PMATH 347 Groups and Rings, Solutions to the Exercises for Chapter 11

1: (a) Find all the units in $\mathbb{Z}\left[\frac{1}{2}+\frac{\sqrt{3}}{2}i\right]$.

Solution: It helps to draw a picture of $\mathbb{Z}\left[\frac{1}{2}+\frac{\sqrt{3}}{2}i\right]=\left\{k+l(\frac{1}{2}+\frac{\sqrt{3}}{2}i)\middle|k,l\in\mathbb{Z}\right\}$. Let a be a unit in $\mathbb{Z}\left[\frac{1}{2}+\frac{\sqrt{3}}{2}i\right]$, say $ab=1$. Then $|a||b|=|ab|=1$. Since there are no elements $b\in\mathbb{Z}\left[\frac{1}{2}+\frac{\sqrt{3}}{2}i\right]$ with $0<|b|<1$, we see that $|a|=1$. The only elements a in $\mathbb{Z}\left[\frac{1}{2}+\frac{\sqrt{3}}{2}i\right]$ with $|a|=1$ are $a=\pm1$ and $a=\pm\frac{1}{2}\pm\frac{\sqrt{3}}{2}i$, and all 6 of these are units.

(b) Find 10 units in $\mathbb{Z}[\sqrt{3}]$.

Solution: Recall that $a=k+l\sqrt{3}$ is a unit in $\mathbb{Z}[\sqrt{3}]$ when $N(a)=|k^2-3l^2|=1$. We easily see that $a=\pm1$ and $a=\pm2\pm\sqrt{3}$ are units. One can find more units by trial and error. A nicer way is to note that if a is a unit in a commutative ring, then so is a^n for $n\in\mathbb{Z}_+$ since $ab=1\Longrightarrow a^nb^n=1$. In this way we obtain infinitely many units. For example, $(2+\sqrt{3})^2=7+4\sqrt{3}$ is another unit as are the elements $\pm7\pm4\sqrt{3}$.

2: Determine which of the following elements are irreducible in $\mathbb{Z}[\sqrt{3}\,i]$.

(a) $3+2\sqrt{3}\,i$

Solution: Let $a=3+2\sqrt{3}\,i$. Then $N(a)=21$, so if $a=bc$ where b and c are not units then we may suppose $N(b)=3$ and $N(c)=7$, that is $|b|=\sqrt{3}$ and $|c|=\sqrt{7}$. A picture of $\mathbb{Z}[\sqrt{3}\,i]$ shows that $b=\pm\sqrt{3}$ and $c=\pm2\pm\sqrt{3}\,i$. And indeed we can take $b=\sqrt{3}\,i$ and $c=2-\sqrt{3}\,i$ to get $a=bc$, so a is reducible.

(b) $2+3\sqrt{3}\,i$

Solution: $N(2+3\sqrt{3}\,i)=31$ which is prime, so $2+3\sqrt{3}\,i$ is irreducible.

(c) 5

Solution: $N(5)=25$, so if $5=bc$ where b and c are not units then $N(b)=N(c)=5$, that is $|b|=|c|=5$. A picture of $\mathbb{Z}[\sqrt{3}\,i]$ shows that there are no such elements b,c, so 5 is irreducible.

(d) 7

Solution: $N(7)=49$, so if $7=bc$ where b and c are not units then $|b|=|c|=\sqrt{7}$. A picture shows that $b,c=\pm2\pm\sqrt{3}\,i$. Indeed, we can take $b=2-\sqrt{3}\,i$ and $c=2+\sqrt{3}\,i$ and we have $bc=7$. So 7 is reducible.

3: (a) Show that $2+\sqrt{5}\,i$ is irreducible but not prime in $\mathbb{Z}[\sqrt{5}\,i]$.

Solution: Let $a=2+\sqrt{5}\,i$. Then $N(a)=9$. If $a=bc$ where b and c are not units, then $N(b)=N(c)=9$ and so $|b|=|c|=3$. A picture of $\mathbb{Z}[\sqrt{5}\,i]$ shows that the only possible values of b and c are ±3 so we cannot have $bc=a$. Thus a is irreducible. On the other hand, a is prime because $a(2-\sqrt{5}\,i)=9=3\cdot3$ so a divides $3\cdot3$ but a does not divide 3 in $\mathbb{Z}[\sqrt{5}\,i]$ (since $a/3\notin\mathbb{Z}[\sqrt{5}\,i]$).

