Proof Techniques	Instructor: Padraic Bartlett

Homework 2

Week 1	*Mathcamp 2012*

Homework instructions: many of the problems below are labeled with the tags $(*)$ or $(+)$. $(*)$ denotes that the problem in question is fairly fundamental to the topics we're studying and is something that you should make sure you understand completely, while $(+)$ denotes a problem that may be much harder than some of the others on the set.

This class is homework-required! What this means is that I'm expecting you to try every problem, to solve almost all of the $(*)$ ones, and most of the non-$(+)$ ones. The $(+)$ ones are certainly problems you are capable of solving, and I want you solve some of these! But they will not be as necessary for your ability to survive and thrive in later lectures, and I don't expect people to solve all of them. If you get stuck, or see a typo, find me! I can offer tons of hints and corrections. HW will be handed in at the start of class every week; I'll try to look over solutions in between classes, and come up with comments.

1. Let x, y be a pair of irrational numbers: i.e. elements in $\mathbb{R}$ that are not elements of $\mathbb{Q}$. Either prove that the following statements are true, or disprove them by finding a pair of elements x, y that show that this statement is false:
   - $x + y$ is irrational.
   - $x \cdot y$ is irrational.
2. [$(*)$] Prove, using only the axioms that we listed for $\mathbb{Z}$ (i.e. the ring axioms along with the ordering axioms) that $x^2 > 0$, for any x.
3. [$(*)$] Prove, using only the axioms that we listed for $\mathbb{Q}$ (i.e. the field axioms along with the ordering axioms) that for any $x, y > 0$ in $\mathbb{Q}$, there is some $n \in \mathbb{N}$ such that $n \cdot x > y$.
4. Prove that $\sqrt{3} - \sqrt{5}$ is an irrational number: i.e. that $\sqrt{3} - \sqrt{5}$ is not an element of $\mathbb{Q}$.
5. [$(*)$], [$(+)$] Take any two elements $p, q \in \mathbb{Q}$ such that $p < q$. Is there always an element $x \in \mathbb{R}$ such that $p < x < q$ and $x \notin \mathbb{Q}$? Prove your claim.

   Similarly, take any two elements $p, q \in \mathbb{R}$ such that $p < q$. Is there always an element $x \in \mathbb{Q}$ such that $p < x < q$? Prove your claim.

Our last few questions deal with the concept of **groups**, which we define here. Students currently in a group theory class should only do the problems that are new to them / don't overlap with work they've already done.

Definition. Take a set G, along with an operation $\cdot$ that gives you some way to "combine" two elements in your group into a new element. Suppose that this operation $+$ satisfies the following four properties that the integers, $\mathbb{Z}$, also did with respect to $+$: namely,

- **Closure(+)**: $\forall a, b \in G$, we have $a + b \in G$.
- **Identity(+)**: $\exists 0 \in G$ such that $\forall a \in G$, $0 + a = a$.
- **Associativity(+)**: $\forall a, b, c \in G, (a + b) + c = a + (b + c)$.
- **Inverses(+)**: $\forall a \in G, \exists$ a unique $(-a) \in G$ such that $a + (-a) = 0$.

We call this kind of thing a **group**: in class, we claimed that $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$, and $\langle \mathbb{R}, + \rangle$ were all groups.

6. [(∗)] Given the above examples, you might think that all groups contain infinitely many elements. This is false! Take the following object:

   - Your set is the numbers $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.
   - Your operation is the operation "addition mod 12," or "clock arithmetic," defined as follows: we say that $a + b \cong c \mod 12$ if the two integers $a + b$ and c differ by a multiple of 12. Another way of thinking of this is as follows: take a clock, and replace the 12 with a 0. To find out what the quantity $a + b$ is, take your clock, set the hour hand so that it points at a, and then advance the clock b hours; the result is what we call $a + b$.

     For example, $3 + 5 \equiv 8 \mod 12$, and $11 + 3 \equiv 2 \mod 12$.

   We denote this object as $\langle \mathbb{Z}/12\mathbb{Z}, + \rangle$. Show that this is a group.

7. [(∗)] Generalize this to $\langle \mathbb{Z}/n\mathbb{Z}, + \rangle$ as follows:

   - Your set is the numbers $\{0, 1, \ldots n - 1\}$.
   - Your operation is the operation "addition mod$n$," defined as follows: we say that $a + b \equiv c \mod n$ if the two integers $a + b$ and c differ by a multiple of n.

     For example, for $n = 3$, we would say that $2 + 2 \equiv 3 \mod 1$, and $2 + 1 = 0 \mod 3$. Similarly, for $n = 10$, we say that $5 + 6 \equiv 1 \mod 10$ and $7 + 7 \equiv 4 \mod 10$.

   Show that this is a group.

8. Similarly, we can define the operation "multiplication mod n" by saying that $a \cdot b \equiv c \mod n$ if $a \cdot b$ and c differ by a multiple of n, and the set $(\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ as the set $\{1, 2, \ldots n - 1\}$.

   Is $\langle (\mathbb{Z}/5\mathbb{Z}) \setminus \{0\}, \cdot \rangle$ a group? How about $\langle (\mathbb{Z}/6\mathbb{Z}) \setminus \{0\}, \cdot \rangle$?

9. [(+)] The one axiom for arithmetic we didn't mention when talking about groups was the concept of **commutativity**:

   - **Commutativity(·)**: $\forall a, b \in \mathbb{N}, a \cdot b = b \cdot a$.

   Find a group $\langle G, \cdot \rangle$ that does not satisfy this property. What is the smallest group (in terms of numbers of elements) that exists that does not satisfy this property?