16 Polynomial rings

Theorem. Let R be a ring. Then set of polynomials over R with indeterminate x

$$R[x] = \{a_0 + \cdots + a_n x^n : n \in \mathbb{N}, a_0, \ldots, a_n \in R, a_n \neq 0\}$$

is a ring under addition $f(x) + g(x)$ and $f(x)g(x)$, where for

$$f(x) = f_0 + \cdots + f_n x^n \quad \text{and} \quad g(x) = g_0 + g_1 x + \cdots + g_m x^m,$$

(1) $f(x) + g(x) = \sum (f_k + g_k) x^k$ where $f_{n+j} = g_{m+j} = 0$ for $j \in \mathbb{N}$,

(2) $f(x)g(x) = c_k x^k$ with $c_k = \sum_{i+j=k} f_i g_j$ for $k = 0, \ldots, n+m$.

Remark If $f(x) = a_0 + \cdots + a_n x^n$ with $a_n \neq 0$, then $f(x)$ has degree n.

In general, $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$ and $\deg(fg) \leq \deg(f) + \deg(g)$.

The equality holds ....

A nonzero constant polynomial has degree 0; the zero polynomial has degree $-\infty$.

Theorem 16.1 If $\mathbb{D}$ is an integral domain, then so is $\mathbb{D}[x]$.

Proof. $\deg(fg) = \deg(f) + \deg(g)$.

Theorem 16.2 If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ division algorithm can be performed, i.e., for every $f(x), g(x) \in \mathbb{F}[x]$ such that $g(x) \neq 0$. Then there is a unique $q(x), r(x)$ such that $\deg(r) < \deg(g)$ satisfying $f(x) = g(x)q(x) + r(x)$.

Proof. By induction on the degree of f.

- **Initial step.** The case $f(x) = 0$ is trivial.

  *) Suppose $f(x) = f_0 \neq 0$ has degree 0. If $\deg(f) < g(x)$, then $f(x) = g(x)0 + r(x)$ with $r(x) = f(x)$ with degree less than that of $g(x)$.

  *) If $g(x) = g_0 \neq 0$, then $f(x) = (f_0/g_0)g(x) + r(x)$ with $r(x) = 0$ of degree $-\infty$, which is less than that of $g(x)$.

- **Inductive step.** Suppose the result holds for $\hat{f}(x)$ of degree at most $n-1$ for $n-1 \geq 0$.

  Assume $f(x) = a_0 + \cdots + a_n x^n$, and $g(x) = b_0 + \cdots + b_m x^m$.

  *) If $n < m$, then $q(x) = 0, r(x) = g(x)$.

  *) If $m \geq n$, then

  $$f(x) - a_n b_m^{-1} x^{n-m} g(x) = f_1(x) = g(x)q_1(x) + r(x)$$

  with $\deg(r) \leq \deg(g)$. So,

  $$f(x) = g(x)(a_n b_m^{-1} + q_1(x)] + r(x).$$

- For uniqueness: If $f(x) = g(x)q(x) + r(x) = g(x)\hat{q}(x) + \hat{r}(x)$, then

  $$g(x)[q(x) - \hat{q}(x)] = \hat{r}(x) - r(x).$$

  So, $q(x) - \hat{q}(x) = 0$, else the degree on the left side is larger than that on the right side. $\square$

Corollary Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$, $a \in \mathbb{F}$. Then the following holds.

(a) $f(x) = (x-a)q(x) + f(a)$, i.e., $f(a)$ is the remainder.

(b) $(x-a)$ is a factor of $f(x)$ if and only if $f(a) = 0$.

(c) If $f(x) \in \mathbb{F}[x]$ has degree n, then $f(x)$ has at most n zeros, counting multiplicities.

Proof. (a) Let $f(x) = (x-a) + r$, where $r \in \mathbb{F}$. Then $f(a) = (a-a) + r = r$.

(b) By (a), $f(a) = 0$ if and only if $f(x) = (x-a)g(x)$.

