Chapter 16 Polynomial rings

Preliminary: Chapter 1 - 15; at least the definitions of Group, Ring, Field.

Motivation Early study of algebra concerns solving (polynomial) equations:

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n = 0, \qquad \text{where } a_0, \ldots, a_n \in R.$$

We consider the problems for $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_2$ and a finite field, say, $\mathbb{Z}_p$.

Some natural questions.

1) Can we find a zero of $f(x)$ in R? That is, find $a \in R$ such that $f(a) = 0$.

2) If not, can we find a zero in a larger ring $\tilde{R}$?

3) What are the structure of the set $R[x]$ of all the polynomials in x over R?

4) Find the common and distinct features of $R[x]$ for different R.

5) What are the relations between the zeros of $f(x)$?

Notation and basic results

Remark One can define a polynomial function $f : R \to R$ by

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

Different polynomials may give rise to the same function.

Notation Let R be a commutative ring. The ring of polynomials over R in the indeterminate x is the set

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

We can consider equality, addition, multiplication and degree of a polynomial $f(x) \in R[x]$.

Theorem 16.1 If D is an integral domain, then $D[x]$ is an integral domain.

Proof. Check the ring axioms, unity, commutativity, no zero divisors.

Note If F is a field, then $F[x]$ behaves like $\mathbb{Z}$ in many regards.

Division Algorithm and Remainder Theorem

Theorem 16.2 [Division Algorithm.] If F is a field, and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$, then there exist unique polynomials $q(x), r(x)$ such that

$$f(x) = g(x)q(x) + r(x) \quad \text{with } \deg(r(x)) \leq \deg(g(x)).$$

Proof. See the proof in p. 301. In practice, we do the following.

Corollary [Remainder Theorem] Let F be a field, $f(x) \in F[x]$, $a \in F$. Then

$$f(x) = (x - a)q(x) + f(a),$$

i.e., $f(a)$ is the remainder.

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

If $\deg(f(x)) = n$, then $f(x)$ has at most n zeros, counting multiplicities.

Principal Ideal Domain

Definition A principal ideal domain is an integral domain R in which every ideal has the form

$$\langle a \rangle = \{ra : r \in R\} \quad \text{for some } a \in R.$$

Theorem 16.3-4 Let F be a field. Then $F[x]$ is a principal ideal domain.

In fact, for any non-zero ideal A of $F[x]$, $A = \langle g(x) \rangle$, where $g(x)$ is a nonzero polynomial in A with minimum degree.

Proof. The result is clear if $A = \{0\}$. Let $g(x) \in A$ have minimum degree. It exists because of the well-ordering principle of positive integers. Then every $f(x)$ is a multiple of $g(x)$. Else, ...

Quotient field

Example 1 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, where $0 + A$ and $1 + A$ are the zero and unity of the field, and the multiplicative inverse of $ax + b + A \in \mathbb{F}$ is $(ax - b)/(2a^2 - b^2) + A$ because

$$\begin{aligned} & (ax + b + A)((ax - b)/(2a^2 - b^2) + A) \\ = \; & (a^2x^2 - b^2)/(2a^2 - b^2) + A \\ = \; & (2a^2 - b^2)/(2a^2 - b^2) + A = 1 + A. \end{aligned}$$

Here note that $2a^2 - b^2 \neq 0$ 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 $y^2 - 2 \in \mathbb{F}[y]$, because

$$(x + A)^2 - (2 + A) = (x^2 - 2) + A = 0 + A.$$

Example 2 Suppose $f(x) = x^2 + 1 \in \mathbb{R}[x]$ and $A = \langle x^2 + 1 \rangle$. Then

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

is a field.

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

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

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

Note that $f(x)$ has no zeros in $\mathbb{R}$. But $x + A \in \mathbb{F}$ is a zero of $y^2 + 1 \in \mathbb{F}[y]$.

Example 3 Suppose $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ and $A = \langle x^2 + x + 1 \rangle$. Then

$$\mathbb{F} = \mathbb{Z}_2[x]/A = \{ax + b + A : a, b \in \mathbb{Z}_2\}$$

is a field with 4 elements.

For every nonzero $ax + b + A \in \mathbb{F}$, one can find the inverse. Here are the inverse pairs:

$$(1 + A, 1 + A), (x + A, 1 + x + A).$$

Note that $f(x)$ has no zeros in $\mathbb{Z}_2$. But $x + A \in \mathbb{F}$ is a zero of $y^2 + y + 1 \in \mathbb{F}$.