HW1 Solutions

Sec. 18 : #12

$F = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field.

<u>proof</u> It is closed under addition & multi. & additive & multi. inverse.

Take $a+b\sqrt{2}$ & $c+d\sqrt{2} \in F$, then:

$$(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2} \in F$$

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2} \in F$$

$$-(a+b\sqrt{2}) = (-a) + (-b)\sqrt{2} \in F$$

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2} \in F$$

(because $\mathbb{Q}$ is a field.)

Also $1 = 1 + 0\sqrt{2} \in F$, and F is Commutative because $F \subset \mathbb{R}$ and $\mathbb{R}$ is Commutative. So F is a field, in fact a subfield of $\mathbb{R}$.

#24

Let $\phi : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ be a (ring) homo$\overline{\text{ism}}$.

Let $\phi(1) = (a, b)$. Then $\forall n \overset{n>0}{\in} \mathbb{Z}$, $n = \underbrace{1 + \cdots + 1}_{n \text{ times}}$, so

$\phi(n) = \phi(1) + \cdots + \phi(1) = (na, nb)$. Similarly for $n \leq 0$ we have

$\phi(n) = (na, nb)$. It follows that any homo$\underline{\text{ism}}$ from $\mathbb{Z}$ to $\mathbb{Z} \times \mathbb{Z}$ is determined by $\phi(1) = (a,b)$. In other words, any homo$\underline{\text{ism}}$ $\phi: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ is of the form $\phi(n) = (na, nb)$ for some $(a,b) \in \mathbb{Z} \times \mathbb{Z}$. But $\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$. This implies that $\phi(1) = (a,b) = (a^2, b^2)$. Hence $a = 0$ or 1 and $b = 0$ or 1. Thus $\phi(1) = (0,0), (0,1), (1,0)$ or $(1,1)$ and $\phi(n) = (0,0), (0,n), (n,0)$ or (n,n), i.e. 4 possible homomorphisms.

$\forall a, b \in R$

#38 $(a+b)(a-b) = a^2 + ba + a(-b) + b(-b)$

$= a^2 + ba - ab - b^2$.

Now, $a^2 + ba - ab - b^2 = a^2 - b^2 \iff ba - ab = 0 \iff ab = ba$, i.e. R commutative.

55

$\forall a \in R$, $(a+a) = (a+a)^2 = (a+a)(a+a) = a^2 + a^2 + a^2 + a^2$

$= a + a + a + a \implies 0 = a + a$, or $a = -a$. $(\star)$

Now, $\forall a, b \in R$ consider :

$(a+b) = (a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2 = a + ab + ba + b$

Canceling $a+b$, we get $0 = ab + ba \implies ab = -ba$.

But by $(\star)$, $-ba = ba$ & hence $ab = ba$ as required.

Sec. 19 #10

Let $n =$ char. of $\mathbb{Z}_6 \times \mathbb{Z}_{15}$. Then n is the smallest pos. number that $n \cdot (1,1) = (0,0)$, i.e. $n \equiv 0 \mod 6$ and $n \equiv 0 \mod 15$,

i.e. n is the least common multiple of 6 and 15 $= 30$.

#14

Since $\det \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} = 0$ we can find a non-zero sol. for $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$

Namely, $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 \\ -1 \end{bmatrix}$. Then $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} 2 & 2 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

#26

a) Suppose $a \neq 0$ and $ac = 0$ for some $c \in R$.

Let b be the unique element with $aba = a$ but then $a(b+c)a = aba + aca = aba = a$, which contradicts uniqueness of b unless $c = 0$. Similarly, if $ca = 0$ we show $c = 0$. Hence R has no zero divisors, and thus has cancellation property (for multi.).

b) Consider $aba = a \Rightarrow baba = ba \Rightarrow bab = b$ (by cancelling a).

c) Fix a, b with $aba = a$ (& hence $bab = b$). We show that $e=ba$ is unity, i.e. $\forall c \in R$ we have:

$$\left.\begin{aligned} &aba=a \Longrightarrow abac=ac \Longrightarrow (ba)c=c. \\ \text{Also, } \quad &bab=b \Longrightarrow cbab=cb \Longrightarrow c(ba)=c. \end{aligned}\right\} (\star)$$

d) Finally, we show that $\forall c \in R$ has multi. inverse.

Let d be s.t. $cdc=c$ & $dcd=d$.

We will show $cd=dc=e$:

$cdc=c \Longrightarrow cdcba=cba \Longrightarrow dcba=ba$. But $e=ba$

is unity (by $(\star)$), so $dc\underbrace{ba}_{e}=dc$ i.e. $dc=e$.

Similarly, using $dcd=d$ we show $cd=e$ as required.

#29

By Contradiction,

Suppose char $= mn$ is not prime.

Then $(m\cdot 1)(n\cdot 1)=(mn)\cdot 1=0$. Since D is int. domain either $m\cdot 1=0$ or $n\cdot 1=0$ which contradicts that $c=mn$ is the smallest number with $c\cdot 1=0$.