Def ① congruent modulo f. (Zn 的推广)

令 F 为一个 field. 固定 $p(x) \in F[x]$. ($\neq 0$)

对于 $g(x), h(x) \in F[x]$,

若 $p(x) \mid g(x) - h(x)$ (或称 $g(x)$ is congruent to $h(x)$ modulo $p(x)$)

则称 $g(x), h(x)$ congruent modulo $p(x)$

写作: $g(x) \equiv h(x) \bmod p(x)$ (或 $g \equiv h \bmod p$)

Thm ① 5.1 congruence modulo $p(x)$ 是个 equivalence relation

F 为 field. $p(x) \in F[x]$ 非 0. 类比 thm 2.1

⇒

(1) reflexive: $\forall f(x) \in F[x]$, $f(x) \equiv f(x) \bmod p(x)$

(2) symmetric: 若 $f(x) \equiv g(x) \bmod p(x)$,
则 $g(x) \equiv f(x) \bmod p(x)$

(3) transitive: 若 $f(x) \equiv g(x) \bmod p(x)$
$g(x) \equiv h(x) \bmod p(x)$
则 $f(x) \equiv h(x) \bmod p(x)$

Thm ② 5.2 类比 Thm 2.2

F 为 field. $p(x) \in F[x]$ 非 0.

若 $f(x) \equiv g(x) \bmod p(x)$

$h(x) \equiv k(x) \bmod p(x)$

则 ⇒ (1) $f(x) + h(x) \equiv g(x) + k(x) \bmod p(x)$

(2) $f(x)\,h(x) \equiv g(x)\,k(x) \bmod p(x)$

Def ② congruence class (或称 residue class)

$F[x]$ 中所有 congruent to $g(x) \bmod p(x)$ 的 polynomials 的 set 写作 $[g(x)]_{p(x)}$ 或 $[g]_p$

即: $[g(x)]_{p(x)} = \{ s(x) \mid s(x) \in F(x) \text{ and } s(x) \equiv f(x) \bmod p(x) \}$

Thm ③ 5.3 (类比 Thm 2.3.)

$f(x) \equiv g(x) \bmod p(x)$

iff $[f(x)]_{p(x)} = [g(x)]_{p(x)}$

(不知道为什么有这个 thm, 实际就是 def 的注意到)

Corollary ④ 5.4 (类比 corollary 2.4)

两个 congruence class modulo $p(x)$

either disjoint or identical

Corollary ⑤ 5.5

令 F 为 field. $p(x) \in F[x]$, degree 为 n.

即 $f(x) = q(x)p(x) + r(x)$

(1) If $f(x) \in F[x]$ 且 $r(x)$ 为 $f(x)$ 被 $p(x)$ divide 时的 remainder. ⇒ $[f(x)]_{p(x)} = [r(x)]_{p(x)}$ (显然)

(2) 令 S 为包含 0_F 和 $F[x]$ 中所有 degree $\leq n$ 的 polynomial 的 set

即: $S = \{0_F\} \cup \{f(x) \in F[x] \mid \deg f(x) \leq n\}$

⇒ $F[x]$ 中每个 $p(x)$ 的 congruent class 都是 S 中某个 polynomial 的 congruent class. 并且 S 中, 每个 different polynomial 都有 distinct congruence class.

注: 就像 Z_n 中每个 congruence class 都是 $\{0, 1, \ldots, n-1\}$ 中某个 int 的 congruence class, 且这个 set 每个 elem 的 congruence class 都 distinct, 也就是一个元素代表一个 congruent class, covering every congruence class.

Def ③

The set of all congruence classes modulo $p(x)$ on $F[x]$ is denoted by:

$$F[x]/(p(x)) \quad ☆$$

与 Z_n 类比, Z_n 把 Z 分为 n 个 congruence classes.

而 $F[x]/(p(x))$ 把 $F[x]$ 分为 $|S|$ 个 (可能 infinite, $S = \{0_F\} \cup \{f(x) \in F[x] \mid \deg f(x) \leq n\}$) congruent classes.

$$F[x]/(p(x)) = \left\{ [f(x)]_{p(x)} \mid f(x) \in S \right\}$$

Thm ⑥ 5.6 (即 Thm 5.2, 5.3 另一个说法)

若 $[f(x)]_{p(x)} = [g(x)]_{p(x)}$, $[h(x)]_{p(x)} = [k(x)]_{p(x)}$

$\in F[x]/(p(x))$.

则 (1) $[f(x) + h(x)]_{p(x)} = [g(x) + k(x)]_{p(x)}$

(2) $[f(x)h(x)]_{p(x)} = [g(x)k(x)]_{p(x)}$

Def ④ $+$ 和 $\times$ in $F[x]/(p(x))$

$+$: $[f(x)]_{p(x)} + [g(x)]_{p(x)} = [f(x)+g(x)]_{p(x)}$

$\times$: $[f(x)]_{p(x)} \cdot [g(x)]_{p(x)} = [f(x)g(x)]_{p(x)}$

Thm ⑦ 5.7

令 F 为 field. $p(x)$ 为 $F[x]$ 上的 non const polynomial.

$\Rightarrow$ $F[x]/(p(x))$ 为一个 commutative ring.

且 $F[x]/(p(x))$ 一定有一个 subring F^* which is isomorphic to F.

这是一个很好的结论. 实际上 $F \subseteq F[x]/(p(x))$. F 自身也是 $F[x]/(p(x))$ 的 subring.

Thm ⑧ 5.8

令 F 为 field. $p(x)$ 为 $F[x]$ 上的 non const polynomial.

$\Rightarrow$ $F[x]/(p(x))$ 为一个 commutative ring. 且 F 为其一个 subring.

(给定一个 field F, 我们总是能构造出一个更大的 ring, 包括它为一个 subring. $F[x]$, $F[x]/(p(x))$ 都是.)

Thm ⑨ 5.9

F 为 field. $p(x) \in F[x]$ 非 const.

$\Rightarrow$ 若 $f(x) \in F[x]$ 且 $f(x)$, $p(x)$ relatively prime. (gcd 为 1 F)

则 $[f(x)]_{p(x)}$ 为 $F[x]/(p(x))$ 的一个 unit.