§1 Lecture 11-20

Corollary 1.1 (If α is a zero of a polynomial, then $(x-\alpha)$ is a factor)
$\alpha \in \mathbb{F}$ is a zero of $p(x) \in \mathbb{F}[x] \Leftrightarrow (x-\alpha)$ is a factor of $p(x)$.

Proof. Apply division algorithm.

$p(x) = (x-\alpha)q(g) + r(x)$ where $\deg(r) < \deg(x-\alpha) = 1$

Hence, $p(\alpha) = 0 \Leftrightarrow r = 0 \Leftrightarrow (x-\alpha) \mid p(x)$ □

Theorem 1.2 (An n degree polynomial has at most n distinct zeros)
Let $p(x) \in \mathbb{F}[x]$ be a nonzero degree n polynomial.

Then $p(x)$ has at most n distinct zeros (roots).

Proof. By induction on $\deg(p)$.

Base case: has $\deg(p) = 0$ so $p(x) = c \neq 0$. (Not equal to 0 because then the degree would be minus infinity)

Hence $p(a) \neq 0$ for all $a \in \mathbb{F}$. Hence at most $\deg(p)$ roots in this case.

Suppose that the statement holds for $n = k$. Now we prove it for $n = k+1$.

Suppose $p(x)$ ha sa root r, so $p(r) = 0$.

So $p(x) = (x-r)q(x)$ for some $q \in \mathbb{F}[x]$ with $\deg(q) = \deg(p) - 1 = k$

Any root r' is either r or is a root of $q(x)$ because $0 = p(r') = (r'-r)q(r')$.

By induction, $q(x)$ has at most k distinct roots. Thus $p(x)$ has at most $k+1$ distinct roots. i.e. the roots of q and r. □

Definition 1.3 (Greatest Common Divisor Definition)**.** Let $p, q \in \mathbb{F}[x]$ where $\mathbb{F}$ is a field. A monic polynomial $d \in \mathbb{F}[x]$ is a gcd of p, q if $d|p$ and $d|q$ and $d'|d$ wherever $d'|p$ and $d'|q$.

Notation: $d = \gcd(p, q)$. p, q are relatively prime if $1 = \gcd(p, q)$.

Example 1.4
If $\mathbb{Z}_5[x]$, consider how $(x+1) = \gcd(x^2+4, x^3+4x^2+2)$.

Proposition 1.5
Let $\mathbb{F}$ be a field and $p, q \in \mathbb{F}[x]$. Also let $d = \gcd(p, q)$.

Then there exists $r, s \in \mathbb{F}[x]$ such that $d = rp + sq$.

Proof. Let d be the smallest degree monic polynomial in the ideal

$$J = \{fp + gq : f, g \in \mathbb{F}[x]\}$$

Then J contains non zero polynomial because $p = 1p + 0q \in J$.

Claim: $d \mid s$ for each $s \in J$ because otherwise $s = hd + r$ with $\deg(r) < \deg(d)$ and $r \neq 0$.

$$r = s - hd = fp + gq - h(f'p + g'q) \in J$$

hence $d \mid p$ and $d \mid q$ so $J = \langle d \rangle$.

Finally, if $d' \mid p$ and $d' \mid q$ then $d' \mid d$ because $p = p'd'$ and $q = q'd'$ so $d = r(p'd') + s(q'd') = d = (rp' + sq')d'$ □

Theorem 1.6
$\mathbb{F}[x]$ is a P.I.D. (principle ideal domain) i.e. every ideal in $\mathbb{F}[x]$ is principal i.e. is $\langle d \rangle$.

Example 1.7
$\mathbb{Z}[x]$ is not a principle ideal domain because $\langle x, y \rangle$ is not principal.

$\mathbb{F}[x, y]$ is not a principle ideal domain because $\langle x, y \rangle$ is not principal.

§1.1 Irreducible Polynomials

Definition 1.8. A $_{polynomial}$f $\in \mathbb{F}[x]$ is irreducible over $\mathbb{F}$ if $f \neq gh$ with $\deg(g) \geq 1$ and $\deg(h) \geq 1$.

Example 1.9
$x^2 - 3$ is irreducible over $\mathbb{Q}$ but not over $\mathbb{R}$.

$x^2 + 1$ is irreducible over $\mathbb{R}$, but it is not over $\mathbb{C}$.

$x^2 + 2$ is not irreducible over $\mathbb{Z}_3$. $(x^2 + 2) = (x - 1)(x - 2)$.

$x^2 + 2$ is irreducible over $\mathbb{Z}_5$ because it has no roots. Hence no degree factors.