Chapter 0

Prerequisites

0.1 The number sets

We follow the standard (Bourbaki) notation for the number sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Thus $\mathbb{N}$ is the set of natural numbers $0, 1, 2, \ldots$; $\mathbb{Z}$ is the set of integers $0, \pm 1, \pm 2, \ldots$; $\mathbb{Q}$ is the set of rational numbers n/d, where $n, d \in \mathbb{Z}$ with $d \neq 0$; $\mathbb{R}$ is the set of real numbers, and $\mathbb{C}$ the set of complex numbers $x + iy$, where $x, y \in \mathbb{R}$.

Note that $\mathbb{Z}$ is an *integral domain*, ie a commutative ring with 1 having no zero divisors:

$$xy = 0 \implies x = 0 \text{ or } y = 0.$$

Also $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all *fields*, ie integral domains in which every non-zero element has a multiplicative inverse.

All 5 sets are *totally ordered*, ie given 2 elements x, y of any of these sets we have either $x < y$, $x = y$ or $x > y$. Also the orderings are compatible (in the obvious sense) with addition and multiplication, eg

$$x \geq 0,\ y \geq 0 \implies x + y \geq 0,\ xy \geq 0.$$

0.2 The natural numbers

According to Kronecker, "God gave us the integers, the rest is Man's".
("Gott hat die Zahlen gemacht, alles andere ist Menschenwerk.")

We follow this philosophy in assuming the basic properties of $\mathbb{N}$.

In particular, we assume that $\mathbb{N}$ is *well-ordered*, ie a decreasing sequence of natural numbers

$$a_0 \geq a_1 \geq a_2 \ldots$$

is necessarily stationary: for some n,

$$a_n = a_{n+1} = \cdots .)$$

We also assume that we can "divide with remainder"; that is, given $n, d \in \mathbb{N}$ with $d \neq 0$ we can find $q, r \in \mathbb{N}$ such that

$$n = qd + r,$$

with remainder

$$0 \leq r < d.$$

If we wanted to prove these results, we would have to start from an axiomatic definition of $\mathbb{N}$ such as the Zermelo-Fraenkel, or ZF, axioms. But we don't want to get into that, and assume as 'given' the basic properties of $\mathbb{N}$.

0.3 Divisibility

If $a, b \in \mathbb{Z}$, we say that a *divides* b, written $a \mid b$, or a is a *factor* of b, if

$$b = ac$$

for some $c \in \mathbb{Z}$.

Thus every integer divides 0; but the only integer divisible by 0 is 0 itself.

0.4 Polynomials

If A is a commutative ring (with 1) we denote the ring of polynomials

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

with coefficients $a_i \in A$ by $A[x]$.

We shall be particularly interested in the ring $k[x]$ of polynomials over a field k, since as we shall see, this ring shares many properties with $\mathbb{Z}$.