Homework Assignment 12

Due Saturday, April 30

1. Let R be a ring. Recall that for $a \in R$ we denote the *additive* inverse of a by $-a$. Establish the following identities.

   (a) $(-a)b = a(-b) = -ab$

   Proof. We'd like to prove that $(-a)b$ is the additive inverse of ab. It suffices (by HW2 problem 7) to show that $(-a)b + ab = 0$. Applying the distributive law:

   $$(-a)b + ab = (-a + a)b = 0b = 0.$$

   Similarly, we observe that:

   $$a(-b) + ab = a(-b + b) = a0 = a.$$

   These together give the result. □

   (b) $(-a)(-b) = ab$

   Proof. By part (a), we compute:

   $$(-a)(-b) = -((a)(-b)) = -(-ab) = ab.$$

   For the last step we use that in any group, the inverse of the inverse of an element is itself. □

   (c) If $1 \in R$ then $(-1)a = -a$.

   Proof. This follows immediately from part (a) and the fact that 1 is the multiplicative identity:

   $$(-1)a = -(1a) = -a.$$

   □

   (d) Suppose R is an integral domain. Show that if $a^2 = 1$ then $a = \pm 1$. (*Recall* A ring is an integral domain if it is commutative, with multiplicative identity $1 \neq 0$, and such that if $ab = 0$ then $a = 0$ or $b = 0$

   Proof. Notice that factoring (or FOILing) is just applying the distributive law twice. Therefore, since $a^2 - 1 = 0$ so we can factor to get:

   $$(a - 1)(a + 1) = 0.$$

   Since R is an integral domain, it has no zero divisors, so that either $a-1 = 0$ or $a+1 = 0$. In the first case $a = 1$ and in the second $a = -1$. □

2. Let R be a ring with $1 \neq 0$.

   (a) Let $R^\times \subseteq R$ be the set of units of R. Show that $R^\times$ is a group under the multiplication operation of R.

Proof. We first show that multiplication is a well defined group operation on $R^\times$. This means that if $r, s \in R^\times$, we must show their product is too. Since r is a unit, there exists $r^{-1} \in R$ such that $rr^{-1} = r^{-1}r = 1$, and similarly for s. Then we see that $s^{-1}r^{-1}$ is an inverse for rs. Indeed:

$$(rs)(s^{-1}r^{-1}) = r1r^{-1} = 1 \quad \text{and} \quad (s^{-1}r^{-1})rs = s^{-1}1s = 1.$$

Therefore $rs \in R^\times$ and so multiplication is well defined. Multiplication in $R^\times$ is associative by the ring axioms. The multiplicative identity $1 \in R$ is a unit (indeed, its inverse is 1), so $R^\times$ has an identity. To see that inverses exists, observe that if $r \in R^\times$, then so is r^{-1} (its inverse is r). □

(b) Suppose that $a \in R$ is a zero divisor. Show that $a \notin R^\times$.

Proof. We prove the contrapositive. Let $a \in R^\times$, so that there there exists some (two-sided) multiplicative inverse a^{-1} to a. If $ab = 0$ then we can multiply on the left by a^{-1} and se that

$$b = a^{-1}ab = a^{-1}0 = 0.$$

Therefore $b = 0$. Similarly, if $ba = 0$ we can multiply on the right by a^{-1} to observe that $b = 0$. In either case, we have seen that we cannot multiply a by anything nonzero and get 0, so a is not a zero divisor. □

3. Let R be a commutative ring. An element $r \in R$ is called *nilpotent* if there exists a positive n such that $r^n = 0$. A commutative ring is called *reduced* if it has no nonzero nilpotent elements.

(a) Show that a nilpotent element of a ring is either 0 or a zero divisor.

Proof. If $a \neq 0$ is nilpotent, then $a^n = 0$ for some n. In fact, one can let n be the minimal number with this property, so that $a^{n-1} \neq 0$. Then $aa^{n-1} = 0$ but both $a, a^{n-1} \neq 0$, so a is a zero divisor. □

(b) Give an example of a ring with a nonzero nilpotent element.

Proof. Consider $3 \in \mathbb{Z}/9\mathbb{Z}$. It is nonzero but $3^2 = 9 \equiv 0 \mod 3$. More generally one can find nilpotents in $\mathbb{Z}/n\mathbb{Z}$ for any n that is not square free.

Another example is in the matrix ring $M_2(F)$ for a field F. Once can consider the nonzero matrix

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

and easily observe that its square is 0. □

(c) Show that the sum of nilpotent elements is nilpotent.

