Rings and Subrings

A **ring** on a set $R$ with two binary operations, $+$ and $*$ such that:

1. $(R, +)$ is an abelian group,
2. $(R, *)$ is closed and has the associative property, and
3. $R$ has the distributive property, that is for all $a, b, c \in R$,
   - $a * (b + c) = a * b + a * c$, and
   - $(a + b) * c = a * c + b * c$.

1. Some examples of rings we have already worked with are $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$.
   (a) In each case, figure out which elements are **invertible** (have multiplicative inverses). There are called **units**.
   (b) Are there any nonzero elements of these rings which multiply to zero? These are called **zero divisors**.

2. We also saw that if $F$ is a field, the set of polynomials $F[x]$ is a ring. In fact, when $R$ is any ring, $R[x_1, x_2, \ldots, x_n]$, the set of polynomials in $n$ variables, is a ring.
   (a) A **subring** is a nonempty subset $S$ of a ring that is closed under sums, products, and taking additive inverses. Check that $R$ is a subring of $R[x_1, \ldots, x_n]$.
   (b) Consider the rings $\mathbb{Z}[x]$. Let $S$ be the set of all linear polynomials, $S = \{a + bx \mid a, b \in \mathbb{Z}\}$. Show that $S$ is a subgroup of $\mathbb{Z}[x]$ but not a subring.

3. All of the rings in the previous examples are rings with **unity**. That is, there is a multiplicative identity $1$ in the ring. Consider the following rings.
   (a) Let $R$ be the set of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ which tend to $0$ in both directions. That is,
      $$R = \{f: \mathbb{R} \to \mathbb{R} \mid f \text{ continuous}, \lim_{x \to \pm \infty} f(x) = 0\}.$$ 
      Then $R$ is a ring under function addition and multiplication. Why is there no identity in this ring? (HW Pass for this answer.)
   (b) Let $S$ be the set of $2 \times 2$ matrices which are zero except for the first (top left) entry. Show this is a subring of $\text{GL}(n, \mathbb{R})$ with no identity.
Take Home HW Pass

Now that we have finished our group theory section, I would like to encourage you to seek out applications of the things we have learned. The following is a list of possible applications. If you look up one of these, and turn in a few paragraphs about how it uses what we’ve learned, along with a list of sources (websites that aren’t wikipedia, etc), that will earn you a HW pass. Feel free to look at a different topic based on your own interests.

1. Elliptic curves as a group, and how they are used for encryption (there are a few youtube videos and blogs that explain this pretty well).

2. Symmetry groups of molecules in Chemistry (I’ve seen a few tutorials, and some interactive websites).

3. Group theory and particle physics (some professors have written nice introductory articles about this).

4. Group actions and manifolds (This is for people who are interested in abstract mathematics and geometry. You can construct projective spaces, Klein bottles, tori, etc as sets of orbits of group actions.)

5. Galois theory (also a more abstract topic, with very nice results. You can use group theory to prove that there could never be a formula for the solutions of a degree 5 polynomial.)