Lecture 5: (1)

Assume F field and $p(x) \in F[x]$.

<u>Def</u>: We define $f(x), g(x) \in F[x]$ <u>congruent</u> modulo $p(x)$ and write $f(x) \equiv g(x) \pmod{p(x)}$ if $p(x) \mid (f(x)-g(x))$.

> **Theorem:**
> i) $f(x) \equiv f(x) \pmod{p(x)}$ for all $f(x) \in F[x]$ (reflexive)
>
> ii) $f(x) \equiv g(x) \pmod{p(x)} \Rightarrow g(x) \equiv f(x) \pmod{p(x)}$ (symmetric)
>
> iii) $\left.\begin{matrix} f(x) \equiv g(x) \pmod{p(x)} \\ g(x) \equiv h(x) \pmod{p(x)} \end{matrix}\right\} \Rightarrow f(x) \equiv h(x) \pmod{p(x)}$ (transitive)

<u>Proof</u>: Copy proof for $\mathbb{Z}$. □

- We define the <u>congruence class</u>

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

and the <u>set of all congruence classes</u> is written $F[x]/(p(x))$ (compare notation $\mathbb{Z}_n$). $F[x]/(p(x))$ constitute a <u>partition</u> of $F[x]$.

<u>Ex</u>: Consider $p(x) = x^2+x+1$ in $\mathbb{Z}_2[x]$ ($\mathbb{Z}_2$ is a field)

Take any $f(x) \in \mathbb{Z}_2[x]$. By polynomial division we get

$f(x) = q(x)p(x) + r(x)$, $\deg r(x) < \deg p(x)$ or $r(x) = 0$.

$\Rightarrow f(x) \equiv r(x) \pmod{p(x)}$ and it follows (as for $\mathbb{Z}$) that (2)

$[f(x)] = [r(x)]$.

The only residues $r(x)$ modulo $p(x)$ in $\mathbb{Z}_2[x]$ are $0, 1, x$ and $x+1$, so

$$\mathbb{Z}_2[x]/(x^2+x+1) = \{[0], [1], [x], [x+1]\}$$

<u>Note</u>: The classes $[r(x)]$ are <u>all different</u>. If $[r_1(x)] = [r_2(x)]$ with $\deg r_1(x), r_2(x) < \deg p(x)$, then $r_1(x) \equiv r_2(x) \pmod{p(x)}$

$\Rightarrow p(x) \mid \underbrace{(r_1(x) - r_2(x))}_{\deg < \deg p(x)} \Rightarrow r_1(x) = r_2(x)$

Therefore, <u>in general</u>,

$$F[x]/(p(x)) = \{ [r(x)] \mid \deg r(x) < \deg p(x) \text{ (or } r(x)=0) \}$$

<u>Ex</u>: $\mathbb{Z}_2[x]/(x^2+x+1) = \{[0],[1],[x],[x+1]\} = \mathbb{Z}_2[x]/(x^2)$

so <u>different polynomials</u> give <u>same classes</u>!

<u>Ex</u>: Assume $p(x) \in \mathbb{Z}_n[x]$, n <u>prime</u>, (Note: not written in the book) and $\deg p(x) = k$.

Then $\mathbb{Z}_n[x]/(p(x)) = \{ [a_{k-1}x^{k-1} + \cdots + a_1 x + a_0];\ a_i \in \mathbb{Z}_n \}$

has <u>n^k elements</u>.

We now want to turn $F[x]/(p(x))$ into a ring by introducing operations $+$ and $\cdot$:

(3)

$$[f(x)] + [g(x)] \overset{\text{def.}}{=} [f(x)+g(x)]$$
$$[f(x)] \cdot [g(x)] \overset{\text{def.}}{=} [f(x)g(x)]$$

These operations are well-defined (see theorem in book).