Proof. We first observe that if $a^n = 0$, then $a^r = 0$ for any $r \geq n$. Indeed,

$$a^r = a^n a^{r-n} = 0a^{r-n} = 0$$

Now suppose a and b are nilpotent. So $a^n = 0$ and $b^m = 0$. Fix any $r > 2\max(m, n)$. Then by the binomial formula:

$$(a+b)^r = \sum_{i=0}^{r} \binom{r}{i} a^i b^{r-i}.$$

Notice that for each i one of i or $r-i$ is $\geq r/2 > \max(m, n) \geq m, n$, so that either $a^i = 0$ or else $b^{r-i} = 0$. Since this is true for each i, this shows $(a+b)^r = 0$ as desired.

We remark that the binomial formula holds for arbitrary rings. Indeed, it is just a direct consequence of the distributive law, together with the fact that the underlying abelian group under $+$ is commutative, allowing one to count how many of each term appear (for example, using Pascal's triangle) to get the right coefficients. One could (and probably should) prove this more formally by induction, but I won't require it for this problem. □

(d) Suppose r is nilpotent. Show that rx is nilpotent for all $x \in R$. (*Note*, in future terminology, (c) and (d) prove that the set of nilpotent elements is an *ideal* of R, which we will call the *nilradical*).

Proof. Suppose $r^n = 0$. Since R is commutative, then $(rx)^n = r^n x^n = 0x^n = 0$. □

(e) Suppose R is a commutative ring with $1 \neq 0$, and suppose $r \in R$ is nilpotent. Show that $1 + r \in R^\times$.

Proof. Suppose $r^n = 0$. Define an element $s \in R$ as the sum:

$$s = 1 - r + r^2 - r^3 + \cdots + (-1)^{n-1} r^{n-1}.$$

Then we compute (the telescoping sum):

$$(1+r)(1 - r + r^2 - r^3 + \cdots + (-1)^{n-1} r^{n-1}) \quad = \quad 1 + (-1)^{n-1} r^n = 1.$$

As R is commutative, this shows that $(1+r)^{-1} = s$ so it is a unit. □

4. Let R be ring, and X any set. Define

$$\mathrm{Maps}(X, R) = \{f : X \to R \mid f \text{ is a function}\}.$$

Define binary operations $+$ and $\times$ as follows.

$$(f+g)(x) = f(x) + g(x) \qquad (f \times g)(x) = f(x)g(x).$$

(a) Show that $\mathrm{Maps}(X, R)$ is a ring.

Proof. We first must show it is an abelian group. Let $\mathbf{0} : X \to R$ be the function that takes every element to 0, that is, $\mathbf{0}(x) = 0 \in R$ for all $x \in X$. Then for every $f \in \text{Maps}(X, R)$, and $x \in X$, we have

$$(\mathbf{0} + f)(x) = \mathbf{0}(x) + f(x) = f(x) = f(x) + \mathbf{0}(x) = (f + \mathbf{0}(x)). \tag{1}$$

Therefore $\mathbf{0}$ is an additive identity. We next show associativity. Associativity in $\text{Maps}(X, R)$ follows from that in R. Indeed: for any $f, g, h \in \text{Maps}(X, R)$ and $x \in X$ we compute:

$$((f + g) + h)(x) = (f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x)) = (f + (g + h))(x). \tag{2}$$

Since this holds for each x, we obtain associativity. To see that inverses exist, given f we define $-f$ by the rule $(-f)(x) = -f(x)$ (where the latter is the additive inverse of $f(x)$ in R). Then it is clear that

$$(f + (-f))(x) = f(x) - f(x) = 0 = \mathbf{0}(x).$$

We similarly observe that $-f + f = \mathbf{0}$. Finally, the additive structure is abelian because the addive structure on R is. Indeed, given $f, g \in \text{Maps}(X, R)$, we know that for each $x \in X$:

$$f(x) + g(x) = g(x) + f(x) \tag{3}$$

We now must consider the multiplicative structure. We first observe associativity, arguing exactly as in Equation (2), but with $+$ replaced by $\times$. Finally, the distributive law follows from that in R. Indeed, for each $f, g, h \in \text{Maps}(X, R)$, and $x \in X$:

$$(f(g + h))(x) = f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x) = (fg + fh)(x).$$

Distributivity on the other side follows identically. I will point out that I probably went into more detail than is strictly necessary. One needs only observe that each of the ring axioms can be checked after evaluating at an arbitrary point x, and that the hold there because they hold in R. Nevertheless, as parts (e) and (f) below indicate, one must be careful in considering which properties can be checked after evaluating at a point. (One could phrase this as saying some properties are local while others are global.) □

(b) Suppose R is commutative, show that $\text{Maps}(X, R)$ is too.

