ALGEBRA NOTE 6

JOHNEW ZHANG

1. Arithmetic Modulo for Polynomial

Overview : If $a, b, m \in \mathbb{Z}, m \geq 1$, then $a \equiv b \pmod{m} \iff m|(a-b)$.

Definition 1. *If F is a field, and $g, h, f \in \mathbb{F}[x], f \neq 0$, then $g \equiv h \pmod{f}$ if and only if $f|(g-h)$.*

$x^3 + x + 1 \equiv x \pmod{x^3 + 1}$.

Theorem 1. *If $a_1 \equiv a_2 \pmod{f}$ and $b_1 \equiv b_2 \pmod{f}$*
($a_1, a_2, b_1, b_2, f \in \mathbb{F}[x], f \neq 0$).
Then $a_1 + b_1 \equiv a_2 + b_2 \pmod{f}$
$a_1 b_1 \equiv a_2 b_2 \pmod{f}$

Definition 2. *The congruence class of g mod f to b*
$[g] = \{h \in \mathbb{F}[x]$ such that $h \equiv g \pmod{f}\}$.

So mod $x^2 - 1$.
$[x^3] = [x]$.
$[x^2 + 1] = 2$.

Next day arithmetic for congruence classes.
Clearly
$g \equiv g \pmod{f}$
$g \equiv h \pmod{f} \iff h \equiv g \pmod{f}$.

$$g \equiv h \pmod{f} \text{ and } h \equiv j \pmod{f} \implies g \equiv j \pmod{f}$$

because $f|(g-h)$ and $f|(h-j) \implies f|(g-j)$.
$[g] = \{h \in \mathbb{F}[x] : h \equiv g \pmod{f}\}$
$[g] = [h] \implies$
$g \equiv g \pmod{f}$

Definition 3. $[g] + [h] = [g + h]$.

Fact : If $a_1 \equiv a_2 \pmod{f}$ and $b_1 \equiv b_2 \pmod{f}$
$(a_1, a_2, b_1, b_2, f \in \mathbb{F}[x], f \neq 0)$.
Then $a_1 + b_1 \equiv a_2 + b_2 \pmod{f}$

If a_1, a_2 are in the same congruence class and b_1, b_2 are in the same congruence class, then $a_1 + b_1, a_2 + b_2$ are in the same congruence class as well.

Also define $[g]h] = [gh]$.

Theorem 2. *The set of congruence class* $\pmod f$ *under these properties is a commutative ring.* $0 = [0], 1 = [1]$.

Example : $\mathbb{F} = \mathbb{Q}$.
$f(x) \in \mathbb{Q}[x]$ is $x^2 + 1$.
$[x-1][x+1] = [(x-1)(x+1)] = [x^2 - 1] = [-2]$.
It is a nice observation : Working modulo f, $deg(f) \geq 1$, every congruence class has a representative g with $deg(g) < deg(f)$.

Proof. If $f(x) \in \mathbb{F}[x], deg(f) \geq 1$ and $h(x) \in \mathbb{F}[x]$, we can write $h(x) = f(x)q(x) + r(x), deg(r) < deg(f)$.
$h \equiv r \pmod f, [h] = [r]$.
Notation : If $\mathbb{F}$ is a field and $f(x) \in \mathbb{F}[x]$ has degree less than or equal to 1, then $\mathbb{F}[x]/(f)$ is the ring of congruence classes $\pmod f$. □

Example : $\mathbb{F} = \mathbb{Z}_3$, $f(x) = x^2 + 1$
$\mathbb{F}[x]/(f) = \mathbb{Z}_3[x]/(x^2 + 1)$.
Every congruence class has a representative of degree less than 2.
Polynomial in $\mathbb{Z}_3[x]$ with degree less than 2. $(0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2)$
The only congruence classes are $[0], [1], [2], [x], [x+1], [x+2], [2x], [2x+1], [2x+2]$
So,$\mathbb{Z}_3[x]/(f) = \{[0], \ldots\}$.
Is this a field? Does every non-zero element have a multiplicative inverse?
This ring is a field.

First example of a finite field where the number of elements is not prime.
What are the finite fields?
$\mathbb{Z}_p, \mathbb{Z}_3[x]/(x^2 + 1)$.

