Lecture 16

3. Polynomial rings

We are familiar with polynomials over the rational or real numbers and we have seen that they form commutative rings. (Depending on the structures one is interested in, you might have considered polynomials over the reals and with bounds on the degree as vector spaces, too).

Definition (Polynomial in an indeterminate x over a ring R)

- Let R be a (commutative) ring. A polynomial in indeterminate x over R is an expression of the form

$$a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

where the coefficients $a_0, \dots a_n$ are elements of R.

- If $a_n \neq 0$ then n is the degree of the polynomial and a_n is the leading coefficient of the polynomial.
- A polynomial is said to be monic if its leading coefficient is the unity of R.
- The set of all polynomials in x over R is denoted $R[x]$.

If we define addition and multiplication in the familiar way, we have the following:

Theorem • The set $R[x]$ of all polynomials in an indeterminate x and with coefficients in R forms a ring under polynomial addition and multiplication.
It is commutative if R is commutative (this will always be the case for us).
• If R is an integral domain, then $R[x]$ is an integral domain.

Examples

(1) $\mathbb{Z}[x]$ is the ring (and integral domain) of polynomials with integer coefficients. The polynomials $x^3 - 3x + 5$ and $x - 3$ are elements of $\mathbb{Z}[x]$. We have

$$(x^3 - 3x + 5) + (x - 3) = x^3 - 3x + 2 \quad , \text{ and}$$

$$(x^3 - 3x + 5) \cdot (x - 3) = x^4 - 3x^3 - 3x^2 + (5x + 9x) - 15 =$$
$$= x^4 - 3x^3 - 3x^2 + 14x - 15$$

(2) $\mathbb{Z}_4[x]$ is a commutative ring. The polynomials $2x^2$ and $2x + 2$ are elements of $\mathbb{Z}_4[x]$. In this ring

$$2x^2 \cdot (2x + 2) = 4x^3 + 4x^2 = 0$$

So $\mathbb{Z}_4[x]$ is not an integral domain (nor is $\mathbb{Z}_4$).

(3) $\mathbb{Q}[x]$ is the ring of polynomials with rational coefficients. As $\mathbb{Q}$ is a field (so in particular an integral domain), $\mathbb{Q}[x]$ is an integral domain. Same is true for $F[x]$ whenever F is a field.

⚠ $R[x]$ is never a field (even if R is a field).

Polynomials with coefficients in a field share some similarities with the ring of integers. For instance, the division algorithm that works in $\mathbb{Z}$ has its analogue in $F[x]$. If we denote, for $f \in F[x]$, $\deg f(x)$ the degree of f, then the following holds.

Division algorithm If $f(x)$ and $g(x)$ are polynomials over a field F, with $g(x) \neq 0$, then there exist unique polynomials $q(x)$ and $r(x)$ over F such that

$$f(x) = g(x)\,q(x) + r(x) \quad \text{with} \quad r(x) = 0 \text{ or } \deg r(x) < \deg g(x).$$

In analogy with $\mathbb{Z}$, the polynomials $q(x)$ and $r(x)$ are called the quotient and the remainder of $f(x)$ divided by $g(x)$.

Examples (1) $f(x) = x^5+1$ and $g(x) = x^3-3x \in \mathbb{Q}[x]$:

$$\begin{array}{r|l} x^5 + 1 & x^3 - 3x \\ \hline -x^5 + 3x^3 & x^2 + 3 \\ \hline 3x^3 + 1 & \\ -3x^3 + 9x & \\ \hline 9x + 1 & \end{array}$$

$q(x)$ $r(x)$

$$\rightsquigarrow \quad x^5+1 = (x^3-3x)(x^2+3) + x+1$$

(2) $a(x) = x^4+3x^3+2x+4$ and $b(x) = x-1 \in \mathbb{Z}_5[x]$

then

$$\begin{array}{r|l} x^4+3x^3+2x+4 & x-1 \\ \hline -x^4+x^3 & x^3+4x^2+4x+1 \\ \hline 4x^3+2x+4 & \\ -4x^3+4x^2 & \\ \hline 4x^2+2x+4 & \\ -4x^2+4x & \\ \hline x+4 & \\ -x+1 & \\ \hline 0 & \end{array}$$

That is, in $\mathbb{Z}_5[x]$:

$x-1$ divides x^4+3x^3+2x+4 and

$$x^4+3x^3+2x+4 = (x^3+4x^2+4x+1)(x-1)$$

In particular, $a(1) = 0$

Formally, evaluating a polynomial at some element of the ring R is a (ring-)homomorphism. We will (as usual) simply write $f(c)$ for the value obtained by substituting in the expression $f(x) = a_0 + a_1x + \dots + a_nx^n$ c in place of x.

We can now state a thm relating the division algorithm to values of polynomials:

Remainder Theorem If $f(x) \in F[x]$ and $c \in F$, then the remainder in the division of $f(x)$ by $x-c$ is $f(c)$.

Indeed, since $\deg(x-c)=1$ then the remainder $r(x)$ must either be zero or have degree 0.

So $r(x)=r \in F$ and

$$f(x)=q(x)(x-c)+r$$

evaluating at c we get

$$f(c)=\underbrace{q(c)(c-c)}_{q(c)\cdot 0 = 0}+r$$

In particular, if $f(x) \in F[x]$ and $c \in F[x]$ then $x-c$ is a factor of $f(x)$ if and only if $f(c)=0$