Proof. Whether 2 functions f and g commute can be checked after evaluating at an arbitrary point x, whence the result follows arguing as in Equation (3), but with $+$ replaced by $\times$. □

(c) Suppose R is unital, show that $\text{Maps}(X, R)$ is too.

Proof. Define the function $\mathbf{1} : X \to R$ by the rle $\mathbf{1}(x) = 1$ for all $x \in X$ (where 1 is the additive identity of R). Then one checks that $\mathbf{1}f = f\mathbf{1} = f$ for all $f \in \text{Maps}(X, R)$ after evaluating at an arbitrary $x \in X$, whence the result follows arguing as in Equation 1 replacing $\mathbf{0}$ with $\mathbf{1}$ and $+$ with $\times$ respectively. □

(d) Suppose R is reduced (defined in Problem 3), show that $\text{Maps}(X, R)$ is too.

Proof. Suppose f is a nilpotent element of $\text{Maps}(X, R)$, so that $f^n = \mathbf{0}$ for some positive integer n. Then for any x, we have $f(x)^n = 0$. Since R is reduced, its only nilpotent element is 0, so that $f(x) = 0$. Since x was arbitrary, this shows that $f = \mathbf{0}$ to begin with. Therefore the only nilpotent element of $\text{Maps}(X, R)$ is the zero map, proving that it is reduced. □

(e) Give an example to show that even if R is a field, $\text{Maps}(X, R)$ need not be.

Proof. The important observation is that if $f : X \to R$ is any function, and $f(x) = 0$ for any x, then f cannot be a unit in $\text{Maps}(X, R)$. Indeed, if f had an inverse g, then $fg = \mathbf{1}$ implies that $f(x)g(x) = 1$, but since $f(x) = 0$, this isn't possible. Therefore any nonzero function which is has a zero is an example of a nonunit. In particular, if X is any set with more than one element, then $\text{Maps}(X, R)$ is not a field, as we can construct f by the rule $f(x) = 0$ for a fixed $x \in X$, and $f(y) = 1$ for all $y \neq x$, and it won't be a unit. □

(f) Give an example to show that even if R is an integral domain, $\text{Maps}(X, R)$ need not be.

Proof. The idea of the proof is the same as part (e). Namely, that a function can be "locally zero" (ie, evaluate to 0 at some points) but not "globally zero" (ie, the 0 function). Indeed, fix $f, g : X \to R$. If $fg = \mathbf{0}$, then this says that $f(x)g(x) = 0$ for all $x \in X$. Since R is an integral domain, then either $f(x) = 0$ or $g(x) = 0$. The important observation is that f can be 0 at some points, and g can be 0 at other points, so that neither has to be the 0 function.

The simplest concrete example is the following. Let $X = \{x, y\}$ be a 2 point set, and R any integral domain. Then define f, g by the rules:

$$\begin{aligned} f(x) &= 0 & g(x) &= 1 \\ f(y) &= 1 & g(y) &= 0. \end{aligned}$$

Then it is clear that neither f or g are 0, but their product is at both x and y, so that $fg = \mathbf{0}$. □

5. Let A be an abelian group (with binary operation $+$). Define the *endomorphism ring* of A as follows:

$$\text{End}(A) = \{f : A \to A \mid f \text{ is a homomorpism}\}.$$

Give $\text{End}(A)$ 2 binary operations $+$ and $\times$ as follows:

$$(f + g)(a) = f(a) + g(a) \qquad (f \times g)(a) = f(g(a)).$$

(a) Prove that $\text{End}(A)$ is a ring.

