MATH 407

5/9/18

* $f \in F[x]$, $\langle f \rangle = fF[x]$, $\deg(f) \geq 1$

$a \equiv b \pmod f$ iff $a - b \equiv 0 \pmod f$

iff $f \mid (a-b)$

iff $(a-b) \in \langle f \rangle$

$\langle f \rangle = \langle 0 \rangle$

iff $a = fq_a + r_a$

$b = fq_b + r_b$

$r_a = r_b$

r_a only $s \in [a]$, $\deg(s) < \deg(f)$

$F[x]/\langle f \rangle = \{[r] : \deg(r) < \deg(f)\}$

* $\{[\lambda] : \lambda \in F\} \Rightarrow \Phi : \lambda \to [\lambda] = \lambda[1]$

bijection F onto const. congr. classes

$F[x]/\langle f \rangle$ is a vector space over F w/ basis

$\{[1], [\lambda], \ldots, [x]^{k-1}\} = [x^k]$

$= \{[a_0 + a_1 x^1 + \ldots + a_{k-1} x^{k-1}]\}$

$= \{a_0[1] + a_1[x] + \ldots + a_{k-1}[x^{k-1}]\}$

$= \{a_0 1 + a_1 x + \ldots + a_{k-1} x^{k-1}\}$

* $[x]^{-1}$ exists iff when $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k$

then $\alpha_0 \neq 0$

$\alpha_0 = -(\alpha_1 x + \ldots + \alpha_k x^k)$

$1 = -\left(\frac{\alpha_1}{\alpha_0} 1 + \ldots + \frac{\alpha_k}{\alpha_0} x^{k-1}\right) x$

Prop If $a(x) \in F[x]$, $0 \leq \deg(a) < \deg(f)$

1) $[a]$ is a zero divisor (in $F[x]/\langle f \rangle$)
2) $\gcd(a,f) \neq 1$
3) $[a]^{-1}$ does not exist

Pf 1) $\Rightarrow$ 3)

For 2) $\Rightarrow$ 1):

If $d = \gcd(a,f)$, $a = \hat{a}d$, $f = \hat{f}d$

$a\hat{f} = \hat{a}(\hat{f}d) = \hat{a}f \equiv 0 \pmod{f}$

For 3) $\Rightarrow$ 2):

Suppose not 2), $\gcd(a,f) = 1$.

Then $ab + fg = 1$, some b, g

Thus $ab - 1 = fg \equiv 0 \pmod{f}$

$ab \equiv 1 \pmod{f}$

$[a][b] = [1]$

Then, not 3). $\therefore$ 3) $\Rightarrow$ 2)

Cor. $F[x]/\langle f \rangle$ is a field iff f is irreducible.

If $F[x]/\langle f \rangle$ is a field and $[a] \neq 0$, $\exists [b] \neq 0$ s.t. $[a][b] = 1$

$[ab - 1] = 0$

* $+, \cdot$ tables in $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

$x^2 = x \cdot x$

$x^2+x+1 \equiv 0$

$\Rightarrow x^2 \equiv x+1$

* $F[x]/f$, $f(x) = a_0 + a_1x^1 + \ldots + a_kx^k$

$\langle f \rangle = \langle 0 \rangle$

$f \equiv 0$

$$\frac{-\left(a_0 + a_1x^1 + \ldots + a_{k-1}x^{k-1}\right) \equiv a_kx^k}{a_k}$$

$$\Rightarrow \frac{-\left(a_0 + a_1x^1 + \ldots + a_{k-1}x^{k-1}\right)}{a_k} \equiv x^k$$