LN XIV

§6.4

Definition Let r, s, f be poly

We say r and s are congruent mod f

if $\exists q.$ $\quad r - s = qf$

($r-s$ is divisible by f)

Notation $\quad r \equiv s \mod f.$

Ex $\quad f = x^2 - 1$

$$f = (x+1)(x-1) = gh.$$

So $\quad gh \equiv 0 \mod f.$

g and h are zero divisors.

Similar to $\mathbb{Z}_4$: $\quad [2]_4 [2]_4 = [0]_4$

To avoid zero-divisors we take

f to be an irreducible poly.

$[r]_f$ polynomial congruence class of r.

$r = qf + t \quad \deg(t) < \deg(f)$.

t is the standard representative of $[r]_f$

Lemma: the standard representative is unique.

Pf) Let $t, s \in [r]_f$ with $\deg(t), \deg(s) < \deg(f)$.

So $t \equiv s \mod f$.

$t - s = q \cdot f$.

$\deg(t-s) < \deg(f)$.

$\deg(qf) = \deg(q) + \deg(f)$ or 0 (when $q = 0$).

$\Rightarrow q = 0$ and $r - s = 0$

So $r = s$ $\square$.

Operations of Congruence Classes

<u>Def</u> $[r]_f + [s]_f = [r+s]_f$

$$[r]_f [s]_f = [rs]_f.$$

For this definition to ~~be~~ actually define sum and product, we need to show that $[r+s]_f$, $[rs]_f$ does not depend on the representation.

Indeed,

<u>Lemma</u>: Let f, r, s, t be poly. with

$$[r]_f = [t]_f$$

Then

$$[r+s]_f = [t+s]_f$$

$$[rs]_f = [ts]_f.$$

Pf] $[r]_f = [t]_f$. So

$r = t + qf$.

Then $r+s = t + qf + s$ So

$r+s \equiv t+s \mod f$.

$rs = (t+qf)s = ts + qs \cdot f$. So

$rs \equiv ts \mod f$ $\square$.

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

$\deg(f)=2$. So the standard represatation of each $[r]_f$ is a constant or linear.

$$[r]_f = [ax+b]_f.$$

The

$$[ax+b]_f + [cx+d]_f = [(a+c)x + b + d]_f.$$

$$[ax+b]_f [cx+d]_f = [ac\,x^2 + (ad+bc)x + bd]_f$$

$$= [ac(x^2+1) + (ad+bc)x + (bd-ac)]_f.$$

$$= [(ad+bc)x + (bd-ac)]_f.$$

Observe, this is related to multiplication of complex numbers.

$$(ai+b)(ci+d) = (ad+bc)i + (bd-ac).$$

<u>Definition</u> The class ~~has~~ $[r]_f$ has an inverse $[s]_f$ if

$$[r]_f[s]_f = [1]_f.$$

<u>Lemma</u>: If f is irreducible. then every $[r]_f$ has an inverse.
$\neq [0]_f$

<u>Pf</u>] $[r]_f \neq [0]_f$

Because f is irreducible

$$\gcd(r,f) = 1$$

So, $\exists$ s,t. s.t.

$$rt + fs = 1$$

$$[r]_f[t]_f = [rt]_f = [1-fs]_f = [1]_f$$

$\square$.

So, if <u>f is irreducible then</u> <u>the set of congruence classes is a field</u>: $(\{[r]_f\}, +, \cdot)$.

<u>Thm</u> (Galois): Every finite field F has $\# F = p^n$ for some prime p and n.

<u>How to construct a field with p^n elements?</u>

1) Take f an irreducible poly of degree n over $\mathbb{Z}_p$.

2) The standard representatives of $[r]_f$ are of the form

$$a_0 + a_1 x + \cdots + a_{n-1} x^n$$

where $a_k \in \mathbb{Z}_p$.

So $\# \{[r]_f\} = p^n$