Proof. We first show that $\text{End}(A)$ is an abelian group under $+$. This follows essentially identically to the computation in 4(a). The additive identity is the 0 map ($\mathbf{0}(a) = 0$), and the inverse is computed pointwise ($(-f)(a) = -f(a)$), and associativity and abelianness is inherited from A. We omit the details. The fact that multiplication is associative

follows because composition of functions is associative. What remains is the distributive law. Fix homomorphisms $f, g, h : A \to A$. For all $a \in A$ we consider:

$$\begin{aligned}((f+g)h)(a) &= (f+g)\circ h(a)\\ &= f(h(a)) + g(h(a))\\ &= ((fh)+(gh))(a)\end{aligned}$$

This was the easy side of the distributive law, and would work for any functions. On the other hand, the other direction of distributivity actually uses the fact that these are homomorphisms (in the third step below):

$$\begin{aligned}(f(g+h))(a) &= f\circ(g+h)(a)\\ &= f(g(a)+h(a))\\ &= f(g(a)) + f(h(a))\\ &= ((fg)+(fh))(a)\end{aligned}$$

As an interesting takeaway, notice that if you just the set S_A of *permutations* of A which need not be homomorphisms, and try to make it into a ring with multiplication given by composition (as above), you get an object which satisfies the distributive law on the right, but not on the left! □

(b) Prove that $(\mathrm{End}(A))^\times \cong \mathrm{Aut}(A)$.

Proof. Notice that there is an obvious inclusion of sets $\mathrm{Aut}(A) \subseteq \mathrm{End}(A)$ (since every automorphism is automatically an endomorphism). Furthermore, an endomorphism $f : A \to A$ is a unit in the endomorphism ring if and only if it has an inverse as a function, that is, if and only if it is an automorphism of A. Therefore the inclusion exhibits a bijection

$$\mathrm{Aut}(A) \leftrightarrow \mathrm{End}(A)^\times.$$

Finally, since on both sides the group law is composition, it is in fact an isomorphism of groups. □

(c) Let E be an elementary abelian p-group of order p^n. Show that $\mathrm{End}(E) \cong M_n(\mathbb{F}_p)$, where we give the latter the operations matrix addition and multiplication. Conclude that $M_n(\mathbb{F}_p)$ is a ring and that $M_n(\mathbb{F}_p)^\times = GL_n(\mathbb{F}_p)$. (You may use Proposition 1 from HW6, after which this should be completely formal.)

Proof. First notice that an elementary abelian p-group of order p^n is isomorphic to $\mathbb{F}_p^n$ (by HW8 Problem 7). By HW8 Problem 6 we know that an endomorphism of $\mathbb{F}_p^n$ is the same data as a linear map from $\mathbb{F}_p^n$ to itself. By linear algebra (Proposition 1 in HW6), this corresponds to a unique matrix in $M_n(\mathbb{F}_p)$. Furthermore, addition of endomorphisms corresponds to addition of matrices, and composition of endomorphisms corresponds to multiplication of matrices, so this identification indeed preserves the ring structure. □

Had we been not been in lockdown on Thursday, we would have encountered the following definition:

Definition 1. *Let R be a ring. A subset $S \subseteq R$ is called a subring if it is a subgroup under addition, and also if $a, b \in S$ then $ab \in S$.*

6. (a) Let R be a ring and $S \subseteq R$ a subring. Show that S is a ring.

Proof. We know that it is an S abelian subgroup by definition, and it inherits a multiplication operation from R since it is closed under that operation. The fact that it is associative follows because multiplication is computed in R which is a ring, and the distributive law holds for the same reason. □

(b) Let $\{S_i \subseteq R\}$ be a nonempty collection of subrings of R. Show that $\bigcap_i S_i$ is a subring of R.

Proof. We already know it is an abelian subgroup (HW4 Problem 2(d)), so it suffices to show it is closed under multiplication. Given r and s in the intersection, we know r and s are in S_i for each i. Therefore so is rs since each S_i is a subring, and we win. □

(c) Suppose S is a subring of R, and R is a subring of T. Show that S is a subring of T.

Proof. We know S is an abelian subgroup of T, and it is closed under multiplication as a subring of R, so we are done. □

7. Let D be an integer which is not a perfect square. One forms a *quadratic integer ring*

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\},$$

with the standard notions of addition and multiplication. We will see that the structure of this ring depends heavily on D.

(a) Show that $\mathbb{Z}[\sqrt{D}]$ is a ring. (*Hint:* You could do this directly, or observe it is a subring of a well known field, and leverage the previous exercise).

