Group Theory and Linear Algebra 05.08.2011

Lecture 6 Greatest common divisors and Euclid's algorithm

Number systems - $\mathbb{F}[t]$ polynomials.

Let $\mathbb{F}$ be a field.

$$\mathbb{F}[t] = \left\{ a_0 + a_1 t + a_2 t^2 + \dots \;\middle|\; \begin{array}{l} a_i \in \mathbb{F}, \text{ all but a finite} \\ \text{number of } a_i \text{ equal } 0 \end{array} \right\}$$

with addition and product so that

$$(5+t+7t^2) + (3+2t+8t^2+(-3)t^3) = 8+3t+15t^2+4t^3,$$

$$(1+2t^2+t^3)(0+0t+t^2+2t^3) = t^2+2t^3+4t^4+8t^5+t^5+2t^6$$
$$= t^2+2t^3+4t^4+9t^5+2t^6,$$

for example.

Let $d \in \mathbb{F}[t]$. The "ideal generated by d," or the set of multiples of d, is

$$d\,\mathbb{F}[t] = \{ dp \mid p \in \mathbb{F}[t] \}.$$

For example, $t^2+2t^3+4t^4+9t^5+2t^6 \in (1+2t^2+t^3)\mathbb{F}[t]$

Let $a, d \in \mathbb{F}[t]$. The polynomial d divides a, $d \mid a$, if $a \in d\mathbb{F}$.

For example

$$(1+2t^2+t^3) \mid (t^2+2t^3+4t^4+9t^5+2t^6).$$

Let $x, m \in \mathbb{F}[t]$. The greatest common divisor of x and m, $\gcd(x,m)$ is a monic polynomial d such that

(a) $d \mid x$ and $d \mid m$

(b) If $\ell \in \mathbb{Z}_{>0}$ and $\ell \mid x$ and $\ell \mid m$ then $\ell \mid d$.

Let $p \in \mathbb{F}[t]$, $p = p_0 + p_1 t + p_2 t^2 + \cdots$ with $p \neq 0$.

The degree of p is $N \in \mathbb{Z}_{\geq 0}$ such that

$p_N \neq 0$ and if $k \in \mathbb{Z}_{\geq 0}$ and $k > N$ then $p_k = 0$.

A polynomial $p = p_0 + p_1 t + p_2 t^2 + \cdots$ is monic if

$p_N = 1$, where $N = \deg(p)$.

Theorem (Euclid's algorithm) Let $a, b \in \mathbb{F}[t]$.

There exist $q, r \in \mathbb{F}[t]$ such that

(a) $a = bq + r$,

(b) Either $r = 0$ or $\deg(r) < \deg(b)$.

Theorem Let $x, m \in \mathbb{F}[t]$.

(a) There exists a monic polynomial ℓ such that

$$\ell\,\mathbb{F}[t] = x\,\mathbb{F}[t] + m\,\mathbb{F}[t]$$

(b) Let $d = \gcd(x,m)$. Then

$$d = \ell.$$

Example Find

$$\gcd\left((x^4-3x^3+3x^2-3x+2),\ (x^3-10x^2+23x-14)\right).$$

$$\begin{array}{r} x+7 \\ x^3-10x^2+23x-14 \overline{)\ x^4-3x^3+3x^2-3x+2} \\ \underline{x^4-10x^3+23x^2-14x} \\ 7x^3-20x^2+11x+2 \\ \underline{7x^3-70x^2+161x-98} \\ 50x^2-150x+100 \end{array}$$

So

$$(x^4-3x^3+3x^2-3x+2)=(x^3-10x^2+23x-14)(x+7)+50(x^2-3x+2)$$

$$x^3-10x^2+23x-14=(x^2-3x+2)(x-7)$$

So $\gcd(x^4-3x^3+3x^2-3x+2,\ x^3-10x^2+23x-14)=x^2-3x+2$

and

$$x^2-3x+2=\frac{1}{50}(x^4-3x^3+3x^2-3x+2)+\left(\frac{1}{50}x-\frac{7}{50}\right)(x^3-10x^2+23x-14).$$