HW 7

① There exists no integral domain A of order 6

Interlude #1

Let F be a finite field, $|F| < \infty$, F is a field

$$\phi : \mathbb{Z} \longrightarrow F \quad \begin{matrix} 1 \\ -1 \\ 0 \end{matrix}$$

$$1 \longmapsto 1$$

$$\left[\begin{array}{l} n \longmapsto \underbrace{1+1+\cdots+1}_{n\text{-times}} \\ 0 \longmapsto 0 \\ -n \longmapsto \underbrace{-1-1\cdots-1}_{n\text{-times}} \end{array}\right]$$

$ab = 0$
$\Rightarrow a = 0$ or $b = 0$

$*$ $$\underbrace{\mathbb{Z}/\ker\phi}_{\text{integral domain}} \cong \operatorname{im}\phi \leq \underset{\text{field}}{F}$$

$\left[\begin{array}{c} a \in F\setminus\{0\},\ \exists b \in F\setminus\{0\} \text{ st} \\ ab = ba = 1 \end{array}\right]$

$cd = 0$

$\left[d = c^{-1}cd = 0 \right]$

$\ker\phi$ is a prime ideal in $\mathbb{Z}$ $\Rightarrow$ $\ker\phi = (p)$, p prime

* F is a field, hence an integral domain
* $\operatorname{im}\phi$, as a subring of F, is then also an integral domain
* $\mathbb{Z}/\ker\phi$, since isomorphic to $\operatorname{im}\phi$, is also an integral domain
* Hence $\ker\phi$ is a prime ideal in $\mathbb{Z}$
* Thus $\ker\phi = (p)$, for a prime p
* $\operatorname{im}\phi \cong \mathbb{Z}/\ker\phi = \mathbb{Z}/p\mathbb{Z}$; $\operatorname{im}\phi = \mathbb{F}_p$

Hence F is a field extension of $\mathbb{F}_p$

* F | $\mathbb{F}_p$ then F can be seen as an $\mathbb{F}_p$-vector space

  → finite-dimensional $\mathbb{F}_p$-vector space, since F is finite

  $\dim_{\mathbb{F}_p} F = n$; there's a basis $\{e_1, \dots, e_n\}$

$x = a_1e_1 + \cdots + a_ne_n$ $\quad a_i \in \mathbb{F}_p$.

$p \quad p \quad p \quad = p^n$

$x \in F \cong \mathbb{F}_p^n$

$x = (a_1, \dots, a_n)$ $\quad p \quad p \quad p$

$a_i \in \mathbb{F}_p$

$\boxed{\# F = p^n}$ (prime power!)

$\boxed{\text{If } F \text{ is a finite field, then } \# F = \text{prime-power}}$ //

$\mathbb{F}_3^2$ $\qquad$ $(\underset{3}{a}, \underset{3}{b})$ $\qquad$ $(0, 0), (0, 1), (0, 2)$; $(1, 0), (1, 1), (1, 2)$; $(2, 0), (2, 1), (2, 2)$ $\qquad$ $\boxed{3^2 = 9}$

Interlude #2

Finite integral domains are fields. //

[So if A was an integral domain, then A being finite would then be a field. But! Finite fields have order as a prime power. 6 not a prime power, Contradiction! A is not an integral domain]

So, let A be a finite integral domain. To conclude its a field, we need to show that for every $a \in A \setminus \{0\}$, $\exists\, b \in A$ st $ab = ba = 1$

Start w/ $a \in A \setminus \{0\}$ consider the

$$\begin{aligned} \phi_a : A &\longrightarrow A \\ x &\longmapsto ax \end{aligned}$$

This is a grp hmph: $\phi_a(x+y) = a(x+y) = ax + ay = \phi_a(x) + \phi_a(y)$

ϕ_a is injective $\Leftrightarrow$ $\ker \phi_a = \{0\}$.

$x \in \ker \phi_a$, then $ax = \phi_a(x) = 0$

But A is an integral domain, so $\boxed{\cancel{a=0}}$ or $x=0$

Hence $x=0$, so ϕ_a is injective.

$$\phi_a : A^{dom} \longrightarrow A^{cod}$$

so $A^{dom} \longleftrightarrow \underbrace{\phi_a(A^{dom})} \leq A^{cod}$

$\# \phi_a(A^{dom}) = \# A^{dom} = \# A^{cod}$ (only works b/c these are finite sets)

$\Rightarrow \phi_a(A^{dom}) = A^{cod}$

$\Rightarrow \phi_a$ is surjective!

* $\phi_a : A \longrightarrow A$

For $1 \in A$, $\exists b \in A$ st $\phi_a(b) = 1 \Rightarrow ab = 1 \Rightarrow a \in A^\times$

Hence $A \setminus \{0\} = A^\times$, so A is a field.