Proof. Consider the inclusion $\mathbb{Z}[\sqrt{D}] \subseteq \mathbb{C}$. We know $\mathbb{C}$ is a field, therefore a ring, so if we show this inclusion makes $\mathbb{Z}[\sqrt{D}]$ into a subring we are done by 6(a). We first observe that it is nonempty (for example, it includes 0). We next observe it is closed under addition and additive inverses:

$$(a_0 + b_0\sqrt{D}) + (a_1 + b_1\sqrt{D}) = (a_0 + a_1) + (b_0 + b_1)\sqrt{D} \in \mathbb{Z}[\sqrt{D}],$$

and

$$-(a + b\sqrt{D}) = -a + (-b)\sqrt{D} \in \mathbb{Z}[\sqrt{D},$$

so that it is an abelian subgroup. It remains to show it is closed under multiplication. We check:

$$\begin{aligned}(a_0 + b_0\sqrt{D})(a_1 + b_1\sqrt{D}) &= a_0a_1 + b_0\sqrt{D}a_1 + a_0b_1\sqrt{D} + b_0\sqrt{D}b_1\sqrt{D} \\ &= (a_0a_1 + b_0b_1D) + (a_1b_0 + a_0b_1)\sqrt{D} \in \mathbb{Z}[\sqrt{D}],\end{aligned}$$

as needed. □

(b) Define the norm of a quadratic integer to be

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}).$$

Prove that the norm gives a map $N : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}$ satisfying $N(xy) = N(x)N(y)$.

Proof. We first foil to compute

$$N(a+b\sqrt{D}) = a^2 - b^2 D,$$

which is indeed an integer. To compute multiplicativity, we introduce some notation. If $x = a + b\sqrt{D}$ then we let $\overline{x} = a - b\sqrt{D}$ (if D is negative this is precisely the complex conjugate!). Then conjugation is multiplicative:

$$\overline{x_0} \cdot \overline{x_1} = (a_0 - b_0\sqrt{D})(a_1 - b_1\sqrt{D}) = (a_0a_1 + b_0b_1D) - (a_1b_0 + a_0b_1)\sqrt{D} = \overline{x_0x_1}.$$

Therefore:

$$N(x_0x_1) = (x_0x_1)(\overline{x_0x_1}) = (x_0\overline{x}_0)(x_1\overline{x}_1) = N(x_0)N(x_1).$$

One could also compute this directly, but it's a bit of a mess. □

(c) Let $x \in \mathbb{Z}[\sqrt{D}]$. Show x is a unit if and only if $N(x) = \pm 1$.

Proof. Suppose x is a unit, and let x^{-1} be it's inverse. Then:

$$N(x)N(x^{-1}) = N(xx^{-1}) = N(1) = 1,$$

so that $N(x) \in \mathbb{Z}^\times = \{\pm 1\}$. Conversely, suppose $N(x) = 1$. This (using the notation from the proof of part (b)), this precisely says that $x\overline{x} = 1$, so that $x^{-1} = \overline{x}$. If $N(x) = -1$, then $-(x\overline{x}) = x(-\overline{x}) = 1$, so that $x^{-1} = -\overline{x}$. Either way, x is a unit. □

(d) Use part (c) to establish the following.

i. Let $i = \sqrt{-1}$. Show $(\mathbb{Z}[i])^\times = \{\pm 1, \pm i\}$.

Proof. Let $\alpha = a + bi$ be a Gaussian integer. Then $N(\alpha) = a^2 + b^2$. Then by part (c), α is a unit if and only if $a^2 + b^2 = \pm 1$, which holds and only if $a = \pm 1$ and $b = 0$ or $b = \pm 1$ and $a = 0$, which in turn holds precisely when $\alpha = \pm 1$ or $\alpha = \pm i$. □

ii. Let $D < -2$. Show $(\mathbb{Z}[\sqrt{D}])^\times = \{\pm 1\}$.

Proof. Let $\alpha = a + b\sqrt{D}$. Then $N(\alpha) = a^2 + b^2(-D)$¡ where $-D \geq 2$. Therefore if $b \neq 0$ we know $b^2 \geq 1$ so that $N(\alpha) \geq 2$, so $N(\alpha) = \pm 1$ if and only if $a = \pm 1$ and $b = 0$. By part (c) we conclude that α is a unit if and only if it is equal to ± 1. □

iii. Show $|(\mathbb{Z}[\sqrt{2}])^\times| = \infty$.

Proof. Consider $\alpha = 1 + \sqrt{2}$. We can compute $N(\alpha) = -1$, and observe that by part (c) α is a unit. Since the unit group is a group under multiplication, so is $\alpha^2, \alpha^3, \alpha^4, \cdots$. But α is a real number larger than 1, so this is a strictly increasing sequence of real numbers, in particular, they are all distinct. Therefore, we have exhibited an infinite collection of units: $\{\alpha^n : n \geq 1.\}$. □