(1) 4/27/2020

D - an integral domain

F - field of fractions

$a/b \in F \quad a/b = c/d \Leftrightarrow ad = bc$

<u>Thm</u> Let D be domain with field of fractions F. If E is a field that contains D, then there is 1-to-1 ring homomorphism $\varphi: F \to E$ s/t $\varphi(a/1) = a \in E$.

<u>Pf</u>: For $a \in D$: $\varphi(a/1) = a \in E$

$$\varphi(a/b) = \varphi(a)\varphi(b)^{-1} = ab^{-1}$$

Well-defined: $a/b = c/d \therefore ad = bc$

$$\Downarrow \text{ in } E$$

$$ab^{-1} = cd^{-1}$$

$$\begin{aligned} \varphi(a/b) &= ab^{-1} \in E \\ &= cd^{-1} \\ &= \varphi(c)\varphi(d)^{-1} \\ &= \varphi(c/d) \end{aligned}$$

φ is a ring homo'sm.

$$\varphi(a/b) = \varphi(c/d) \Rightarrow \varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1}$$

$$\Rightarrow ab^{-1} = cd^{-1} \Rightarrow ad = bc \text{ in } D \;\square$$

(2)

Cor Let D be an integral domain. Every field that contains D contains the field of fractions of D.

Ex $D = \mathbb{Z}$, $F = \mathbb{Q}$

$\mathbb{Z} \subseteq \mathbb{R}$ $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

~~Thm~~ Recall: char $D = 0$ if $n \cdot 1 \neq 0$ for all $n \in \mathbb{N}$. and char $D = n$ if $n \cdot 1 = 0$ and n is the least number with that property. I.e. char $D = |1|$ in $\langle D, + \rangle$.

Thm: Let D be an integral domain. If char $D = 0$, then there is a ~~such~~ subdomain $D' \subseteq D$ with $D \cong \mathbb{Z}$. If char $D = p$, then $D' \subseteq D$ with $D' \cong \mathbb{Z}_p$.

(3) Let $1'$ be the mult. identity in D

$\varphi: \mathbb{Z} \to D$

$\varphi(n) = n \cdot 1'$

is a ring homo'sm:

$$\varphi(n+m) = (n+m)\cdot 1' = n\cdot 1' + m\cdot 1' = \varphi(n) + \varphi(m)$$

$$\varphi(nm) = (nm)\cdot 1' = (n\cdot 1')(m\cdot 1') = \varphi(n)\varphi(m)$$

$$D' = \varphi(\mathbb{Z}) = \{m\cdot 1' \mid m \in \mathbb{Z}\}$$

If $\operatorname{char} D = 0$, then $\operatorname{Ker}\varphi = \{0\}$

First Iso Thm:

$$\begin{array}{ccc} \mathbb{Z}/\operatorname{Ker}\varphi & \cong & \varphi(\mathbb{Z}) \\ \parallel & & \parallel \\ \mathbb{Z} & & D' \end{array}$$

If $\operatorname{char} D = p$, then

~~Ker pZ~~ $\operatorname{Ker}\varphi = p\mathbb{Z} = \langle p \rangle$

$$\begin{array}{ccc} \mathbb{Z}/\langle p\rangle & \cong & \varphi(\mathbb{Z}) \\ \parallel & & \parallel \\ \mathbb{Z}_p & & D' \end{array}$$

④ <u>Cor</u> Let E be a field.
If char $E = 0$, then $\mathbb{Q}$ is a subfield of E.
If char $E = p$, then $\mathbb{Z}_p$ is a subfield of E.

<u>Pf</u> E is a domain, so contains $\mathbb{Z}$ or $\mathbb{Z}_p$ and hence the corresponding field of fractions. □

$\mathbb{Q}$ and $\mathbb{Z}_p$ are called prime fields.

—— x ——

Find the zeros of x^2+x+1

In $\mathbb{R}$ there are none

In $\mathbb{Z}_3$ there is 1: $(x-1)^2 = x^2-2x+1$
$= x^2+x+1$

In $\mathbb{Z}_7$ – – 2: $(x-4)(x-2) =$
$x^2-6x+8 =$
x^2+x+1

(5)

Def Let R be a ring. A poly with coefficients in R is an expression

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{where } a_i \in R$$

$$= a_n x^n + a_{n-1} x^{n-1} + \dots + \underset{\underset{a_1 x}{\parallel}}{a_1 x^1} + \underset{\underset{a_0}{\parallel}}{a_0 x^0}$$

If $a_i = 0$ $\forall i$, then $f(x)$ is called the 0-polynomial (zero-poly).

If $f(x)$ is not the zero-polynomial, then the degree of f is $\max\{i \mid a_i \neq 0\}$ i.e. ~~given by~~ the

* largest term.

The function $R \to R$ given by

$f(r) = a_n r^n + a_{n-1} r^{n-1} + \dots + a_1 r + a_0$

is called the polynomial function $f(x)$.

Over $\mathbb{Z}_2$ $\quad f(x) = x+1$ and

$g(x) = x^2 + 1$

$h(x) = x^3 + 1$

determine same function but different as polynomials.

(6) <u>Def</u> Let R be a ring. For poly.

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{and} \quad g(x) = \sum_{i=0}^{m} b_i x^i$$

set

$$f(x) + g(x) = \sum_{i=0}^{\max(m,n)} c_i x^i \; : \; c_i = a_i + b_i$$

$$f(x) g(x) = \sum_{i=0}^{n+m} d_i x^i \; : \; d_i = \sum_{k=0}^{i} a_k b_{i-k}$$

$$= a_0 b_i + a_1 b_{i-1} \cdots a_i b_0$$

<u>Ex</u> $f(x) = 2x^2 - x + 7$ $\quad g(x) = 5x^3 + x + 1$

$a_2 = 2$ $\quad b_3 = 5$

$a_1 = -1$ $\quad b_2 = 0$

$a_0 = 7$ $\quad b_1 = 1$

$b_0 = 1$

$$d_3 = 7(5) + (-1)0 + 2(1) + 0(5)$$

$$= 35 + 2$$

$$= 37$$

$$(2x^2 - x + 7)(5x^3 + x + 1) =$$

$$\cdots + (35+2)x^3 + \cdots \qquad + 7$$