SOLUTIONS TO LECTURE 23 PROBLEMS 85 – 90:

P85 # 19 of pg. 235

Let R be a ring. The center of R is the set $H = \{x \in R \mid ax = xa \ \forall a \in R\}$. Prove the center H is subring of R

Notice $a(0) = 0(a) \ \forall a \in R \ \therefore \ 0 \in H \neq \emptyset$.

Let $a, b \in H$ then $ax = xa$ and $bx = xb \ \forall x \in R$.

Observe, $(a-b)x = ax - bx = xa - xb = x(a-b) \ \forall x \in R$.

Also, $(ab)x = a(bx) = a(xb) = (ax)b = x(ab) \ \forall x \in R$.

Thus by the subring test we find $\underbrace{H = \{a \in R \mid ax = xa \ \forall x \in R\}}$ is a subring of R.

Remark: sorry I swapped notation of x & a here. I hope you see this does not change the logic.

P86 # 22 of pg. 236

Let R be commutative ring with unity and $U(R) = \{x \in R \mid \exists y \in R \text{ with } xy = 1 \text{ and } yx = 1\}$

Prove $U(R)$ is a group under multiplication of R

Notice $1 \cdot 1 = 1$ thus $1 \in U(R)$ provided R is commutative ring with unity 1. We find $U(R) \neq \emptyset$. Let $a, b \in U(R)$ hence $\exists x, y \in R$ for which $ax = 1$ and $by = 1$. Hence $x, y \in U(R)$.

Thus $x = a^{-1} \in U(R)$ so $U(R)$ is closed under inversion.

Moreover, $(ab)^{-1} = b^{-1}a^{-1}$ we are thus inspired to consider $(ab)(yx) = a(by)x = a(1)x = ax = 1 \ \therefore \ ab \in U(R)$.

Finally since R is ring multiplication is associative. In summary, $U(R)$ has a closed, associative multiplication with identity 1 and inverses.

P86 comment:

I was about to apply a subgroup test for $U(R)$ but, it hit me,... subgroup of what??

The sol^{n} is not that $U(R)$ is a subgroup, rather, it has multiplication which is associative, binary, with identity, closed under inversion. In addition, $U(R)$ is abelian since R was assumed commutative.

P87 # 23 pg. 237 Determine $U(\mathbb{Z}[i])$ where $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$

That is, find the group of units in the Gaussian Integers

Find all sol^{n}'s of $(a+bi)(x+iy) = 1$

$$\Rightarrow a+bi = \frac{1}{x+iy} = \frac{x-iy}{x^2+y^2} \quad \text{believe it!}$$

Thus, $a = \dfrac{x}{x^2+y^2}$ and $b = \dfrac{-y}{x^2+y^2}$ where $a, b, x, y \in \mathbb{Z}$.

We find $x^2+y^2 = 1$ and $a = x$ and $b = -y$. If $x = 0$ then $y^2 = 1 \Rightarrow y = \pm 1$ $\therefore$ $b = \mp 1$. If $x = 1$ then $1+y^2 = 1$ $\therefore$ $y^2 = 0 \Rightarrow y = 0$, likewise $x = -1 \Rightarrow y = 0$

Thus $x = \pm 1$ and $a = \pm 1$ where $b = -y = 0$. In summary, $\boxed{U(\mathbb{Z}[i]) = \{1, -1, i, -i\}}$

$\boxed{P88}$ # 40 from pg. 237

Let $R = \left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} \,\middle|\, a, b \in \mathbb{Z} \right\}$. Prove or disprove R subring of $\mathbb{Z}^{2\times 2}$

Well, $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$ is good.

Also, $\begin{bmatrix} a & a \\ b & b \end{bmatrix} + \begin{bmatrix} x & x \\ y & y \end{bmatrix} = \begin{bmatrix} a+x & a+x \\ b+y & b+y \end{bmatrix}$ shows R closed under $+$.

Consider, $\begin{bmatrix} a & a \\ b & b \end{bmatrix}\begin{bmatrix} x & x \\ y & y \end{bmatrix} = \left[\begin{array}{c|c} ax + ay & ax + ay \\ \hline bx + by & bx + by \end{array}\right]$ thus R closed under multiplication.

