1 Polynomial Rings

- **Reading:** Gallian Ch. 16

- **Def:** Let $R$ be a commutative ring with unity. The ring of polynomials over $R$ is the ring $R[x]$ consisting of all expressions of the form $a_0 + a_1 x + a_2 x^2 + \cdots$, where each $a_i \in R$ and all but finitely many $a_i$’s are zero. (We usually omit the zero terms, so $1 + 5x + 10x^2 + 3x^3$ is shorthand for $1 + 5x + 10x^2 + 3x^3 + 0x^4 + 0x^5 + \cdots$.)

For two polynomials $p(x) = \sum_i a_i x^i$ and $q(x) = \sum_i b_i x^i$, their sum $(p + q)(x)$ is defined to be the polynomial $\sum_i (a_i + b_i) x^i$ and their product $(pq)(x)$ is the polynomial $\sum_i (\sum_{j=0}^i (a_j b_{i-j})) x^i$, where $a_i + b_i$ and $a_j b_{i-j}$ are defined using the operations of $R$.

- **Def:** The degree $\text{deg}(p)$ of a nonzero polynomial $p(x) = \sum_i a_i x^i$ is the largest $d$ such that $a_d \neq 0$. $a_d$ is called the leading coefficient of $p$. $p$ is called **monic** if $a_d = 1$.

- **Examples:** $p(x) = 3x^3 + 4x + 1$ and $q(x) = 5x + 6$ in $\mathbb{Z}_7[x]$.

- **Remarks:**
  - $R[x]$ is a commutative ring with unity.
  - Two different polynomials can define the same function on $R$, but we still treat them as different elements of $R[x]$. For example $p(x) = x \cdot (x-1) \cdot (x-p+1)$ defines the zero function on $\mathbb{Z}_p$, but is not the zero polynomial (why?).
  - For polynomials of degree at most $n$, their sum can be computed using $n$ operations over $R$ and their product using $O(n^2)$ operations over $R$. (Best known multiplication algorithm uses $O(n \log n)$ operations.) Note similarity with sum and product of integers!

- **Thm 16.1:** $R$ an integral domain $\Rightarrow R[x]$ an integral domain.

  **Proof:**
• We will focus on the case that the coefficient ring \( R \) is a field \( F \). In this case, we will see that the ring \( F[x] \) has many similar properties to the ring \( \mathbb{Z} \). In fact, things tend to be easier to prove and to compute over \( F[x] \) than over \( \mathbb{Z} \).

• **Division with Remainder (Thm 16.2):** \( f(x), g(x) \in F[x], g(x) \) nonzero, then there exist (unique) polynomials \( q(x) \) and \( r(x) \) with \( \deg(r) < \deg(g) \) and \( f(x) = q(x)g(x) + r(x) \). Moreover, if \( f \) and \( g \) have degree at most \( n \), then \( q(x) \) and \( r(x) \) can be computed using \( \mathcal{O}(n^2) \) operations from \( F \). We sometimes write \( f(x) \mod g(x) \) for the remainder \( r(x) \).

**Proof and algorithm (long division of polynomials):** Inputs are \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \), \( g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \). We’ll compute \( q(x) = c_{n-m} x^{n-m} + \cdots + c_1 x + c_0 \).

1. Let \( f_0(x) = f(x) \).
2. For \( i = 0 \) to \( n - m \):
   - (a) Let \( a \) be the coefficient of \( x^{n-i} \) in \( f_i(x) \), and let \( c_{n-m-i} = b_m^{-1} a \).
   - (b) Let \( f_{i+1}(x) = f_i(x) - c_{n-m-i} x^{n-m-i} \cdot g(x) \). (This zeroes out the term of degree \( n - i \).)
3. Output \( q(x) = c_{n-m} x^{n-m} + \cdots + c_1 x + c_0 \).

• **Example:** \( f(x) = 3x^3 + 4x + 1 \) divided by \( g(x) = 5x + 6 \) in \( \mathbb{Z}_7[x] \).

• **Note:** all we used about \( F \) being a field is that \( b_m \) has an inverse. Over general rings \( R \), division is possible if the leading coefficient of \( g(x) \) is a unit (e.g. if \( g \) is monic).

• **Corollary:** Let \( R \) be a commutative ring with unity, \( f(x) \in R[x] \), and \( a \in R \). Then \( f(a) = 0 \) if and only if \( (x - a) \) divides \( f(x) \) in \( R[x] \).

