Math 521A

4.1 – Polynomial Arithmetic and the Division Algorithm

- Although $\mathbb{Z} \cup \{\pi\}$ is not a ring, we can form a ring from $\mathbb{Z}$ and $\{\pi\}$:

$$\mathbb{Z}[\pi] = \{a_0 + a_1\pi + a_2\pi^2 + \cdots + a_n\pi^n \mid a_i \in \mathbb{Z}, n \geq 0\}$$

- More generally, let R be any ring and $x \notin R$. We can form a new ring $R[x]$ where:
  - (i) R is a subring of $R[x]$;
  - (ii) $ax = xa \quad \forall\, a \in R$;
  - (iii) $a_0 + a_1x + \cdots + a_nx^n = b_0 + b_1x + \cdots + b_mx^m$ if and only if $m = n$ and $a_i = b_i$ for $i = 1, \ldots, n$.
- $R[x]$ is described as

$$R[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in R, 0 \leq i \leq n, n \in \mathbb{Z}^{>0}\}$$

  and it is called the the ring of polynomials with coefficients in the ring R.
- An element of $R[x]$ is called a polynomial and is denoted by $a(x)$. If $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ then $a_0, \ldots, a_n$ are called the coefficients of the polynomial $a(x)$ whereas x is called the indeterminate.

Multiplication is done using distributivity: Let
$a(x) = a_0 + a_1x + \cdots + a_nx^n$ and
$b(x) = b_0 + b_1x + \cdots + b_mx^m$.

Then:
$$\begin{aligned} a(x) \cdot b(x) &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 \\ &\quad + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)x^3 + \cdots + a_nb_mx^{m+n}. \end{aligned}$$

Note that for each $k \geq 0$, the coefficient of x^k equals:
$$\sum_{i=0}^{k} a_i b_{k-i}.$$

Definition

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ with $a_n \neq 0_R$. Then a_n is called the leading coefficient of $f(x)$, and n the degree of $f(x)$. Notation: $n = \deg f(x)$.

Remarks: The elements of R, when considered as polynomials in $R[x]$, are called constant polynomials. The constant polynomial 0_R **does not have a degree**.

Proposition

- *R commutative $\Rightarrow$ $R[x]$ commutative;*
- *R has an identity 1_R $\Rightarrow$ $R[x]$ has an identity 1_R;*
- *R integral domain $\Rightarrow$ $R[x]$ integral domain.*

Note that if F is a field, it is not true that $F[x]$ is a field. For example: $x \in F[x]$, but $x^{-1} \notin F[x]$; for x^{-1} would have to be an element in $F[x]$ such that when multiplied by x would produce 1_F. It does not exist.

Remark: Suppose
$f(x) = a_0 + a_1x + \cdots + a_nx^n$ with $\deg f(x) = n$, and
$g(x) = b_0 + b_1x + \cdots + b_mx^m$ with $\deg g(x) = m$.

Thus the leading coefficient of $f(x)g(x)$ equals a_nb_m if and only if $a_nb_m \neq 0$. This shows that $\deg[f(x)g(x)] \leq \deg f(x) + \deg g(x)$.

The Division Algorithm in $F[x]$:

Theorem

Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique $q(x), r(x) \in F[x]$ such that

$$f(x) = g(x)q(x) + r(x)$$

with either $r(x) = 0_F$ or $\deg r(x) < \deg g(x)$.

- The polynomials $q(x)$ and $r(x)$ (quotient and remainder, respectively) can be calculated via polynomial long division.
- This is taught in MATH 141, but we will work out an example on the board involving the field $F = \mathbb{Z}_3$ and the polynomials $f(x) = x^4 + x + 1$ and $g(x) = x^2 + 1$ in $F[x]$.
- Note: To divide by $a \neq 0$ in a field means to multiply by the multiplicative inverse of a: For example, to divide by 3 in $\mathbb{Z}_5$ means to multiply by 2. To divide by 4 means to multiply by 4, and so on.