

MATH 415  
Modern Algebra I

**Lecture 27:**  
**Rings of polynomials.**  
**Division of polynomials.**

## Polynomials in one indeterminate

*Definition.* A **polynomial** in an indeterminate (or variable)  $X$  over a ring  $R$  is an expression of the form

$$p(X) = c_0X^0 + c_1X^1 + c_2X^2 + \cdots + c_nX^n,$$

where  $c_0, c_1, \dots, c_n$  are elements of the ring  $R$  (called **coefficients** of the polynomial). The **degree**  $\deg(p)$  of the polynomial  $p(X)$  is the largest integer  $k$  such that  $c_k \neq 0$ . The set of all such polynomials is denoted  $R[X]$ .

*Remarks on notation.* The polynomial is denoted  $p(X)$  or  $p$ . The terms  $c_0X^0$ ,  $c_1X^1$  and  $1X^k$  are usually written as  $c_0$ ,  $c_1X$  and  $X^k$ . Zero terms  $0X^k$  are usually omitted. Also, the terms may be rearranged, e.g.,  $p(X) = c_nX^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$ . This does not change the polynomial.

*Remark on formalism.* Formally, a polynomial  $p(X)$  is determined by an infinite sequence  $(c_0, c_1, c_2, \dots)$  of elements of  $R$  such that  $c_k = 0$  for  $k$  large enough.

## Algebra of polynomials over a field

First consider polynomials over a field  $\mathbb{F}$ . If

$$\begin{aligned}p(X) &= a_0 + a_1X + a_2X^2 + \cdots + a_nX^n, \\q(X) &= b_0 + b_1X + b_2X^2 + \cdots + b_mX^m,\end{aligned}$$

then  $(p+q)(X) = (a_0+b_0) + (a_1+b_1)X + \cdots + (a_d+b_d)X^d$ , where  $d = \max(n, m)$  and missing coefficients are assumed to be zeros. Also,  $(\lambda p)(X) = (\lambda a_0) + (\lambda a_1)X + \cdots + (\lambda a_n)X^n$  for all  $\lambda \in \mathbb{F}$ . This makes  $\mathbb{F}[X]$  into a vector space over  $\mathbb{F}$ , with a basis  $X^0, X^1, X^2, \dots, X^n, \dots$ .

Further,  $(pq)(X) = c_0 + c_1X + c_2X^2 + \cdots + c_{n+m}X^{n+m}$ ,

where  $c_k = a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0$ ,  $k \geq 0$ .

Equivalently, the product  $pq$  is a bilinear function defined on elements of the basis by  $X^nX^m = X^{n+m}$  for all  $n, m \geq 0$ .

Multiplication is associative, which follows from bilinearity and the fact that  $(X^nX^m)X^k = X^n(X^mX^k)$  for all  $n, m, k \geq 0$ .

Thus  $\mathbb{F}[X]$  is a commutative ring and an associative  $\mathbb{F}$ -algebra.

## Ring of polynomials

Now consider polynomials over an arbitrary ring  $R$ . If

$$\begin{aligned}p(X) &= a_0 + a_1X + a_2X^2 + \cdots + a_nX^n, \\q(X) &= b_0 + b_1X + b_2X^2 + \cdots + b_mX^m,\end{aligned}$$

then  $(p+q)(X) = (a_0+b_0) + (a_1+b_1)X + \cdots + (a_d+b_d)X^d$ ,

where  $d = \max(n, m)$  and missing coefficients are assumed to be zeros. Also,  $(\lambda p)(X) = (\lambda a_0) + (\lambda a_1)X + \cdots + (\lambda a_n)X^n$  for all  $\lambda \in R$ . This makes  $R[X]$  into a **module over  $R$** . If  $1 \in R$ , the module has a basis  $X^0, X^1, X^2, \dots, X^n, \dots$  (a **free module**).

Further,  $(pq)(X) = c_0 + c_1X + c_2X^2 + \cdots + c_{n+m}X^{n+m}$ ,

where  $c_k = a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0$ ,  $k \geq 0$ .

One can show that multiplication is associative and distributes over addition. Now  $R[X]$  is a **ring of polynomials**. If  $R$  is commutative (a domain, a ring with unity), then so is  $R[X]$ .

Notice that  $\deg(p \pm q) \leq \max(\deg(p), \deg(q))$ . If  $p, q \neq 0$  and  $R$  is a domain, then  $\deg(pq) = \deg(p) + \deg(q)$ .