<u>Ex</u>: • In $\mathbb{Z}_2[x]/(x^2+x+1)$:

$x^2 \equiv x+1 \pmod{x^2+x+1}$ since $x^2-(x+1) \equiv x^2+x+1 \equiv 0 \pmod{x^2+x+1}$

This means $[x]\cdot[x] = [x^2] = [x+1]$

• In $\mathbb{Z}_2[x]/(x^2)$:

We have $[x]\cdot[x] = [x^2] = [0]$ $(\neq [x+1])$

<u>Ex</u>: In $\mathbb{Q}[x]/(x^3-2)$:

[redacted] $(2x^2+4x)(x^2-\frac{1}{4}) = 2x^4 + 4x^3 - \frac{1}{2}x^2 - x =$

pol. div.
$= (2x+4)(x^3-2) + (-\frac{1}{2}x^2 + 3x + 8)$

This means $[2x^2+4x]\cdot[x^2-\frac{1}{4}] = [-\frac{1}{2}x^2+3x+8]$

<u>Easier</u>: Since $x^3 \equiv 2$, ~~construct the rule $x^3 \to 2$~~ ~~("x^3 is replaced by 2") We get~~ we replace x^3 by 2:

$2x^4 + 4x^3 - \frac{1}{2}x^2 - x \equiv 2x\cdot 2 + 4\cdot 2 - \frac{1}{2}x^2 - x =$
$= -\frac{1}{2}x^2 + 3x + 8$

(4)

> **Theorem:** $F[x]/(p(x))$ is a commutative ring with identity.

<u>Proof</u>: Exercise. $[0]$ is zero, $[1]$ is unity. □

> **Theorem:** Let $\deg p(x) \geq 1$. Then $F[x]/(p(x))$ contains a subring F^* isomorphic to F.

<u>Proof</u>: (Idea: F^* corresponds to the elements $[a]$, $a \in F$)

We define the mapping $\varphi : F \to F[x]/(p(x))$ by $\varphi(a) = [a]$, $a \in F$. Now

$\varphi(a+b) = [a+b] = [a]+[b] = \varphi(a) + \varphi(b)$

and $\varphi(ab) = [ab] = [a][b] = \varphi(a)\varphi(b)$,

so φ <u>homomorphism</u>. Furthermore

φ is <u>injective</u> since $\varphi(a) = \varphi(b) \Leftrightarrow [a] = [b]$
$\Leftrightarrow a \equiv b \pmod{p(x)} \Leftrightarrow p(x) \mid a-b \Leftrightarrow a = b$,
since $\deg p(x) \geq 1$ but $a-b \in F$ (degree 0).

[redacted] Since φ homom., it follows that $F^* = \varphi(F)$ subring and that $\varphi : F \to F^*$ isomorphism. □

<u>Note</u>: We will identify F^* with F and say that $F[x]/(p(x))$ contains F.

The following theorem is analogous to the one for the case $\mathbb{Z}_p$, p prime:

> **Theorem:** The following are equivalent ($\deg p(x) \geq 1$)
>
> 1. $p(x)$ irreducible
> 2. $F[x]/(p(x))$ is a field
> 3. $F[x]/(p(x))$ is an integral domain

Proof: 1 $\Rightarrow$ 2: We want to show that every $[a(x)] \neq [0]$ has an inverse: $[a(x)] \neq [0] \Rightarrow p(x) \nmid a(x)$

$\Rightarrow (a(x), p(x)) = 1 \Rightarrow a(x)u(x) + p(x)v(x) = 1$ for some $u(x), v(x) \Rightarrow 1 \equiv a(x)u(x) \pmod{p(x)}$

$\Rightarrow [a(x)]\cdot[u(x)] = [1] \Rightarrow [a(x)]^{-1} = [u(x)]$.

2 $\Rightarrow$ 3: True since every field is an int. domain (earlier theorem)

3 $\Rightarrow$ 1: Assume the contrary, i.e. that

$p(x) = r(x)s(x)$ with $\deg r(x) \geq 1$ and $\deg s(x) \geq 1$.