(b) Draw a picture of each of the ideals $\langle2\rangle$, $\langle1+\sqrt{3}\,i\rangle$ and $\langle2,1+\sqrt{3}\,i\rangle$ in $\mathbb{Z}[\sqrt{3}\,i]$.

Solution: We have $\langle2\rangle=\left\{2(k+l\sqrt{3}\,i)\middle|k,l\in\mathbb{Z}\right\}=\left\{k(2)+l(2\sqrt{3}\,i)\middle|k,l\in\mathbb{Z}\right\}=\mathrm{Span}_{\mathbb{Z}}\left\{\begin{pmatrix}2\\0\end{pmatrix},\begin{pmatrix}0\\2\sqrt{3}\end{pmatrix}\right\}$, and
$\langle1+\sqrt{3}\,i\rangle=\left\{(1+\sqrt{3}\,i)(k+l\sqrt{3}\,i)\middle|k,l\in\mathbb{Z}\right\}=\left\{k(1+\sqrt{3}\,i)+l(-3+\sqrt{3}\,i)\middle|k,l\in\mathbb{Z}\right\}=\mathrm{Span}_{\mathbb{Z}}\left\{\begin{pmatrix}1\\\sqrt{3}\end{pmatrix},\begin{pmatrix}-3\\\sqrt{3}\end{pmatrix}\right\}$.
Let $I=\langle2,1+\sqrt{3}\,i\rangle$. Since $2\in I$ and $1+\sqrt{3}\in I$ and I is closed under $+$, we must have $J\subset I$ where $J=\left\{k(2)+l(1+\sqrt{3}\,i)\middle|k,l\in\mathbb{Z}\right\}=\mathrm{Span}_{\mathbb{Z}}\left\{\begin{pmatrix}2\\0\end{pmatrix},\begin{pmatrix}1\\\sqrt{3}\end{pmatrix}\right\}$. This set J is an ideal since it is closed under multiplication by elements of the ring: $\big(k(2)+l(1+\sqrt{3}\,i)\big)(m+n\sqrt{3}\,i)=km2+ln\sqrt{3}\,i-3ln=(km-2ln)(2)+ln(1+\sqrt{3}\,i)$. Thus $I=J$.

4: (a) Determine whether the set $\left\{\begin{pmatrix}2&1\\3&1\end{pmatrix},\begin{pmatrix}4&1\\1&2\end{pmatrix},\begin{pmatrix}3&1\\2&4\end{pmatrix}\right\}$ is linearly independent in $M_2(\mathbb{Z}_5)$.

Solution: Row reduce $\begin{pmatrix}2&4&3\\1&1&1\\3&1&2\\1&2&4\end{pmatrix}$ over $\mathbb{Z}_5$ to get $\begin{pmatrix}1&0&3\\0&1&3\\0&0&0\\0&0&0\end{pmatrix}$. The last column has no pivot, so they are not linearly independent; indeed from the reduced matrix we see that $\begin{pmatrix}3&1\\2&4\end{pmatrix}=3\begin{pmatrix}2&1\\3&1\end{pmatrix}+3\begin{pmatrix}4&1\\1&2\end{pmatrix}$.

(b) Find the line of intersection of the planes $x+3y+z=1$ and $2x+y+4z=1$ in $(\mathbb{Z}_5)^3$.

Solution: Row reduce $\left(\begin{array}{ccc|c}1&3&1&1\\2&1&4&1\end{array}\right)$ over $\mathbb{Z}_5$ to get $\left(\begin{array}{ccc|c}1&3&0&4\\0&0&1&2\end{array}\right)$. Thus $\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}4\\0\\2\end{pmatrix}+t\begin{pmatrix}2\\1\\0\end{pmatrix}$.

(c) How many invertible matrices are there in $M_2(\mathbb{Z}_2)$?

Solution: The first row can be any row other than (0,0), so there are 3 choices for the first row. The second row cannot be in the line spanned by the first row, so there are 2 choices for the second row. This gives 6 invertible matrices.