MAT 3530: Assignment 5
More About Rings!

Charles Delman

March 7, 2012

Due at the beginning of class on Monday, March 5.

1 The Group of Units in a Ring

Let $(R, +, \cdot)$ be a ring with unit element 1; we will refer to this ring simply as R for short (although technically R just denotes the set of elements in the ring), and we will refer to its two operations as addition and multiplication, respectively. In general, the set R does not form a group under the multiplication operation. Although there is an identity element for this operation, it is possible that not every element has a multiplicative inverse. In fact, very few elements may have inverses; for example, in the ring of integers, only ± 1 do.

If we restrict our set to those elements of R that do have inverses, however, we obtain a group under multiplication. Note that if the multiplication operation is not commutative, then left and right inverses can be different; when we say an element has an inverse we mean a two-sided inverse. Thus, let $U = \{u \in R : (\exists v \in R)uv = vu = 1\}$. As you will recall, two-sided inverses are unique, so we are justified in denoting the inverse of an element u by u^{-1}. The elements of U are called *units*; do not confuse them with the unit *element*, 1 (which is itself always a unit, but not generally the only one). If $U = R - \{0\}$, that is, if every non-zero element is invertible, then R is called a *field* if it is commutative and a *division ring* or *skew field* if it is not.

Two show that $(U, \cdot)$ is a group, we must show four things:

- Multiplication is an associative operation on U. This is obvious, since it is associative as an operation on the whole ring R.
- $1 \in U$. This is clear as well, since 1 is its own multiplicative inverse: $1 \cdot 1 = 1$.
- If $u \in U$ and $v \in U$, then $uv \in U$. (This result shows that multiplication defines a binary operation on U; that is, if the inputs of multiplication are restricted to elements of U, then the output is an element of U.)
- If $u \in U$, then $u^{-1} \in U$. (This result shows that every element of U has an inverse in U with respect to the operation. You might ask why there is anything to prove, since U is precisely the set of elements of R that have inverses! The point is that not only does u^{-1} exist, but u^{-1} is itself a unit. That it is should be fairly obvious, since u and u^{-1} are *inverses of each other*.)

1. The following steps complete the verification that U is a group by proving the last two items.

   (a) Prove that U is closed under multiplication: if $u \in U$ and $v \in U$, then $uv \in U$. (Hint: construct the inverse of uv by combining u^{-1} and v^{-1} in a suitable fashion. Make clear why associativity of multiplication is important to verifying that the element you constructed is indeed the inverse - both on left and right - of uv.)

   (b) Prove that U is closed under inversion: if $u \in U$, then $u^{-1} \in U$. (Hint: as indicated above, this is very quick and easy! What is the inverse of u^{-1}?)

2. Prove that in any ring R, $(-1)r = -r$ for any $r \in R$. (Hint: the same proof that works for the real numbers works in general, since rings satisfy the distributive property. It is important in mathematics to recognize the most general context in which a proof is valid.)

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

4. Prove that the group of units is closed under *additive* inverses: if u is a unit, then $-u$ is a unit.

As an example, the units in the matrix group $M_2(\mathbb{Z})$ of 2×2 matrices with integer entries are the invertible matrices. This group is called $GL_2(\mathbb{Z}$. ("GL" stands for *general linear*. Recall that in order to be invertible, the determinant of the matrix, which is an integer if the entries are integers, must be invertible. The matrices with determinant 1, as opposed to -1, form a subgroup denoted $SL_2(\mathbb{Z})$, where "SL" stands for *special linear*.)

From linear algebra you should be familiar with $M_2(\mathbb{R})$, the 2×2 matrices with real entries. (In general, we most commonly work with matrices whose entries are in a field, because they represent linear maps of vector spaces over that field. Instead of considering real matrices we could just consider rational matrices. The point is to be able to divide.) You can think of the units of $M_2(\mathbb{Z})$ as those matrices that are invertible as real matrices and whose inverses have integer entries. You may recall from linear algebra that a matrix with real coefficients is invertible if and only if its determinant is not zero. You can easily check that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix}$$

Since $D = ad - bc = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$, the determinant of matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, it is clear that the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ exists if and only if $D \neq 0$, in which case it is $\begin{bmatrix} \frac{d}{D} & \frac{-b}{D} \\ \frac{-c}{D} & \frac{a}{D} \end{bmatrix}$. Since a, b, c, and d are integers, the inverse has integer values exactly when $D = \pm 1$. In summary,

$$GL_2(\mathbb{Z}) = \{M \in M_2(\mathbb{Z}) : |M| = \pm 1\}$$

.

