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 $a_0 + a_1x + a_2x^2 + \cdots$, 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 $p(x) = \sum_i a_ix^i$ and $q(x) = \sum_i b_ix^i$, 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 $\sum_i (\sum_{j=0}^i (a_jb_{i-j}))x^i$, where $a_i + b_i$ and $a_jb_{j-i}$ are defined using the operations of $R$.

• Def: The degree $\deg(p)$ of a nonzero polynomial $p(x) = \sum_i a_ix^i$ 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 $p(x) = x \cdot (x - 1) \cdots (x - p + 1)$ 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):** If \( f(x), g(x) \in F[x] \), \( g(x) \) 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 \( O(n^2) \) 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:**
• **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.