Some slides for 19th Lecture, Algebra

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

25-11-2010

Let R be a ring and $f = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$. The derivative of f is

$$D(f) = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \cdots + 2 a_2 X + a_1$$

If we see the polynomial f as a map $\mathbb{N} \to R$, the derivative of f is $D(f)(n-1) = n f(n)$

Let $f, g \in R[X]$ and $\lambda \in R$. Then

- $D(f+g) = D(f) + D(g)$
- $D(\lambda f) = \lambda D(f)$
- $D(fg) = fD(g) + D(f)g$

Lemma 4.3.8

Let $f, g \in R[X]$

- If f^2 divides g then f divides $D(g)$
- $\alpha \in R$ is a multiple root of f if and only if α is a root of f and $D(f)$.

Funny phenomena in characteristic p:

- Let $X^p \in \mathbb{F}_p[X]$,

$$D(X^p) = pX^{p-1} = 0$$

- $D(X^n) = 0$ if and only if p divides n.

Gauss:

If R is a unique factorization domain then $R[X]$ is a unique factorization domain.

But we prove:

Proposition 4.6.1

The polynomial ring $F[X]$ is a Euclidean domain (and therefore a principal ideal domain and a unique factorization domain).

Proof:

- $\deg : F[X] \setminus \{0\} \to \mathbb{N}$ is a Euclidean function on $F[X]$
- For $f \in F[X]$ and $d \in F[X] \setminus \{0\}$ then there exists $q, r \in F[X]$ s.t.

$$f = qd + r$$

where $r = 0$ or $\deg(r) < \deg(d)$.

Hence, we can use the Euclidean algorithm to compute the GCD of two polynomials.

If $f \in F[X]$ is not an irreducible polynomial there is a factorization $f = f_1 f_2$ s.t.

$$0 < \deg(f_1), \deg(f_2) < \deg(f)$$

Proposition 4.6.3

Let $f \in F[X]$

1. $\langle f \rangle$ is a maximal ideal if and only if f is irreducible. In this case the quotient ring $F[X]/\langle f \rangle$ is a field
2. If $f \neq 0$ then f is a unit if and only if $\deg(f) = 0$
3. If $\deg(f) = 1$ then f is irreducible.
4. If f is irreducible and $\deg(f) > 1$ then f does not have any roots.
5. If $\deg(f)$ is 2 or 3 then f is irreducible if and only if f has no roots.

$X^4 + X^2 + 1 \in \mathbb{F}_2$ does not have any roots but it is not irreducible.

Polynomial rings modulo ideals

- $R \subset R[X]$
- Let $I \subset R[X]$ with $R \cap I = \langle 0 \rangle$ (no constant polynomials in I excepting 0)
- For $r_1, r_2 \in R$: if $[r_1] = [r_2]$ in $R[X]/I$ then $r_1 - r_2 \in R \cap I$. Hence $r_1 = r_2$.
- Therefore, if $R \cap I \langle 0 \rangle$ we may forget "[ ]" to denote $[r]$ in $R[X]/I$

Proposition 4.6.7

Let R be a ring and

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in R[X]$$

a monic polynomial of positive degree n. Then $R \cap \langle f \rangle = \langle 0 \rangle$.

The elements $[g] = g + \langle f \rangle$ in the quotient ring $R[X]/\langle f \rangle$ can be expressed uniquely as polynomials of degree $< n$

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

where $b_0, \ldots, b_{n-1} \in R$ and $\alpha = [X]$.

In $R[X]/\langle f \rangle$ we have the identity

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0$$