(c) Induction on the degree of $f(x)$. If $n = 1$, then $f(x) = (x-a)$.
Assume the result holds for polynomial of degree $n-1$.
Suppose $f(x)$ has degree n.
If $f(x)$ has no zero in $\mathbb{F}$, then the conclusion holds.
If $f(a) = 0$, then $f(x) = (x-a)g(x)$, and $g(x)$ has at most $n-1$ zeros. The result holds.

Theorem If $\mathbb{F}$ is a finite field, then the nonzero elements in $\mathbb{F}$ is a cyclic group under multiplication.

Proof. By FTFGG, $(\mathbb{F}^*, \cdot)$ is isomorphic to $\mathbb{Z}_{p_1^{n_1}} \cdots \mathbb{Z}_{p_r^{n_r}}$. Consider the polynomial $x^N - 1 = 0$ with $N = |\mathbb{F}^*|$. There are at most N zeros. So, $p_1, \ldots, p_r$ are distinct. The result follows. $\square$

Theorem Let $\mathbb{F}$ be a field, and $f(x) = a_0 + \cdots + a_n x^n$ with $n \geq 2$ be irreducible, and $A = \langle f(x) \rangle = \{f(x)h(x) : h(x) \in \mathbb{F}[x]\}$. Then

$$\mathbb{E} = \mathbb{F}[x]/A = \{g(x) + A : g(x) \in \mathbb{F}[x]\} = b_0 + \cdots + b_{n-1}x^{n-1} + A : b_0, \ldots, b_{n-1} \in \mathbb{F}\}$$

is a field, containing $\mathbb{F} \equiv \{a + A : a \in \mathbb{F}\}$ as a subfield. Moreover, $f(X) \subseteq \mathbb{E}[X]$ has a zero $x + A$.

Proof. Only needs to check that every $\mathbb{E}^*$ has an inverse. This follows from the fact that for any $g(x) + A \in \mathbb{E}$, there is $r(x), s(x) \in \mathbb{F}[x]$ such that $f(x)r(x) + g(x)s(x) = 1$. So, $s(x) + A$ is the inverse of $g(x) + A$.

Let $f(X) \in \mathbb{E}[X]$. Then $f(x + A) = f(x) + A = A$. $\square$

Construction of a new field containing zeros of irreducible polynomials

Example 1 Suppose $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Then ...

Example 2 Suppose $f(x) = x^2 + 1 \in \mathbb{Z}_3[x]$. Then ....

Remark Let $f(x) = x^2 + ax + b \in \mathbb{Z}_p[x]$. Then ...

Example 3 Suppose $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ and $A = \langle x^2 - 2 \rangle$. Then

$$\mathbb{F} = \mathbb{Q}[x]/A = \{ax + b + A : a, b \in \mathbb{Q}\}$$

is a field. For every nonzero $ax + b + A \in \mathbb{F}$, the multiplicative inverse is $(ax - b)/(2a^2 - b^2) + A$ as

$$(ax + b + A)((ax - b)/(2a^2 - b^2) + A)$$

$$= (a^2x^2 - b^2)/(2a^2 - b^2) + A = (2a^2 - b^2)/(2a^2 - b^2) + A = 1 + A.$$

Here note that $2a^2 - b \neq 0$ because $a, b \in \mathbb{Q}$.

By the factor theorem, $f(x)$ has no zeros in $\mathbb{Q}$. But $x + A \in \mathbb{F}$ is a zero of the equation $y^2 - 2 \in \mathbb{E}[y]$ for $\mathbb{E} = \mathbb{F}[x]/A$ because $2 = 2(1+A) = 2+A$, as $(x+A)^2 - (2+A) = (x^2-2)+A = 0+A$.

Fact: (a) Every finite field has $q = p^r$ elements for a prime p.

(b) For every $r \in \mathbb{N}$, there is an irreducible polynomial $f(x)$ of degree r, which is a factor of $h(x) = x^{N-1} - x$ so that $\mathbb{Z}_p[x]/\langle f(x) \rangle$ has p^r elements.