2/26
Weds.
week 6

Chapter 9

Prop: Let F be a field and $p(x) \in F[x]$.
Then $p(x)$ has a factor of degree 1 in $F[x]$
iff there exists $\alpha \in F$ with $p(\alpha) = 0$.

proof:

($\Leftarrow$) Suppose there exists $\alpha \in F$ with $p(\alpha) = 0$.

By the division algorithm, we can divide $x-\alpha$ into $p(x)$ and then there exists $q(x), r(x) \in F[x]$ with

$$p(x) = (x-\alpha)\,q(x) + r(x)$$

with either $r(x)=0$ or $\deg(r(x)) < \deg(x-\alpha) = 1$.

So, in either case $r(x)$ is a constant.
Thus, $p(x) = (x-\alpha)\,q(x) + C$ where $C \in F$.
Since $p(\alpha)=0$ we get

$$0 = p(\alpha) = \underbrace{(\alpha-\alpha)\,q(\alpha)}_{0} + C = C.$$

So, $C=0$.
Thus, $p(x) = (x-\alpha)\,q(x)$.
So, $x-\alpha$ is a factor of degree 1 of $p(x)$.

($\Rightarrow$) Suppose $p(x)$ has a factor $ax+b$ of degree 1 where $a, b \in F$ and $a \neq 0$.

Thus,

$$p(x) = (ax+b)\,f(x) \quad \text{where } f(x) \in F[x].$$

Since $a \neq 0$, a^{-1} exists in our field F.
And $p(-ba^{-1}) = \boxed{a(-ba^{-1}) + b}\, f(-ba^{-1}) = 0 \cdot f(-ba^{-1}) = 0$.
Thus $p(x)$ has the root $-ba^{-1} \in F$. ▨

Ex:

Let $f(x) = x^3 - x^2 + x - 1$ be in $\mathbb{R}[x]$.

$\alpha = 1 \in \mathbb{R}$ and $f(1) = 0$.

And $f(x) = (x-1)(x^2+1)$

$f(x) = x^3 - x^2 + x - 1$ factors completely in $\mathbb{C}[x]$

$f(x) = (x-1)(x+i)(x-i)$

Ex: $g(x) = x^2 + 1$ be in $\mathbb{R}[x]$

g has no roots in $\mathbb{R}$.

So g has no linear factors in $\mathbb{R}[x]$

Prop: A polynomial $f(x)$ of degree two or three over a field F is reducible in $F[x]$ iff $f(x)$ has a root in F.

means in $F[x]$

pf: Suppose $f(x) \in F[x]$ has degree 2 or 3

($\Leftarrow$) Suppose $f(\alpha)=0$ where $\alpha \in F$.

By the previous proposition

$$f(x) = (x-\alpha)\, g(x)$$

where $g(x) \in F[x]$.

Since f has degree 2 or 3, we must have that $g(x)$ has degree 1 or 2.

So neither $x-\alpha$ nor $g(x)$ is a unit in $F[x]$.

Thus $f(x)$ is reducible in $F[x]$.

Recall
The units of $F[x]$ are the non-zero constants, or $F^\times = F \setminus \{0\}$

In an integral domain R, $p \in R$ is <u>irreducible</u> if whenever $p=ab$ with $a,b \in R$ then a is a unit or b is a unit.

p is <u>reducible</u> if there exist non-units $a,b \in R$ with $p=ab$.

($\Rightarrow$) Suppose $f(x) \in F[x]$ is reducible.

Then there exist <u>non-units</u> $a(x), b(x) \in F[x]$ with $f(x) = a(x)\,b(x)$.

Check out the possibilities →

$\deg(f(x))$	$\deg(a(x))$	$\deg(b(x))$
2	1	1
3	1	2
3	2	1

$\deg(a(x)) \neq 0$
$\deg(b(x)) \neq 0$
since they aren't units

So, no matter what $f(x)$ has a factor from $F[x]$ of degree 1.

So, by the previous prop, $\exists \alpha \in F$ with $f(\alpha)=0$. ▨

Ex: Is $f(x) = x^3 + \bar{2}x^2 + x + \bar{1}$ reducible or irreducible in $\mathbb{Z}_3[x]$??

$\deg(f) = 3$

So we just need to check if it has a root in $\mathbb{Z}_3$.

$f(\bar{0}) = \bar{1}$
$f(\bar{1}) = \bar{5} = \bar{2}$
$f(\bar{2}) = \bar{19} = \bar{1}$

} $f(x)$ has no roots in $\mathbb{Z}_3$. So, $f(x)$ is irreducible in $\mathbb{Z}_3[x]$.

Prop: (Rational roots theorem)

Let

$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

be in $\mathbb{Z}[x]$ with $a_n \neq 0$.

If $\frac{r}{s} \in \mathbb{Q}$ written in lowest terms [i.e. $\gcd(r,s) = 1$]

and $p\left(\frac{r}{s}\right) = 0$ then

$r \mid a_0$ and $s \mid a_n$.

Number theory

$a, b, c \in \mathbb{Z}$
$a \neq 0$

$a \mid bc$
$\gcd(a,b) = 1$
$\Rightarrow a \mid c$

Pro

Mu

So

Th

Si

ts theorem)

$+\cdots+a_1x+a_0$

$a_n \neq 0$.

itten in

$\gcd(r,s)=1$]

then

Number theory
$a,b,c \in \mathbb{Z}$
$a \neq 0$

$a \mid bc$ } $\Rightarrow a \mid c$
$\gcd(a,b)=1$

Proof: Since $p\left(\frac{r}{s}\right)=0$ we have

$$a_n\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0 = 0.$$

Multiply by s^n to get

$$a_n r^n + a_{n-1} s r^{n-1} + \cdots + a_1 s^{n-1} r + a_0 s^n = 0$$

So,

$$a_n r^n = s\left[-a_{n-1} r^{n-1} - \cdots - a_1 s^{n-2} r - a_0 s^{n-1}\right].$$

Thus, $s \mid a_n r^n$.

Since $\gcd(s,r)=1$ we have $s \mid a_n$.

Similarly,

$$r\left(-a_n r^{n-1} - a_{n-1} r^{n-2} s - \cdots - a_1 s^{n-1}\right) = a_0 s^n.$$

So, $r \mid a_0 s^n$.

Since $\gcd(r,s)=1$, we have $r \mid a_0$.

▨

Prop: (Gauss's Lemma)
Let $p(x) \in \mathbb{Z}[x]$. If $p(x)$ is reducible in $\mathbb{Q}[x]$, then $p(x)$ is reducible in $\mathbb{Z}[x]$.

Note: Since $\mathbb{Z} \subseteq \mathbb{Q}$, if $p(x)$ is reducible in $\mathbb{Z}[x]$, then $p(x)$ is reducible in $\mathbb{Q}[x]$.