Integral Domains & The Field of Quotients

What is an Integral Domain: A commutative ring w/ unity and no zero divisors.

Examples: $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$

"integer like" domain

Recall: Characteristic of a commutative ring R with unity is the smallest $n \in \mathbb{N}$ s.t. $\forall a \in R$ $n \cdot a = \underbrace{a+a+\dots+a}_{n\text{-times}} = 0$

If no such value exists, we say the characteristic of $R = 0$.

$\forall a \in R$, $|a|_+ \mid \text{char}(R)$

$\boxed{\text{Thm}}$ $\forall a \neq 0 \in D$ $|a|_+ = \text{char}(D)$ for integral domain D

$\boxed{\text{Proof}}$ Sps. for some $a \neq 0$, $|a|_+ = m < \underbrace{\text{char}(D)}_{n}$

$\Rightarrow m \cdot a = \underbrace{a + a + \dots + a}_{m} = 0$

$\underbrace{1a + 1a + 1a + \dots 1a}_{m} = \underbrace{(1+1+\dots+1)}_{m} a = \underbrace{(m \cdot 1)}_{=0} a = 0$

$\Rightarrow \forall x \in D$ $\quad m \cdot x = (m \cdot 1)x = 0x = 0$

$\Rightarrow \text{char}(D) = m \quad \Rightarrow \Leftarrow$

$\boxed{\text{Thm}}$ In an ID D, char(D) is either 0 or prime.

$\boxed{\text{Thm}}$ Every finite ID is actually a field.

$\boxed{\text{Proof}}$ Let D be an arbitrary finite ID

$D = \{0, 1, a_1, a_2, \dots, a_n\}$ $\leftarrow n+2$ elements in D.

Let a_i be an arbitrary non-zero element of D

Consider $a_iD = \{a_i0, a_i1, \dots, a_ia_n\}$ $\leftarrow$ $n+2$ distinct elements of D

Since otherwise $a_ia_j = a_ia_k \Rightarrow a_ia_j - a_ia_k = 0$

$a_i(a_j - a_k) = 0 \Rightarrow \Leftarrow$

$1 \in a_iD \Rightarrow \exists\, a_j \in D$ s.t. $a_ia_j = 1$

$\Rightarrow a_i$ has a mult. inverse $\Rightarrow D$ is a field.

$\boxed{\text{Thm}}$ Every commutative ring w/ unity contains a subring $\cong \mathbb{Z}$ or $\mathbb{Z}_n$ $\leftarrow$ (Zee subring Thm)

$\boxed{\text{Proof}}$ Let R be an arb. comm. ring w/ unity

Consider $\phi: \mathbb{Z} \to R$ defined as $\phi(z) = z \cdot 1$ $\forall z \in \mathbb{Z}$.

NTS: ϕ is a ring homomorphism

Let a, b be $\in \mathbb{Z}$, $\phi(a+b) = (a+b)\cdot 1 = \underbrace{1+1+\dots+1}_{a+b} = \underbrace{(1+1+\dots+1)}_{a} + \underbrace{(1+1+\dots+1)}_{b}$

$= (a \cdot 1) + (b \cdot 1)$

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

$\varphi(ab) = \left.\begin{array}{l} \overbrace{1 + 1 + 1 + \dots + 1}^{a} \\ + 1 + 1 + 1 + \dots + 1 \\ \vdots \\ + 1 + 1 + \dots + 1 \end{array}\right\} b = \underbrace{(1+1+\dots+1)}_{a}(b \cdot 1) = (a \cdot 1)(b \cdot 1)$

$= \varphi(a)\varphi(b)$

φ is a ring homomorphism. $\therefore$ By the 1st isomorphism thm for rings

$\mathbb{Z}/\text{Ker}\,\varphi \cong \varphi(\mathbb{Z}) \subseteq R$

What is the $\text{Ker}\,\varphi$?

if char$(R) = n \Rightarrow \text{Ker}\,\varphi = \langle n \rangle$

if char$(R) = 0 \Rightarrow \text{Ker}\,\varphi = \{0\}$

$\varphi(\mathbb{Z}) \cong \mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$

$\varphi(\mathbb{Z}) \cong \mathbb{Z}/\{0\} = \mathbb{Z}$

What if R is a field?

