other areas of mathematics, and it also has a wide range of applications. These connections will be illustrated in the course. One underlying theme throughout will be applications of abstract algebra. The definitions and some examples of basic algebraic structures are given in Section 2.

The course will not be solely based on a single book. Therefore, the best study source will be the lecture notes. Some useful texts are:

1. P.J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, Cambridge, 1994.

2. A.P. Street and W.D. Wallis, *Combinatorial Theory: an Introduction*, CBRC, Manitoba, 1977.

3. J.H. van Lint and R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press, Cambridge, 1992.

All these books, as well as all tutorial sheets and solutions, will be available in Mathematics/Physics library on short loan. Also, any other book containing in its title the words such as 'finite mathematics', 'discrete mathematics', 'combinatorics' is likely to contain material relevant to the course.

2. A review of some algebraic structures

In this section we recall definitions and some important examples of groups, fields and vector spaces.

Definition 2.1. A *group* is a non-empty set G with a binary operation $\cdot$, satisfying the following axioms.

(G1) $xy \in G$ for all $x, y \in G$ (closure).

(G2) $x(yz) = (xy)z$ for all $x, y, z \in G$ (associativity).

(G3) There exists an element $e \in G$ (called the *identity* element) such that $xe = ex = x$ for all $x \in G$.

(G4) For each $x \in G$ there exists an element $x^{-1} \in G$ (called the *inverse* of x) such that $xx^{-1} = x^{-1}x = e$.

If, in addition, G satisfies $xy = yx$ for all $x, y \in G$ then G is said to be an *abelian group*, and the operation $\cdot$ is said to be *commutative*.

Example 2.2. For every $n \geq 1$, the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with addition modulo n is an abelian group of order n. The set S_n of all permutations of the set $\{1, 2, \ldots, n\}$ with the composition of mappings is a non-abelian group of order $n!$.

For abelian groups it is customary to use *additive notation*, with $+$ denoting the operation, 0 denoting the identity element, and $-x$ denoting the (additive) inverse of x.

One of the main tasks of group theory is to describe all finite groups, but this does not seem to be attainable.

Definition 2.3. A *field* is a set F with two binary operations $+$ and $\cdot$ and two distinguished elements 0 and 1, such that the following axioms are satisfied.

(F1) F with the operation $+$ is an abelian group, with identity element 0.

(F2) $F\backslash\{0\}$ with the operation $\cdot$ is an abelian group, with identity element 1.

(F3) $x(y+z) = xy + xz$ for all $x, y, z \in F$ (distributivity).

Example 2.4. The number fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are the main examples of fields. Also, if p is a prime then $\mathbb{Z}_p$, with addition and multiplication modulo p, is a field.

Unlike groups, one can describe all finite fields relatively easily.

Theorem 2.5 (The Fundamental Theorem for Finite Fields) *If F is a finite field then its order is a power of a prime. Conversely, if n is a power of a prime, then there exists a unique (up to isomorphism) field of order n.*

For prime power n, we denote the unique finite field of order n by $\mathrm{GF}(n)$. For *prime* n we often write $\mathbb{Z}_n$ instead of $\mathrm{GF}(n)$.

In the following example we show how to construct $\mathrm{GF}(4) = \mathrm{GF}(2^2)$.

Example 2.6. Consider the set $F = \{0, 1, x, x+1\}$ of all constant and linear polynomials over the field $\mathbb{Z}_2$. Let the addition in F be the ordinary addition of polynomials, and let the multiplication be the ordinary multiplication of polynomials, with the additional condition that $x^2 = x + 1$. We can construct tables for these two operations:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Clearly, F with $+$, and $F\backslash\{0\}$ with $\cdot$ are abelian groups. The multiplication of polynomials is distributive over addition, so F is a field.

In fact all finite fields can be constructed in a similar way. To construct a field with p^n elements (p prime) one considers all polynomials of degree less than n over the field $\mathbb{Z}_p$, and uses a rule of the form $f(x) = 0$, where f is an irreducible polynomial of degree n, to simplify polynomials of higher degrees.

Definition 2.7. Let F be a field, let V be an abelian group, and let there be an external multiplication of elements from V by elements from F. Then V is said to be a *vector space* over F if the following axioms are satisfied:

(V1) $(\alpha + \beta)x = \alpha x + \beta x$;

(V2) $\alpha(x + y) = \alpha x + \alpha y$;

(V3) $(\alpha\beta)x = \alpha(\beta x)$;

(V4) $1x = x$;

for all $\alpha, \beta \in F$ and all $x, y \in V$.

We shall assume the familiarity with the elementary theory of vector spaces. In particular we shall consider as known the following concepts: subspaces, linear independence, basis, dimension, isomorphism.

Example 2.8. Let F be a field. Then the set $V = F^d = \{(x_1, \ldots, x_d) : x_i \in F\}$ is a vector space over F with respect to the component-wise addition and scalar multiplication. The dimension of this space is d.

Actually, the above example is generic, as the following theorem shows.

Theorem 2.9. (The Fundamental Theorem for Finite-dimensional Vector Spaces) *If V is a d-dimensional vector space over a field F, then V is isomorphic to F^d.*

Example 2.10. Let V be the (unique) 3-dimensional vector space over GF(2) = $\mathbb{Z}_2$. By the fundamental theorem for finite-dimensional vector spaces, V is isomorphic to $\mathbb{Z}_2^3$. The elements of V are

$$(0,0,0), (1,0,0), (0,1,0), (0,0,1), (1,1,0), (1,0,1), (0,1,1), (1,1,1)$$

and there are $2^3 = 8$ of them. To see that $\mathbb{Z}_2^3$ is a vector space, you should note that $\mathbb{Z}_2$ is a field, that $(V, +)$ forms an abelian group (with identity $(0,0,0)$ and such that the inverse of (a,b,c) is (a,b,c)), and that axioms V1, V2, V3 and V4 all hold.