Chapter 10

Polynomials over a Field

Let $K$ be a field. We can define the commutative ring $R = K[x]$ of polynomials with coefficients in $K$ as in chapter 7. Suppose $f = a_n x^n + \ldots$, where $a_n \neq 0$ and $x^n$ is the highest power of $x$ in $f$. Then $n$ is called the degree of $f$, $\deg(f)$, and $a_n x^n$ the leading term. A polynomial of degree 0 called a constant polynomial will be regarded as an element of $K$.

It turns out that $R$ behaves much like $\mathbb{Z}$. In particular, one has a version of the division algorithm:

**Theorem 10.1.** Let $f, g \in R$ with $\deg(g) \neq 0$. Then there exists unique polynomials $q$ and $r$, such that

$$f = qg + r, \deg(r) < g$$

**Proof.** The proof is by induction on $\deg(f)$. If $\deg(f) < \deg(g)$, then take $q = 0$ and $r = f$. Otherwise, let $ax^n$ and $bx^m$ be leading coefficients of $f$ and $g$. Set $q_1 = (ab^{-1})x^{n-m}$ then $f_2 = f - q_1g$ has degree less than $\deg(f)$. Then by induction $f_2 = q_2g + r$. Therefore $f = (q_1 + q_2)g + r$. \qed

Given an element $b \in K$, $f(b) \in K$ is defined by substituting $b$ for $x$ in the expression for $f$. We say $b$ is a root of $f$ if $f(b) = 0$.

**Corollary 10.2.** If $b$ is a root of $f$, then $x - b$ divides $f$.

**Proof.** Then $f = g \cdot (x - b) + r$ where $r$ has degree 0. In other words $r$ is an element of $K$. Then $r = f(b) = 0$. \qed

**Corollary 10.3.** A nonzero polynomial of degree $n$ can have at most $n$ distinct roots.

With the division algorithm in hand, much of the arithmetic of integers can be carried over to polynomials. Given two polynomials, $f$ and $g$, we say that $f$ divides $g$ if $g = fq$. A common divisor of $f$ and $g$ can be defined as before. A polynomial $p$ is called a greatest common divisor (or gcd) if $\deg(p)$ is maximal among all common divisors. It’s unique up to multiplication by a nonzero element of $K$. The analogue of corollary 5.3 holds:
Theorem 10.4. If \( p \) is a greatest common divisor of \( f, g \in K[x] \), then there exists polynomials \( f_1, g_1 \in K[x] \) such that \( ff_1 + gg_1 = p \).

The proof, which is a modification of the previous one, leads to an algorithm which can easily be implemented in Maple (when \( K = \mathbb{Q} \)).

\[
\begin{align*}
    f_1 &:= (f, g) \rightarrow \text{if } (g = 0) \text{ then } 1/f \text{ else } g1(g, \text{rem}(f, g, x)) \text{ fi; } \\
    g1 &:= (f, g) \rightarrow \text{if } (g = 0) \text{ then } 0 \text{ else } \\
    &\quad f1(g, \text{rem}(f, g, x)) - \text{quo}(f, g, x) \times g1(g, \text{rem}(f, g, x)) \text{ fi; }
\end{align*}
\]

In calculus class one learns about partial fractions. There is an implicit assumption that it’s possible. Let’s prove this in special case.

Corollary 10.5. Let \( f, g \) be nonconstant polynomials with 1 as a gcd. Then there exists polynomials \( p, q \) and \( s \) with \( \deg(p) < f \) and \( \deg(g) < g \) such that

\[
\frac{1}{fg} = s + \frac{p}{f} + \frac{q}{g}
\]

Proof. We have \( ff_1 + gg_1 = 1 \). Therefore

\[
\frac{1}{fg} = \frac{g1}{f} + \frac{f1}{g}
\]

Now apply the division to write \( g1 = q1f + r1 \) and \( f1 = q2g + r2 \) and substitute above. \( \square \)

The analogue of a prime number is an irreducible polynomial. Given a polynomial \( f \), and a nonzero element \( a \in K \), we can always factor \( f \) as \( a^{-1}(af) \). We will call this a trivial factorization.

Definition 10.6. A polynomial \( f \in K[x] \) is irreducible if the only factorizations of it are the trivial ones.

The analogue of the fundamental theorem of arithmetic is the following:

Theorem 10.7. Any nonconstant polynomial \( f \in K[x] \) can be factored into a product of irreducible polynomials. Furthermore if \( f = p1 \ldots pn = q1 \ldots qm \) are two such factorizations, them \( n = m \), and after renumbering there \( q \)'s, \( q_i = a_i p_i \) where \( a_i \in K \).

The concept of irreducibility and factorizations depends very much on the field \( K \). For example \( x^2 + 4 \) is irreducible as a polynomial over \( \mathbb{Q} \) but not over \( \mathbb{Q}(i) \) or \( \mathbb{C} \). The Maple procedures \texttt{irreduc(f)} and \texttt{factor(f)} can be used to test irreducibility and do factorizations in \( \mathbb{Q}[x] \). You can also get it to factor in \( \mathbb{Q}(i)[x] \) by typing \texttt{factor(f, I)}.

One of the most important properties of the field of complex numbers is the fundamental theorem of algebra:

Theorem 10.8. Any nonconstant polynomial in \( \mathbb{C}[x] \) has a root.
Corollary 10.9. Any irreducible nonconstant polynomial over \( \mathbb{C} \) is linear, i.e. it has degree 1. Consequently any nonconstant polynomial can be factored into a product of linear polynomials.

Proof. If \( f \in \mathbb{C}[x] \) is a nonconstant linear polynomial then it has a root \( b \). Therefore \( f = (x - b)g \). Since this must be a trivial factorization \( g \) must be a nonzero constant.

10.10 Exercises

1. Find polynomials \( f_1, g_1 \in \mathbb{Q}[x] \) such that \( ff_1 + gg_1 = 1 \) where \( f = x^3 - 2 \) and \( g = x^2 + x + 1 \). Use this to find the partial fraction decomposition of \( \frac{1}{(x^3-2)(x^2+x+1)} \) over \( \mathbb{Q} \).

2. Prove that \( x^n + 1 \) is not irreducible over \( \mathbb{Q}[x] \) if \( n \) is odd.

3. Using Maple, factor \( x^n + 1 \) in \( \mathbb{Q}[x] \) and \( \mathbb{Q}(i)[x] \) for \( n = 2, 4, 6 \ldots 16 \). Can you make a conjecture for when this is irreducible over \( \mathbb{Q}[x] \)?

4. Prove that any nonconstant irreducible polynomial \( f \in \mathbb{R}[x] \) is either linear or quadratic.

   (a) Recall that the conjugate of a complex number is \( \overline{a + bi} = a - bi \). Prove that \( (x - c)(x - \overline{c}) \in \mathbb{R}[x] \) for any complex number \( c \).

   (b) Prove that for \( f \in \mathbb{R}[x] \) and \( c \in \mathbb{C} \), \( \overline{f(c)} = f(\overline{c}) \). In particular, if \( c \) is a complex root of \( f \), then so is \( \overline{c} \).

   (c) Let \( f \in \mathbb{R}[x] \) be a nonconstant irreducible polynomial, factor \( f \) over \( \mathbb{C}[x] \), and then apply the previous results to prove that \( f \) is linear or quadratic.