This means $p(x) \nmid r(x)$ and $p(x) \nmid s(x)$, and thus that $[r(x)], [s(x)] \neq [0]$. Now

$[r(x)]\cdot[s(x)] = [r(x)s(x)] = [p(x)] = [0]$,

and since we have zero-divisors it cannot be an integral domain. Contradiction! □

Ex: We notice that $p(x) = x^3+4x+2 \in \mathbb{Z}_5[x]$ is irreducible (none of the elements 0,1,2,3,4 is a root. Check!), so by theorem it follows that $\mathbb{Z}_5[x]/(p(x))$ is a field.

Find the inverse of $[x^2+3x+1]$:

We solve the equation

$$u(x)(x^2+3x+1) + v(x)(x^3+4x+2) = 1 \quad \text{in } \mathbb{Z}_5[x]$$

by Euclid's alg. "backwards":

$$x^3+4x+2 = (x^2+3x+1)(x+2) + 2x$$

$$x^2+3x+1 = (3x+4)\cdot 2x + 1 \longleftarrow \text{GCD}$$

and thus

$$\begin{aligned}1 &= (x^2+3x+1) - (3x+4)2x = \\ &= (x^2+3x+1) - (3x+4)\big((x^3+4x+2) - (x^2+3x+1)(x+2)\big) = \\ &= \big(1 + (x+2)(3x+4)\big)(x^2+3x+1) - (3x+4)(x^3+4x+2) = \\ &= \underbrace{(3x^2+4)}_{=u(x)}(x^2+3x+1) \underbrace{-(3x+4)}_{=v(x)}(x^3+4x+2)\end{aligned}$$

We get $[3x^2+4]\cdot[x^2+3x+1] = [1]$

and that $[x^2+3x+1]^{-1} = [3x^2+4]$

Exercise: Check that $[3x^2+4]\cdot[x^2+3x+1] = [1]$

Note: $\mathbb{Z}_5$ in the above example is a subfield of the field $\mathbb{Z}_5[x]/(p(x)) = \mathbb{K}$, so $\mathbb{K}$ is an

extension field of $\mathbb{Z}_5$. Now consider $p(x)$ as a polynomial with coeff. in $\mathbb{K}$. Then it follows that $[x] \in \mathbb{K}$ is a root of $p(x)$:

$$p([x]) = [x]^3 + [4][x] + [2] = [x^3+4x+2] = [0]$$

This is a general property:

> **Theorem:** F field, $p(x)$ irreducible in $F[x]$. Then $F[x]/(p(x)) = K$ is an extension field of F containing a root of $p(x)$.

Proof: $[x]$ is a root of $p(x)$, since

$p([x]) = [p(x)] = [0]$ (compare note above). □

> **Corollary:** If $f(x) \in F[x]$, $\deg f(x) \geq 1$, then there exists an extension field K of F containing a root of $f(x)$.

Proof: Let $p(x)$ be an irreducible factor of $f(x)$ and construct $K = F[x]/(p(x))$.

Since $f(x) = p(x)g(x)$, we get

$$f([x]) = p([x])g([x]) \underset{\text{by proof above}}{=} [0]\cdot g([x]) = [0]. \quad \square$$

Ex: $p(x) = x^2+1$ is irreducible in $\mathbb{R}[x]$ (has no roots in $\mathbb{R}$)

We want to extend $\mathbb{R}$ to a field where we can solve $x^2+1=0$.

By theorem above $K = \mathbb{R}[x]/(x^2+1)$ works!

What is K? We note that the elements of K are $[a+bx]$, $a,b \in \mathbb{R}$, since $p(x)$ has degree 2.

Furthermore

$$[a+bx] + [c+dx] = [(a+c)+(b+d)x]$$

and

$$\begin{aligned}[a+bx]\cdot[c+dx] &= [(a+bx)(c+dx)] = \\ &= [ac + (ad+bc)x + bdx^2] \overset{x^2 \equiv -1 \pmod{x^2+1}}{=} \\ &= [(ac-bd) + (ad+bc)x]\end{aligned}$$

Looks similar to $\mathbb{C}$. In fact $K \cong \mathbb{C}$ via the isomorphism $\varphi([a+bx]) = a+bi$.