# 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) $(-a)b = a(-b) = -ab$
   (b) $(-a)(-b) = ab$
   (c) If $1 \in R$ then $(-1)a = -a$.
   (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 $b = 0$

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

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.
   (b) Give an example of a ring with a nonzero nilpotent element.
   (c) Show that the sum of nilpotent elements is nilpotent.
   (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*).
   (e) Suppose $R$ is a commutative ring with $1 \neq 0$, and suppose $r \in R$ is nilpotent. Show that $1 + r \in R^\times$.

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.
   (b) Suppose $R$ is commutative, show that $\mathrm{Maps}(X, R)$ is too.
   (c) Suppose $R$ is unital, show that $\mathrm{Maps}(X, R)$ is too.
   (d) Suppose $R$ is reduced (defined in Problem 3), show that $\mathrm{Maps}(X, R)$ is too.
   (e) Give an example to show that even if $R$ is a field, $\mathrm{Maps}(X, R)$ need not be.
   (f) Give an example to show that even if $R$ is an integral domain, $\mathrm{Maps}(X, R)$ need not be.

5. Let $A$ be an abelian group (with binary operation $+$). Define the *endomorphism ring* of $A$ as follows:
$$\mathrm{End}(A) = \{f : A \to A \mid f \text{ is a homomorpism}\}.$$
Give $\mathrm{End}(A)$ 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 $\mathrm{End}(A)$ is a ring.
   (b) Prove that $(\mathrm{End}(A))^\times \cong \mathrm{Aut}(A)$.
   (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.)

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.
   (b) Let $\{S_i \subseteq R\}$ be a nonempty collection of subrings of $R$. Show that $\bigcap_i S_i$ is a subring of $R$.
   (c) Suppose $S$ is a subring of $R$, and $R$ is a subring of $T$. Show that $S$ is a subring of $T$.

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).
   (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 $N(xy) = N(x)N(y)$.
   (c) Let $x \in \mathbb{Z}[\sqrt{D}]$. Show $x$ is a unit if and only if $N(x) = \pm 1$.
   (d) Use part (c) to establish the following.
      i. Let $i = \sqrt{-1}$. Show $(\mathbb{Z}[i])^\times = \{\pm 1, \pm i\}$.
      ii. Let $D < -2$. Show $(\mathbb{Z}[\sqrt{D}])^\times = \{\pm 1\}$.
      iii. Show $|(\mathbb{Z}[\sqrt{2}])^\times| = \infty$.