Some slides for 12th Lecture, Algebra 2

Diego Ruano

Department of Mathematical Sciences Aalborg University Denmark

14-03-2014

Diego Ruano Some slides for 12th Lecture, Algebra 2

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.

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*) ≤ *n*.
- Unique q, r

The map

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

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 $f = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ and $\alpha \in R$. The map

$$\varphi_{\alpha}: R[X] \rightarrow R$$

 $f \mapsto f(\alpha) = a_n \alpha^n + \dots + a_1 \alpha + a_0$

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* ∈ ℕ such that (*X* − *α*)^{*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*.

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

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

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

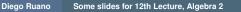
- If f^2 divides g then f divides D(g)
- $\alpha \in R$ is a multiple root of *f* if and only if α is a root of *f* and D(f).

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*.



 $\xi \in \mathbb{C}$ is called an *n*th root of unity (enhedsrod) for a positive integer *n* if $\xi^n = 1$.

Remember polar coordinates: $\xi = re^{i\theta} = r(\cos(\theta) + i\sin(\theta))$

 $\xi \in \mathbb{C}$ is called a primitive *n*th root of unity (primitiv n'te enhedsrod) for a positive integer *n* if $\xi^n = 1$ and $\xi, \xi^2, \dots, \xi^{n-1} \neq 1$.

Lemma 4.4.1

 $\xi \in \mathbb{C}$ is a primitive *n*th root of unity if and only if

$$\xi = e^{(k2\pi i)/n}$$

where $1 \le k \le n$ and gcd(k, n) = 1. If ξ is a primitive *n*th root of unity and $\xi^m = 1$ then n|m.

Let $n \in \mathbb{N}$ with $n \ge 1$. The *n*th cyclotomic polynomial (cyklotomiske polynomium)is

$$\Phi_n(X) = \prod_{1 \le k \le n, \gcd(k, n) = 1} (X - e^{2\pi i k/n}) \in \mathbb{C}[X]$$

Degree of $\Phi_n(X)$?

Proposition 4.4.3

Let $n \ge 1$. Then

•
$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

• $\Phi_n(X) \in \mathbb{Z}[X]$

We may consider the unique ring homomorphism $\kappa : \mathbb{Z} \to R$, for a ring *R*. And therefore

$$\kappa':\mathbb{Z}[X]\to R$$

Hence, we can see $X^n - 1 = \prod_{d|n} \Phi_d(X)$ in R[X]