Of course, I should have checked subtraction,

if $\begin{bmatrix} a & a \\ b & b \end{bmatrix}, \begin{bmatrix} x & x \\ y & y \end{bmatrix} \in R$ then $\begin{bmatrix} a & a \\ b & b \end{bmatrix} - \begin{bmatrix} x & x \\ y & y \end{bmatrix} = \left[\begin{array}{c|c} a-x & a-x \\ \hline b-y & b-y \end{array}\right] \in R$

and we've also shown $\begin{bmatrix} a & a \\ b & b \end{bmatrix}\begin{bmatrix} x & x \\ y & y \end{bmatrix} = \left[\begin{array}{c|c} ax+ay & ax+ay \\ \hline bx+by & bx+by \end{array}\right] \in R$

hence as $R \neq \phi$ we find by subring test that R is subring of $\mathbb{Z}^{2\times 2}$.

$\boxed{P89}$ # 43, pg. 237 Let R be ring with unity 1.

Show that $S = \{ n \cdot 1 \mid n \in \mathbb{Z} \}$ is a subring of R

Note that $0 \cdot 1 = 0 \in S \therefore S \neq \phi$. Suppose

$x, y \in S$ then $\exists\, m, n \in \mathbb{Z}$ s.t. $x = m \cdot 1$ and $y = n \cdot 1$

hence $x - y = m \cdot 1 - n \cdot 1 = (m-n) \cdot 1$ by Lemma ①

thus $x - y = (m-n) \cdot 1 \in S$ as $m - n \in \mathbb{Z}$.

Likewise, $xy = (m \cdot 1)(n \cdot 1) = (mn) \cdot 1$ (by # 15 on p. 235)

thus $xy = (mn) \cdot 1 \in S$ as $mn \in \mathbb{Z}$.

Therefore, S is a subring of R by subring test. //

Lemma ①: $(m \cdot 1) - (n \cdot 1) = (m-n) \cdot 1$

proof

Lemma ①: $(m\cdot 1)-(n\cdot 1) = (m-n)\cdot 1$ for $m,n \in \mathbb{Z}$

Proof: if $m,n>0$ in $\mathbb{Z}$ then,

$$m\cdot 1 = \underbrace{1+1+1+\cdots+1}_{m-\text{fold}} \qquad n\cdot 1 = \underbrace{1+1+\cdots+1}_{n-\text{fold}}$$

$$\therefore (m\cdot 1)-(n\cdot 1) = (\underbrace{1+1+\cdots+1}_{m\text{-copies}}) - (\underbrace{1+1+\cdots+1}_{n\text{-copies}}) = (m-n)\cdot 1.$$

where $(m-n)\cdot 1 = \begin{cases} 1+1+\cdots+1 & : m-n>0 \\ 0 & : m=n \\ -1-1-\cdots-1 & : m-n<0 \end{cases}$

Continuing, if $m>0$ and $n<0$ then

$$m\cdot 1 = \sum_{j=1}^{m} 1 \quad \text{and} \quad n\cdot 1 = \sum_{l=1}^{-n}(-1)$$

thus $(m\cdot 1)-(n\cdot 1) = \sum_{j=1}^{m} 1 - \sum_{l=1}^{-n}(-1) = \underbrace{1+1+\cdots+1}_{m} + \underbrace{1+\cdots+1}_{-n}$

again, $(m\cdot 1)-(n\cdot 1) = (m+(-n))\cdot 1 = (m-n)\cdot 1.$

Similar annoying arguments can be given for the $m<0$, $n>0$ and $m<0, n<0$ cases. I think I've shown enough.

P90 # 48 from pg. 237

Suppose R is ring with $a^2 = a$ for all $a \in R$. Show that R is commutative.

Notice $(-a)(-a) = a^2$ thus $-a = a$ for each $a \in R$.

However, $(a+b)(a+b) = a^2 + ab + ba + b^2 \quad \forall a, b \in R$.

Thus, $(a+b)^2 = a+b \Rightarrow a^2 + ab + ba + b^2 = a+b$

and as $a^2 = a$ and $b^2 = b \Rightarrow a + ab + ba + b = a + b$

Hence $ab + ba = 0 \quad \forall a, b \in R$. Or,

$ab = -ba = ba \quad \forall a, b \in R$ using $b = -b$

as we proved at the outset. Thus R is commutative.

Again, but, less

<u>Proof</u>: since $(-a)(-a) = a^2$ we find $-a = a$ from $x^2 = x$ for each $x \in R$. Continuing, if $a, b \in R$ then,

$$\begin{aligned}
(a+b)^2 = a+b &\Rightarrow (a+b)(a+b) = a+b \\
&\Rightarrow a^2 + ab + ba + b^2 = a+b \\
&\Rightarrow a + ab + ba + b = a+b \\
&\Rightarrow ab + ba = 0 \\
&\Rightarrow ab = -ba = ba.
\end{aligned}$$

Thus $ab = ba \quad \forall a, b \in R$ and we find R commutative.//