Chapter 5.2

Chapter 5 Congruence in $F[x]$ and Congruence Class Arithmetic

<u>F is a field</u>

Both $F[x]$ and $\mathbb{Z}$ are rings.

We present a construction similar to modular arithmetic for $F[x]$ instead of $\mathbb{Z}$.

<u>Modular arithmetic (Chapter 2):</u>

From $\mathbb{Z}$ and $n>0$, $n\in\mathbb{Z}$ we constructed $\mathbb{Z}_n$ - the ring of congruence classes modulo n

<u>Now (Chapter 5)</u>

From $F[x]$ and $p\in\mathbb{Z}$, we will construct $F[x]/(p)$ - another ring

---

<u>Congruences</u>

<u>Def</u> Let $p\in F[x]$, $p\neq 0_F$; let $f, g\in F[x]$.

f is congruent to g modulo p $\left.\begin{array}{l} \\ f\equiv g \pmod{p}\end{array}\right\}$ means $p \mid (f-g)$

Otherwise $f\not\equiv g \pmod{p}$

Th 5.1 The relation $\equiv$ on $F[x]$ is an <u>equivalence relation</u> $\Big\}$ reflexive, symmetric, transitive

(parallel to Th 2.1)

The congruence relation $\equiv$ thus determines a partition of $F[x]$ into equivalence classes (aka congruence classes or residue classes)

<u>Notation</u> $F[x]/(p)$ – the set of equivalence classes

$\mathbb{Z}_n \left(= \mathbb{Z}/(n) \right)$

An equivalence class which contains (a representative) $f \in F[x]$ is denoted by

$$[f] = \{ g \in F[x] \mid g \equiv f \ (\mathrm{mod}\, p) \}$$

$$f \equiv g \ (\mathrm{mod}\ p) \quad \text{means } [f] = [g]$$

$f \in \mathbb{Z}$

$[f]$

$$[f] = \{ g \in \mathbb{Z} \mid g \equiv f \ (\mathrm{mod}\, n) \}$$

We have Euclid's Lemma in $F[x]$:

$$f = qp + r \qquad r = 0_F \text{ or } \deg r < \deg p$$

As a set,

$$F[x]/(p) = \{ [0_F] \} \cup \{ r \in F[x] \mid r \neq 0_F, \ \deg r < \deg p \}$$

$\mathbb{Z}_n = \{ [0], [1], \dots, [n-1] \}$

– all possible remainders from division by n

$$f = qn + r, \quad 0 \le r < n$$

Two polynomials in this set are not congruent

$$\deg(r - r') \le \max(\deg r, \deg r') < \deg p$$

implies $p \nmid (r - r')$ means $[r] \neq [r']$

<u>Operations</u> of addition and multiplication on $F[x]/(p)$ $\qquad p \in F[x]$

$$\left| \begin{array}{l} [f]+[g]=[f+g] \\ [f][g]=[fg] \end{array} \right.$$

<u>To check:</u> these operations are well-defined (easy)

With these operations, $F[x]/(p)$ becomes a ring

Th 5.7 Let $p \in F[x]$ be a non-constant polynomial. The set $F[x]/(p)$ with the operations defined above is a commutative ring with identity $1_{F[x]/(p)} = [1_F]$. Furthermore, $F[x]/(p)$ contains a subring which is <u>isomorphic to F</u>. $\leftarrow$ new

exactly parallel to $\mathbb{Z}_n$, $n \in \mathbb{Z}$

Comments on "Furthemore...".

As a set, $F[x]/(p) = \{[0_F]\} \cup \{[r] \mid r \in F[x], r \neq 0_F, \deg r < \deg p\}$ $\qquad \deg p > 0$

In particular, $\qquad \deg r = 0$ iff $r \in F$, $r \neq 0_F$

$$F[x]/(p) \supseteq \{[0_F]\} \cup \{[r] \mid r \in F, r \neq 0_F\}$$

$$= \{[r] \mid r \in F\} = F^*$$

The operations on $F[x]/(p)$ are defined in way such that F^* is a subring of $F[x]/(p)$.

The isomorphism $F \to F^*$
$a \mapsto [a]$

Remarks 1) If p is a constant polynomial meaning $p \in F$, $p \neq 0_F$, then we produce <u>one equivalence class</u>.

Every two polynomials are congruent modulo a unit $u \in F[x]$

$f \equiv g \pmod{u}$ means $u \mid (f-g)$ means $\underline{f-g = u \cdot h,\ h \in F[x]}$

$h = u^{-1}(f-g)$ $u^{-1} \in F[x]$

Thus (one still has to check that we again produce a ring) $F[x]/(p)$ in this case is a ring out of one element - zero ring.

2) If $p = 0_F$

$\underline{f \equiv g \pmod{0_F}}$ means $f - g = 0_F \cdot h = 0_F$ means $\underline{f = g}$

then every element in $F[x]$ belongs to its own equivalence class.

Thus $F[x]/(0_{F[x]}) \cong F[x]$ as rings

Recall: units in $\mathbb{Z}_n$: $\{[a] \mid (a,n) = 1\}$

Th 5.1 The units in $F[x]/(p)$: $\{[f] \mid (f,p) = 1_F\}$ (p - non-constant polynomial)

Remark: all non-zero constants $u \in F \subset F[x]/(p)$ are among the units.

In particular, the sum of two such units is again a unit (if non-zero) because F is field.

In contrast, in $\mathbb{Z}$, $1 \in \mathbb{Z}$ is a unit, while $1+1=2 \in \mathbb{Z}$ is not a unit.