Some slides for 10th Lecture, Algebra

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

7-03-2014

Let R be a ring and $R[\mathbb{N}]$ the set of functions $f : \mathbb{N} \to R$ such that $f(n) = 0$ for n large enough. Think in $f(i)$ as the coefficient of X^i

Given $f, g \in R[\mathbb{N}]$ we define $+$ and $\cdot$

$$(f+g)(n) = f(n) + g(n)$$

$$(fg)(n) = \sum_{i+j=n} f(i)g(j)$$

where $i, j \in \mathbb{N}$

We denote by $X^i \in R[\mathbb{N}]$ the function with $X^i(i) = 1$ and $X^i(n) = 0$ if $n \neq i$

Notice that: $X^i X^j = X^{i+j}$

We view an element of $a \in R$ as the function with $a(0) = a$ and $a(n) = 0$ if $n > 0$.

So an element $f \in R[\mathbb{N}]$ can be written as

$$f = a_0 + a_1 X + \cdots + a_n X^n$$

were $a_i = f(i)$ and $f(i) = 0$ if $i > n$.

- 0 is the neutral element for the sum
- $1 = X^0$ is the neutral element for multiplication
- $fg = gf$
- $f(g + h) = fg + fh$
- $f(gh) = (fg)h$

Definition 4.1

We define $R[X]$ the polynomial ring in one variable over the ring R as $R[\mathbb{N}]$. Here X denotes the function X^1.

Concepts: Term, coefficient, degree, leading term, leading coefficient, monic polynomial.

Proposition 4.2.2

Let $f, g \in R[X] \setminus \{0\}$. If the leading coefficient of f or g is not a zero divisor then

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

$2X + 1$ is a unit in $\mathbb{Z}/4\mathbb{Z}[X]$, but in a domain the units have degree 0:

Proposition 4.2.3

Let R be a domain. Then $R[X]^* = (R[X])^* = R^*$

Proposition 4.2.4

Let d be a non-zero polynomial in $R[X]$. Assume that the leading coefficient of d is not a zero divisor in R. Given $f \in R[X]$, there exists polynomials $q, r \in R[X]$ such that

$$f = qd + r$$

and either $r = 0$ or none of the terms in r is divisible by the leading term of d.

$$f = qd + r$$

and either $r = 0$ or none of the terms in r is divisible by the leading term of d.

- $\mathrm{LT}(d) = aX^m$
- $f = qd + (r + s)$, where $q = 0$, $r = 0$ and $s = f$.
- If $s = 0$ we are done, if not: $\mathrm{LT}(s) = bX^n$
- If aX^m divides bX^n
  - Then $n \geq m$ and we have $b = ca$ and $bX^n = cX^{n-m}aX^m$.
  - Set $q := q + cX^{n-m}$ and $s := s - cX^{n-m}d$
- If aX^m does not divide bX^n
  - Set $r := r + bX^n$ and $s := s - bX^n$
- $f = qd + (r + s)$, still holds
- Repeat this process for the new s until you get $s = 0$.

Let d be a non-zero polynomial in $R[X]$. Assume that the leading coefficient of d is invertible in R. Given $f \in R[X]$, there exist unique polynomials $q, r \in R[X]$ such that

$$f = qd + r$$

and either $r = 0$ or $\deg(r) < \deg(d)$.
r is called the remainder of f divided by d.

- The leading term of d divides a term of degree n if and only if $\deg(d) \leq n$.
- Unique q, r

The map

$$\begin{array}{rcl} j : R & \to & R[X] \\ r & \mapsto & r + 0X + 0X^2 + \cdots \end{array}$$

is an injective ring homomorphism. We identify $j(R)$ and R and we view R as a subring of $R[X]$.

Proposition 4.3.1

Let $f = a_nX^n + \cdots + a_1X + a_0 \in R[X]$ and $\alpha \in R$. The map

$$\begin{array}{rcl} \varphi_\alpha : R[X] & \to & R \\ f & \mapsto & f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 \end{array}$$

is a ring homomorphism.

The element $\alpha \in R$ is called root of f if $f(\alpha) = \varphi_\alpha(f) = 0$. We denote the set of roots of $f \in R[X]$ by
$V(f) = \{\alpha \in R : f(\alpha) = 0\}$

Corollary 4.3.2

Let $f \in R[X]$. Then $\alpha \in R$ is a root of f if and only if $X - \alpha$ divides f.

- The multiplicity of α as a root in a non-zero polynomial f is the largest power $n \in \mathbb{N}$ such that $(X - \alpha)^n | f$.
- The multiplicity of α is denoted $\nu_\alpha(f)$.
- A multiple root is a root with $\nu_\alpha(f) > 1$.
- Notice that $\nu_\alpha(f) \leq \deg(f)$ and $f = (X - \alpha)^{\nu_\alpha(f)} h$, where $h(\alpha) \neq 0$.

$X^2 + 3X + 2 \in \mathbb{Z}/6\mathbb{Z}[X]$ has 4 roots but:

Lemma 4.3.4

Let R be a domain and $f, g \in R[X]$. Then $V(fg) = V(f) \cup V(g)$.

Theorem 4.3.5

Let R be a domain and $f \in R[X] \setminus \{0\}$. If $V(f) = \{\alpha_1, \ldots, \alpha_r\}$ then

$$f = q(X - \alpha_1)^{\nu_{\alpha_1}(f)} \cdots (X - \alpha_r)^{\nu_{\alpha_r}(f)}$$

where $q \in R[X]$ and $V(q) = \emptyset$. The number of roots of f counted with multiplicity is bounded by the degree of f.