In other words, it is the group of matrices whose determinants are units in the ring of integers.

Another way to see that a matrix with entries in a ring is invertible only if its determinant is invertible is the general result that $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \begin{vmatrix} e & f \\ g & h \end{vmatrix} = \left| \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right|$. However, to prove the converse requires the inversion formula.

As another example, consider the Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, which is a subring of the complex number field. Addition and multiplication are determined by the commutativity of addition, the distributive law, and the rule that $i^2 = -1$: thus, $(a + bi) + (c + di) = (a + c) + (b + d)i$, and $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$. It is clear that the result in each case belongs to $\mathbb{Z}[i]$ (since the integers are closed under multiplication, addition, and subtraction).

5. Consider the ring of matrices $M_2(R)$ with entries in a *commutative* ring R.

   (a) Verify that
   $$\begin{vmatrix} a & b \\ c & d \end{vmatrix} \begin{vmatrix} e & f \\ g & h \end{vmatrix} = \left| \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right|.$$
   (You have undoubtedly done this in linear algebra, but you should remember how to do it! In addition, we are generalizing to the context that the entries are in a commutative ring, not necessarily a field. The same proof works.)

   (b) Verify that
   $$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad - bc & 0 \\ 0 & ad - bc \end{bmatrix}$$

   In both parts, be sure to indicate where the commutativity of R is needed.

6. The following steps verify that $\mathbb{Z}[i]$ is a commutative ring.

   (a) Check that addition in $\mathbb{Z}[i]$ is associative and commutative.

   (b) Check that $0 = 0 + 0i$ is the additive identity.

   (c) Check that multiplication in $\mathbb{Z}[i]$ is associative and commutative.

   (d) Check that $1 = 1 + 0i$ is the multiplicative identity.

   (e) Check that the distributive law holds in $\mathbb{Z}[i]$.

7. To determine the units in $\mathbb{Z}[i]$, it is once again helpful to pass to a larger ring in which we can divide, namely $\mathbb{C}$, the field of complex numbers. As I expect you remember, a complex number has the form $z = a + bi$, where a and b can be any real numbers; addition and multiplication are extended in the obvious way (and the proofs you gave of the properties above do not depend on a and b being integers). You can easily check that $(a + bi)(a - bi) = a^2 + b^2$. The complex number $a - bi$ is called the *conjugate* of $a + bi$ and denoted by $\bar{z}$. The quantity $\sqrt{a^2 + b^2}$ is just the distance of the vector (a, b) from the origin $(0, 0)$, so if $z = a + bi$ it is natural to denote $a^2 + b^2$ by $|z|^2$. Thus we can summarize what we have so far as $z\bar{z} = |z|^2$.

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

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

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

   (a) Prove that $\sim_L$ is an equivalence relation.

   (b) As an example, what are the equivalence classes, with respect to this relation, of 0, 1, 2, and -4 for $R = \mathbb{Z}$? (Denote the equivalence class of r by $[r]$.)

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

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

   (a) Prove that this is an equivalence relation.

   (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. (Hint: Where are the zero entries when you multiply by this matrix on the right? On the left?)

2 Domains and Integral Domains

Definition. A ring R is a *domain* if, for any $a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$. (Note that the converse is always true, thanks to the distributive law.) If R is also commutative, it is called an *integral domain*.

1. Prove that if R is a field or division ring (that is, if $U = R \setminus \{0\}$, where U is the group of units of R), then R is a domain.

2. Prove that if R is a subring of a field or division ring, then R is a domain.

In the remaining sections of this assignment, we will restrict our attention to commutative rings. Although this will exclude matrix rings, many important rings are not only commutative but also integral domains. For example, it comes as no surprise that $\mathbb{Z}$ is an integral domain! So is any field or subring thereof (as you proved above, since any subring of a commutative ring is clearly commutative); in particular, the ring of Gaussian integers is also an integral domain. So is any ring of polynomials with coefficients in an integral domain.

3. Prove that if R is a domain, then $R[x]$ is a domain. (Hint: Use an argument about the highest degree term of the product to reduce to the case that both factors are constants; then use the hypothesis.)

4. Prove that if R is commutative, then $R[x]$ is commutative.