Theorem 3. *If $\mathbb{F}$ is a field, and $f(x) \in \mathbb{F}[x]$ has degree ≥ 1, then $\mathbb{F}[x]/(f)$ is a field if and only if f(x) is irreducible.*

Proof. If f(x) is not irreducible, then $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{F}[x], deg(g), deg(h) < deg(f)$
$[g], [h] \neq 0$ since $f \nmid g, f \nmid h$.
But $[g][h] = [gh] = [f] = 0$.
If $[g]$ had a multiplicative inverse, then $[g]^{-1}[g][h] = [0]$
$[h] = 0$, Therefore, this contradicts, so $[g]$ has an inverse $\implies$ $\mathbb{F}[x]/(f)$ is not a field.
If f(x) is irreducible, then for any $[g] \neq 0$, so $f \nmid g$, $gcd(f, g) = 1$
So we can choose $s, t \in \mathbb{F}[x]$ with $sf + tg = 1$.
$[1] = [sf + tg] = [tg] = [t][g]$.
So $[g]^{-1} = [t]$, Since $[g] \neq 0$, was any element of $\mathbb{F}/(f)$, this is a field. □

x^2+1 is irreducible in $\mathbb{Q}[x]$, so $\mathbb{Q}[x]/(x^2+1)$ is a field.
Consider : think of $\mathbb{Q}$ being in this field, since for every rational $q \in \mathbb{Q}, [q] \in Q[x]/(x^2+1)$.
If $[q_1] = [q_2]$, $q_1, q_2 \in \mathbb{Q}$, then $x^2+1|(q_1 - q_2)$.
$q_1 = q_2$ as rational numbers, so the function $q \implies [q]$ is injective (one-to-one).
This function also contains a square root of -1.
$[x]^2 = [x^2] = [-1]$.
Field is "the same" as $\mathbb{Q}[i]$.
$\mathbb{Q}[x][y]$ = polynomials in x and y with coefficients in $\mathbb{Q}$.

2. Finite Field

Theorem 4. *Let $\mathbb{F}$ be a field, and $f(x) \in \mathbb{F}[x]$ an irreducible polynomial of degree ≥ 1. Then $\mathbb{F}[x]/(f)$*
(i) is a field.
(ii) contains a copy of $\mathbb{F}$.
(iii) contains a root of f(x).

Proof. (i) is already done.
(ii) We can define a function $g(a) = [a]$ for $\mathbb{F}$ to $\mathbb{F}[x]/(f)$.
By definition, $g(a+b) = g(a) + g(b), g(ab) = g(a)g(b)$.
And also g is an injective function, because $g(a) = g(b)$, then $[a] = [b]$, so $f(x)|(b-a)$. This is impossible unless $b = a$.
(iii) $f([x]) = [f(x)] = [0] = 0$

□

Proposition 1. *Let p be a prime, and $f(x)Z_p[x]$ an irreducible polynomial of degree $d \geq 1$. Then $\mathbb{Z}_p[x]/(f)$ is a field with p^d elements.*

Proof. Every congruence class contains a unique polynomial r(x) with $deg(r) \leq d-1$. If $r_1(x), r_2(x)$ have degree $\leq d-1$.
then if $[r_1] = [r_2]$, we have $f|(r_2 - r_1)$ $deg(f) > deg(r_2 - r_1)$.
So this is only possible if $r_1 = r_2$.
The congruence classes are in one-to-one correspondence with polynomial in $\mathbb{Z}_p[x]$ of degree $\leq d-1$.
The number of polynomials in $\mathbb{Z}_p[x]$ with degree $\leq d-1$ is the number of sequences $a_0, a_1, \ldots, a_{d-1} \in \mathbb{Z}_p$.
So there are p^d choices. □

Theorem 5. *Fermat's Little Theorem for Finite Fields :*
If $\mathbb{F}$ is a field with n ($< \infty$) elements, and $a \in \mathbb{F}$ is non-zero, then $a^{n-1} = 1$.

Proof. Define $f : F \to F$ by $f(X) = ax$.
$Clearly, f(0) = 0$
f is one-to-one because if $f(x) = f(y)$, then $ax = ay \implies a(x-y) = 0$
$a^{-1}a(x-y) = a^{-1}0$
Therefore, $x = y$.

f is onto, since for any $x \in \mathbb{F}$, $f(a_{-1}x) = x$.
So $\Pi_{x\in\mathbb{F},x\neq 0}x = \Pi_{x\in\mathbb{F},x\neq 0}f(x) =_x \in \mathbb{F}, x \neq 0(ax) = a^{n-1}\Pi_{x\in\mathbb{F},x\neq 0}x$.
$\Pi_{x\in\mathbb{F},x\neq 0}x \neq 0$
So $1 = a^{n-1}$. □

Corollary 1. *If $\mathbb{F}$ is a finite field with n elements, then $x^n = x$ factors as $\Pi_{a\in\mathbb{F}}(x-a)$.*

Proof. For each $a \in \mathbb{F}$, either $a = 0$, so $a^n - a = 0^n - 0 = 0$.
or $a \neq 0$, and
$a^n - a = a(a^{n-1} - 1) = a0 = 0$.
$\Pi_{a\in\mathbb{F}}(x-a)|x^n - x$.
But both have the same degree (n), so $c\Pi_{a\in\mathbb{F}}(x-a)|x^n - x = (x^n x)$ for some $c \in \mathbb{F}$.
so $c = 1$. and $\Pi_{a\in\mathbb{F}}(x-a)|x^n - x = (x^n x)$ □