**Proof:**

• **Corollary:** A polynomial of degree \( n \) over an integral domain \( R \) has at most \( n \) zeroes.
  - This simple fact is extremely useful! Ought to be called the “fundamental thm of algebra” (which is unfortunately used for the fact that every polynomial has a root in \( \mathbb{C} \)).
  - Another example of “If an algebraic identity fails, then it fails often.”

**Proof:**
2 Factorization of Polynomials

- Reading: Gallian Ch. 16

- Def: For \( f(x), g(x) \in F[x] \), not both zero, the greatest common divisor of \( f(x) \) and \( g(x) \) is the monic polynomial \( h(x) \) of largest degree such that \( h(x) \) divides both \( f(x) \) and \( g(x) \).

- Euclidean Algorithm for Polynomials: Given two polynomials \( f(x) \) and \( g(x) \) of degree at most \( n \), not both zero, their greatest common divisor \( h(x) \), can be computed using at most \( n + 1 \) divisions of polynomials of degree at most \( n \). Moreover, using \( O(n) \) operations on polynomials of degree at most \( n \), we can also find polynomials \( s(x) \) and \( t(x) \) such that \( h(x) = s(x)f(x) + t(x)g(x) \).

Proof: analogous to integers, using repeated division.

Euclid\((f, g)\):

1. Assume WLOG \( \text{deg}(f) \geq \text{deg}(g) > 0 \).
2. Set \( i = 1 \), \( f_1 = f \), \( f_2 = g \).
3. Repeat until \( f_{i+1} = 0 \):
   - (a) Compute \( f_{i+2} = f_i \mod f_{i+1} \) (i.e. \( f_{i+2} \) is the remainder when \( f_i \) is divided by \( f_{i+1} \)).
   - (b) Increment \( i \).
4. Output \( f_i \) divided by its leading coefficient (to make it monic).

Here the complexity analysis is simpler than for integers: note that the degree of \( f_{i+2} \) is strictly smaller than that of \( f_i \), so \( f_{n+2} \) is of degree zero, and \( f_{n+3} = 0 \). Thus we do at most \( n \) divisions.

The Extended Euclidean Algorithm (finding the polynomials \( s(x) \) and \( t(x) \)) is obtained analogously to the case of the integers.

- Def: Let \( R \) be a commutative ring with unity. An element \( a \in R \) is irreducible if \( a \) is not a zero or a unit, and if \( a = bc \) then either \( b \) or \( c \) is a unit.

- Examples:
  - Units in \( \mathbb{Z} \):
  - Irreducible elements of \( \mathbb{Z} \):
  - Units in \( F[x] \) for a field \( F \):
  - Irreducible polynomials in \( F[x] \) of degree 1:
  - Irreducible polynomials in \( F[x] \) of degree 2:
  - Irreducible polynomials in \( F[x] \) of degree 3:
  - Irreducible polynomials in \( F[x] \) of degree 4+:
  - No simple characterization in general for high degree polynomials. (The conditions in Gallian are necessary or sufficient, but not both.) But there are efficient algorithms for testing irreducibility (see discussion of factorization below).
• **Euclid’s Lemma for Polynomials:** If \( p(x) \) is irreducible and \( p(x)|(f(x)g(x)) \), then \( p(x)|d(x) \) or \( p(x)|g(x) \).

• **Proof:** Similar to proof for integers. If \( p(x) \) does not divide \( f(x) \), then \( \gcd(p(x), g(x)) = 1 \) because the only factors of \( p(x) \) are 1 and \( p(x) \) (up to multiplication by units). So \( 1 = s(x)p(x) + t(x)f(x) \) for some polynomials \( s(x) \) and \( t(x) \). Then \( g(x) = s(x)p(x)g(x) + t(x)f(x)g(x) \) is divisible by \( p(x) \) because both terms on the right-hand side are divisible by \( p(x) \).

• **Thm (Unique Factorization of Polynomials):** Every \( f(x) \in F[x] \) can be written as a product of irreducible polynomials \( f(x) = g_1(x)g_2(x)\cdots g_k(x) \), and this factorization is unique up to the order of the \( g_i \)'s and multiplying them by units (elements of \( F \)).

  - Compare with unique factorization over \( Z \), unique up to multiplication by \( \pm 1 \).

**Proof:** Similar to integers. Existence of factorization by induction on the degree. Uniqueness by Euclid’s Lemma.

• Unlike \( Z \), there are efficient algorithms known for factoring polynomials over fields. The best known deterministic algorithms use \( \text{poly}(n, p, \log q) \) operations over \( F \), where \( p \) is the characteristic of \( F \) and \( q \geq p \) is the size of \( F \). The best known randomized algorithms use \( \text{poly}(n, \log q) \) operations.