## Polynomials in several variables

The ring  $R[X, Y]$  of polynomials in two variables  $X$  and  $Y$  over a ring  $R$  can be defined in several ways. We can define it via “currying” as  $R[X][Y]$  (that is, polynomials in  $Y$  over the ring  $R[X]$ ) or  $R[Y][X]$  (that is, polynomials in  $X$  over the ring  $R[Y]$ ).

Also, we can define  $R[X, Y]$  directly as the set of expressions of the form

$$c_1 X^{n_1} Y^{m_1} + c_2 X^{n_2} Y^{m_2} + \dots + c_k X^{n_k} Y^{m_k},$$

where each  $c_i \in R$ , each  $n_i$  and  $m_i$  is a nonnegative integer, and the pairs  $(n_i, m_i)$  are all distinct.

Similarly, we can define the ring  $R[X_1, X_2, \dots, X_n]$  of polynomials in  $n$  variables over  $R$ .

## Division of polynomials

Let  $f(x), g(x) \in \mathbb{F}[x]$  be polynomials over a field  $\mathbb{F}$  and  $g \neq 0$ . We say that  $g(x)$  **divides**  $f(x)$  if  $f = qg$  for some polynomial  $q(x) \in \mathbb{F}[x]$ . Then  $q$  is called the **quotient** of  $f$  by  $g$ .

Let  $f(x)$  and  $g(x)$  be polynomials and  $\deg(g) > 0$ . Suppose that  $f = qg + r$  for some polynomials  $q$  and  $r$  such that  $\deg(r) < \deg(g)$  or  $r = 0$ . Then  $r$  is the **remainder** and  $q$  is the (partial) **quotient** of  $f$  by  $g$ .

Note that  $g(x)$  divides  $f(x)$  if the remainder is 0.

**Theorem** Let  $f(x)$  and  $g(x)$  be polynomials and  $\deg(g) > 0$ . Then the remainder and the quotient of  $f$  by  $g$  are well defined. Moreover, they are unique.

## Long division of polynomials

**Problem.** Divide  $x^4 + 2x^3 - 3x^2 - 9x - 7$  by  $x^2 - 2x - 3$ .

$$\begin{array}{r|l} & x^2 + 4x + 8 \\ x^2 - 2x - 3 & \overline{x^4 + 2x^3 - 3x^2 - 9x - 7} \\ & \underline{x^4 - 2x^3 - 3x^2} \\ & 4x^3 \phantom{- 8x^2} - 9x - 7 \\ & \underline{4x^3 - 8x^2 - 12x} \\ & 8x^2 + 3x - 7 \\ & \underline{8x^2 - 16x - 24} \\ & 19x + 17 \end{array}$$

We have obtained that

$$x^4 + 2x^3 - 3x^2 - 9x - 7 = x^2(x^2 - 2x - 3) + 4x^3 - 9x - 7,$$

$$4x^3 - 9x - 7 = 4x(x^2 - 2x - 3) + 8x^2 + 3x - 7, \text{ and}$$

$$8x^2 + 3x - 7 = 8(x^2 - 2x - 3) + 19x + 17. \text{ Therefore}$$

$$x^4 + 2x^3 - 3x^2 - 9x - 7 = (x^2 + 4x + 8)(x^2 - 2x - 3) + 19x + 17.$$

## Zeros of polynomials

*Definition.* An element  $\alpha \in \mathbb{F}$  is called a **zero** (or a **root**) of a polynomial  $f \in \mathbb{F}[x]$  if  $f(\alpha) = 0$ .

**Theorem**  $\alpha \in \mathbb{F}$  is a zero of  $f \in \mathbb{F}[x]$  if and only if the polynomial  $f(x)$  is divisible by  $x - \alpha$ .

*Idea of the proof:* The remainder under division of  $f(x)$  by  $x - \alpha$  is  $f(\alpha)$ .

**Problem.** Find the remainder under division of  $f(x) = x^{100}$  by  $g(x) = x^2 + x - 2$ .

We have  $x^{100} = (x^2 + x - 2)q(x) + r(x)$ , where  $r(x) = ax + b$  for some  $a, b \in \mathbb{R}$ . The polynomial  $g$  has zeros 1 and  $-2$ . Evaluating both sides at  $x = 1$  and  $x = -2$ , we obtain  $f(1) = r(1)$  and  $f(-2) = r(-2)$ . This gives rise to a system of linear equations  $a + b = 1$ ,  $-2a + b = 2^{100}$ . Unique solution:  $a = (1 - 2^{100})/3$ ,  $b = (2^{100} + 2)/3$ .