# Chapter 1
# Polynomials

**Definition 1.1.** A *polynomial* of degree *n* over a field **F** is a function $p:\mathbf{F}\to\mathbf{F}$ of the form $p(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots a_1x+a_0$, where $a_0,a_1,\ldots,a_n\in\mathbf{F}$ and $a_n\neq 0$. $\mathbf{F}[x]$ will denote the set of all polynomials over **F** and $\mathbf{F}_n[x]$ will denote the set of all polynomials over **F** of degree at most *n*.

**Definition 1.2.** An element *t* of **F** is called a *root* of a polynomial p iff it is a solution to the equation p(x)=0, i.e. if p(t)=0.

We add and multiply polynomials as we do functions. It can be easily verified that the product of two polynomials of degrees *n* and *k* is a polynomial of degree *n*+*k* and the sum is a polynomial of degree at most max(*n*,*k*).

**Lemma 1.1.** (Remainder lemma) For every two polynomials f and g from $\mathbf{F}[x]$ there exist unique polynomials q and r in $\mathbf{F}[x]$ such that $f(x)=g(x)q(x)+r(x)$ and $0\leq deg\,r(x)<deg\,g(x)$.

It can be easily verified that the long division algorithm works in every $\mathbf{F}[x]$ and it leads to the result.

**Theorem 1.1** (Division theorem, Bezout theorem) An element *t* is a root of a polynomial *p* iff *p*(x) is divisible by x-t, in other words, there exists a polynomial *g*(x) of degree one less than that of *p* such that *p*(x)=*g*(x)(x-t). □

The introduction of the imaginary unit *i* resulted in such a field **C** that every non-constant polynomial from $\mathbf{C}[x]$ has roots in the field of coefficients **C**. This is not a particularly common situation. For example there are plenty of non-solvable polynomial equations in $\mathbf{R}[x]$ – to mention just a few: $x^2+1=0$, $x^2+x+1=0$ and so on. It is even worse in $\mathbf{Q}[x]$ – some polynomial equations solvable in $\mathbf{R}[x]$ are not solvable here: $x^2-2=0$ is as good an example as any.

**Theorem 1.2** (Main Theorem of Algebra)
For every polynomial $f(x)\in\mathbf{C}[x]$ of degree greater 0 that there exists a complex number z such that f(z)=0.□

**Corollary.** Every polynomial from **C**[x] of degree n>0 has exactly n roots (a root of multiplicity k is counted k times).

**Proof**. Induction on n. A polynomial of degree one looks like $a_1x+a_0$. Its only root is clearly $\frac{-a_0}{a_1}$. Consider a polynomial *f* of degree n+1. By the Main Theorem of Algebra *f* has a root *t*. By the division theorem there exists a polynomial *g* of degree n such that $f(x)=g(x)(x-t)$. By the induction hypothesis *g* has exactly n roots. Those roots, together with *t*, form n+1 roots of *f*.□

For example De Moivre law guarantees that every polynomial equation of the form $x^n-a=0$ with $a\neq 0$ has exactly n different roots.

**Theorem 1.3** If $f\in\mathbf{R}[x]$ then, for every complex number *z*, *z* is a root of *f* if and only if $\bar{z}$ is a root of *f*. In other words, $f(z)=0$ iff $f(\bar{z})=0$.

**Proof**. The theorem follows easily from the fact that conjugation is an isomorphism of **C** with itself: Let $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots a_1x+a_0$, where $a_n,a_{n-1},\ldots,a_1,a_0\in\mathbf{R}$ and $f(z)=0$. Then

$$0=\bar{0}=\overline{a_nz^n+\ldots+a_1z+a_0}=\overline{a_n}\,\overline{z^n}+\ldots+\overline{a_1}\,\overline{z}+\overline{a_0}=a_n(\bar{z})^n+\ldots+a_1\bar{z}+a_0=f(\bar{z}).$$□

**Corollary.** If $f\in\mathbf{R}[x]$ then *f* can be expressed as a product of polynomials from **R**[x] of degree at most 2 each.

**Proof**. According to the last theorem *f* has an even number of non-real roots (i.e. those with nonzero imaginary part) $z_1,\bar{z}_1,\ldots,z_k,\bar{z}_k$ plus some real roots $t_1,\ldots,t_q$. By the division theorem, $f(x)=(x-z_1)(x-\bar{z}_1)\ldots(x-z_k)(x-\bar{z}_k)(x-t_1)\ldots(x-t_q)$. Each product of two terms of the form $(x-z_s)(x-\bar{z}_s)$ can be expressed as $(x-a_s-b_si)(x-a_s+b_si)=x^2-2a_ax+a_s^2+b_s^2$, which is a real polynomial of degree 2. □

**Corollary.** If $f\in\mathbf{R}[x]$ and *f* has an odd degree then *f* has at least one real root.

**Proof**. According to the Main Theorem of Algebra *f* has an odd number of roots. The last theorem implies that *f* has an even number of non-real roots. Hence some of the roots must be real. □