Hw 3 Solution

§5.1 #7

u a unit $a^n = 1$. Say $uv = 1$, i.e. $v = u^{-1}$

$$1 = (u-a)(v + av^2 + \cancel{+}a^2v^3 + \cdots + a^n v^{n+1})$$

$\therefore$ $(u-a)$ is a unit, $(u-a)^{-1} = v + av^2 + a^2v^3 + \cdots + a^n v^{n+1}$

§5.2 #3

$\varphi : F \to E$ ring hom, F, E fields, φ onto.

$\ker\varphi$ is an ideal of F.

An ideal containing a unit contains 1, hence everything

$\therefore$ Either $\ker\varphi = \{0\}$, so φ is 1-1 and onto, hence an iso

Or $\ker\varphi = F$ when $\varphi(1) = 0 \neq 1$ $\#$ $\varphi(1) = 1$ ...

$\therefore$ φ is an iso

#11

R, S non-zero rings. $R \times S$ is not an integral domain:

$$(1,0)\cdot(0,1) = (0,0)$$

non-zero zero divisors!

§ 5.3 # 12(a)(b)

(a) Let $N = \{\text{nilpotents}\}$

Closed under + : if $a, b \in N$ then $a^n = 0$, $b^m = 0$

$\therefore (a+b)^{m+n} = \sum_{j=0}^{m+n} \binom{m+n}{j} a^j b^{m+n-j}$

either $j \geq n$ when $a^j = 0$

or $j < n$ when $m+n-j > m$
so $b^{m+n-j} = 0$

$\therefore RHS = 0$

$\therefore a+b$ is nilpotent ✓

Contain 0 ✓

Extra-closed under · : if $a \in N$, $b \in R$ then $a^n = 0$

so $(ab)^n = a^n b^n = 0$ so $ab \in N$ ✓

(b) Say $x + N \in R/N$ is nilpotent.

Then $(x+N)^n = 0$ some $n > 0$

$\therefore x^n + N = 0$

$\therefore x^n \in N$

$\therefore x^n = y$ some $y \in N$. Choose k so $y^k = 0$

Then $(x^n)^k = x^{nk} = y^k = 0$ $\therefore$ x is nilpotent

$\therefore x \in N$ $\therefore$ $x + N = 0$ ← shows: R/N has no non-zero nilpotents.

§5.3 #13

(a) $I+J$ is an ideal:

Closed under $+$ ✓

Extra-closed under $\cdot$: Take $i \in I$, $j \in J$, $r \in R$.

Then $r(i+j) = ri + rj \in I+J$ as $ri \in I$, & $rj \in J$ ✓

Contains 0: $0 = 0+0$ ✓

(b) $n\mathbb{Z} + m\mathbb{Z} = \langle m,n \rangle$

Let $d = GCD(m,n) = sm + tn$.

Then $d \in \langle m,n \rangle$ so $\langle d \rangle \subseteq \langle m,n \rangle$

Also $m \in \langle d \rangle$, $n \in \langle d \rangle$, so $\langle m,n \rangle \subseteq \langle d \rangle$

$\therefore \langle m,n \rangle = \langle GCD(m,n) \rangle$

#17

$R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a,b,c,d \in \mathbb{Q},\ a=d,\ c=0 \right\} = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \right\}$

(a) $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\begin{bmatrix} a' & b' \\ 0 & a' \end{bmatrix} = \begin{bmatrix} aa' & ab'+ba' \\ 0 & aa' \end{bmatrix} = \begin{bmatrix} a' & b' \\ 0 & a' \end{bmatrix}\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$ ✓ commutative

Other axioms easy as 2×2 matrices form a (non-commutative) ring.

(b) $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\begin{bmatrix} 0 & c \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & ac \\ 0 & 0 \end{bmatrix}$ ✓ It's an ideal

(c) Map $R \to \mathbb{Q}$ $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mapsto a$ is additive, multiplicative, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mapsto 1$ $\therefore$ A homomorphism.

It's surjective. Kernel $= I$. So $R/I \cong \mathbb{Q}$ by 1st $\cong$ theorem

§5.3 #21

$m+ni \in \langle 1+2i \rangle$

$\iff$ $m+ni = (1+2i)(a+bi) = (a-2b) + i(2a+b)$ for some $a, b \in \mathbb{Z}$

$\therefore$ $\left.\begin{aligned} m &= a-2b \\ n &= 2a+b \end{aligned}\right\}$ for $a, b \in \mathbb{Z}$

$\therefore$ $\left.\begin{aligned} m+2n &= 5a \\ n-2m &= 5b \end{aligned}\right\}$

$\therefore$ $m+2n$ and $n-2m$ are integers divisible by 5.

Conversely, if $m+2n = 5a$, $n-2m = 5b$

then $\left.\begin{aligned} m &= a-2b \\ n &= 2a+b \end{aligned}\right\}$

$\therefore$ $(m+ni) = (1+2i)(a+bi)$ $\therefore$ $m+ni \in \langle 1+2i \rangle$

So: nec & suff conditions are: $\boxed{m+2n \text{ and } n-2m \text{ are integer multiples of } 5}$

$$\begin{aligned} \langle 1+2i \rangle \cap \mathbb{Z} &= \{ m \in \mathbb{Z} \mid m+2\cdot 0 \text{ and } 0-2m \text{ are mult of } 5 \} \\ &= \{ m \in \mathbb{Z} \mid m \text{ is a mult of } 5 \} \\ &= \langle 5 \rangle \end{aligned}$$

My Question

Consider $\varphi : \mathbb{Z} \to \mathbb{Z}[i]/\langle 5-i \rangle$

$n \mapsto n + \langle 5-i \rangle$

Kernel? its a principle ideal, $\langle d \rangle$ say

$26 \mapsto 26 + \langle 5-i \rangle = 0$ as $(5-i)(5+i) = 26$

$\therefore d \mid 26$

13? no $\delta(13) = 169$

2? Does $5-i \mid 2$? no $\delta(5-i) = 26$ $\delta(2) = 4$

$26 \nmid 4$

1? no.

$26 \nmid 169$

$\therefore$ kernel $= \langle 26 \rangle$

$\therefore \operatorname{Im}\varphi \cong \mathbb{Z}_{26}$

What is $\left| \mathbb{Z}[i]/\langle 5-i \rangle \right|$? If its ≤ 26, done.

as $i \equiv 5 \pmod{5-i}$

can represent cosets by $n + \langle 5-i \rangle$ $n \in \mathbb{Z}$

as $26 \equiv 0$ get just $0, 1, \ldots, 25$

as representatives

So $|\cdot| \leq 26$ ✓

this ends, so $\mathbb{Z}_{26} \cong \mathbb{Z}[i]/\langle 5-i \rangle$