MAT 3530: Sample Solutions to Assignment 5
More About Rings!

Charles Delman

March 7, 2012

1 The Group of Units in a Ring

3. Prove that in any ring R, -1 is a unit.

   Proof. We simply need to check that -1 has a multiplicative inverse; in fact, it is its own multiplicative inverse, since $(-1)(-1) = -(-1)$, by the result of the previous problem, and $-(-1) = 1$, since $-1 + 1 = 0$. $\square$

   Remark. In other words, regarding the last step, 1 is the multiplicative inverse of -1 – symbolically, $-(-1)$ – because it does the right thing operationally, and this is the case because -1 is, by definition, the additive inverse of 1. Additive inverses come in pairs: x is the additive inverse of y if and only if y is the additive inverse of x. You can look at it, $x + y = 0$ either way.

7. (a) Prove that $z \in \mathbb{Z}[i]$ is a unit if and only if $|z| = 1$.

   We begin by establishing that $|wz| = |w||z|$, which is true in general for complex numbers:

   Lemma. *For any complex numbers w and z, $|wz| = |w||z|$.*

   Proof. We have established that, for any complex number w, $w\bar{w} = |w|^2$. We have also established that $\overline{wz} = \bar{w}\bar{z}$. Thus $|wz|^2 = wz\overline{wz} = wz\bar{w}\bar{z} = w\bar{w}z\bar{z} = |w|^2|z|^2$. Taking the positive square root of both sides we obtain the result. $\square$

   Now we complete the problem by proving that $z \in \mathbb{Z}[i]$ is a unit if and only if $|z| = 1$.

   Proof. First suppose that z is a unit; then there is an element $z^{-1} \in \mathbb{Z}[i]$ such that $zz^{-1} = 1$. It follows from the lemma just proven that $|z|\,|z^{-1}| = |1| = 1$. Since the only divisors of 1 are ± 1 and $|z|$ is by definition positive, $|z| = 1$. (Observe that this calculation also shows directly that $|z^{-1}| = 1$, but of course this fact follows from the result anyway, since z^{-1} is also a unit if z is.)

Conversely, suppose $|z| = 1$, and let $z = a + bi$ (where a and b are integers). This is only possible if $|z|^2 = a^2 + b^2 = 1$, which in turn is only possible if $a = \pm 1$ and $b = 0$ or if $a = 0$ and $b = \pm 1$. Thus the only possibilities are ± 1 and $\pm i$. It is easily checked that these elements are all units. $\square$

(b) Using the result above, identify all of the units of $\mathbb{Z}[i]$. (There are four of them.)

The answer to this question should now be obvious!

8. Given a ring R, define a relation on R as follows: $r \sim_L s \Leftrightarrow (\exists u \in U) ur = s$.

   (c) What are the equivalence classes, with respect to this relation, of 0, 1, 2, and $2 + 3i$ for $R = \mathbb{Z}[i]$?

   $[0] = \{0\}$, since any multiple of 0 is 0 in any ring. $[1] = \{1, -1, i, -i\}$. $[2] = \{2, -2, 2i, -2i\}$. $[2 + 3i] = \{2 + 3i, -2 - 3i, 3 - 2i, -3 + 2i\}$.

9. Given a ring R, define a relation on R as follows: $r \sim_R s \Leftrightarrow (\exists u \in U) ru = s$.

   (b) If R is commutative, then the relations $\sim_L$ and $\sim_R$ are clearly the same (since $ur = ru$), but note that if R is not commutative, then they are different. As an example, prove that the equivalence classes of the matrix $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbb{Z})$ with respect to these two equivalence relations are different.

   Any matrix equivalent to $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ with respect to $\sim_L$ would have the form

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix}.$$

   Any matrix equivalent to $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ with respect to $\sim_R$ would have the form

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}.$$

   Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be any invertible element of $M_2(\mathbb{Z})$ such that $b \neq 0$; $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is an example. Since $b \neq 0$, the matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$$

   cannot be equivalent to $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ with respect to $\sim_L$. (A similar argument can be made using an invertible matrix whose lower left entry is not 0, such as $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. Both $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ are elements of $SL_2(\mathbb{Z})$, as you can easily check.)