$\Rightarrow F$ has a subring $\cong \underset{\text{field}}{\mathbb{Z}_p}$ or $\underset{\mathbb{Q}}{\mathbb{Z}}$

$\boxed{\text{Thm}}$ (Steinitz) Every field F contains a subfield $\cong$ to $\mathbb{Z}_p$ for some prime $p = \text{char}(F)$ or to $\mathbb{Q}$ if char$(F) = 0$

corollary

$\boxed{\text{Proof}}$ By Z-subring thm $\Rightarrow F$ contains a subring $S \cong \mathbb{Z}$. (ψ)

Construct $T = \{ab^{-1} \mid a, b \in S, \text{ and } b \neq 0\}$

• Prove T is well-defined & a subring of F. (2-step subring test)

Let x, y be $\in T$ $\Rightarrow x = a_1b_1^{-1}$ and $y = a_2b_2^{-1}$ for $a_1, a_2 \in S$, $b_1, b_2 \in S$ & $\neq 0$.

$x - y = a_1b_1^{-1} - a_2b_2^{-1}$

$= a_1b_1^{-1}b_2b_2^{-1} - a_2b_2^{-1}b_1b_1^{-1}$

$= (a_1b_2 - a_2b_1)(b_1^{-1}b_2^{-1})$

$= \underbrace{(a_1b_2 - a_2b_1)}_{\in S}\underbrace{(b_2b_1)}_{S}^{-1} \in T$ Know $b_2b_1 \neq 0$ since $b_1 \neq 0 \neq b_2$ no zero divisors

$xy = (a_1b_1^{-1})(a_2b_2^{-1})$

$= (a_1a_2)(b_1b_2)^{-1} \in T$

T is a subring of F

Define the map $\psi': T \to \mathbb{Q}$ by

$\psi'(t) = \psi'(ab^{-1}) = \psi(a)\psi(b)^{-1}$ $\forall t = ab^{-1} \in T$ by defn of T $a, b \in S$

NTS: ① ψ' is a ring homomorphism ✓

② ψ' is a bijection ✓

① Let x, y be $\in T$, as before $x = a_1b_1^{-1}$ $y = a_2b_2^{-1}$

$\psi'(x+y) = \psi'(a_1b_1^{-1} + a_2b_2^{-1}) = \psi'((a_1b_2 + a_2b_1)(b_1b_2)^{-1})$

$= \psi(a_1b_2 + a_2b_1)\psi(b_1b_2)^{-1}$

$= (\psi(a_1)\psi(b_2) + \psi(a_2)\psi(b_1))\psi(b_2)^{-1}\psi(b_1)^{-1}$

$= \psi(a_1)\psi(b_1)^{-1} + \psi(a_2)\psi(b_2)^{-1} = \psi'(x)\psi'(y)$

$\psi'(xy) = \psi'(a_1b_1^{-1}a_2b_2^{-1}) = \psi'(a_1a_2(b_1b_2)^{-1}) = \psi(a_1a_2)\psi(b_1b_2)^{-1}$

$= \psi(a_1)\psi(a_2)\psi(b_1)^{-1}\psi(b_2)^{-1} = \psi(a_1)\psi(b_1)^{-1}\psi(a_2)\psi(b_2)^{-1} = \psi'(x)\psi'(y)$

② ψ' is a bij.

Let x be $\in \text{Ker}\,\psi'$ $\Rightarrow \psi'(x) = \psi'(ab^{-1})$

$= \psi(a)\cancel{\psi(b)^{-1}}^{\neq 0} = 0$

$\Rightarrow \psi(a) = 0 \Rightarrow a = 0$ (ψ is the isomorphism from $S \to \mathbb{Z}$)

$x = 0b^{-1} = 0 \Rightarrow \text{Ker}\,\psi' = \{0\}$

ψ' is 1-1

Let $\frac{m}{n}$ be $\in \mathbb{Q} \Rightarrow m, n \in \mathbb{Z}$, $n \neq 0$

$\exists\, a, b \in S$ s.t. $\psi(a) = m$, $\psi(b) = n$

since $n \neq 0 \Rightarrow b \neq 0$ $\therefore ab^{-1} \in T$ s.t. $\psi'(ab^{-1}) = \frac{m}{n}$ $\therefore$ onto