Math 403 Chapter 12: Introduction to Rings

1. **Introduction:** In a group we have just one binary operation but in many structures there are two natural ones. For example in $\mathbb{R}$ we can add and multiply. Sure, we can also subtract and divide but these two often come along with addition and multiplication, as do exponents and then even logarithms, etc.

2. **Definition:** A *ring* R is a set with two closed binary operations, addition denoted by $a+b$ and multiplication denoted by ab such that for all $a,b,c \in R$ we have:

   (a) $a+b=b+a$.
   (b) $(a+b)+c=a+(b+c)$.
   (c) There is an additive identity 0.
   (d) There are additive inverses, for a we denote it $-a$ and write $a-b$ instead of $a+(-b)$.
   (e) $(ab)c=a(bc)$.
   (f) $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$.

   Basically a ring is an Abelian group under addition in which multiplication is introduced and which is associative and distributes over addition. Note however that:

   - There no guarantee of a *multiplicative identity* (also called a *unity*).
   - If there is a unity then there is no guarantee that elements have *multiplicative inverses*; If there is a unity then an element with a multiplicative inverse is a *unit*.
   - There is no guarantee of multiplicative *commutativity*.

   For $a \in R$ and $n \in \mathbb{Z}^+$ we write a^n to mean $aa...a$ (n times) and na to mean $a+a+...+a$. If there is any confusion between na for $n \in \mathbb{Z}^+$ and ba for $b \in R$ then we'll write $n \cdot a$ instead.

   Example: $\mathbb{Z}$ is a commutative ring with unity 1 and units ± 1.

   Example: $\mathbb{Z}_n$ is a commutative ring with unity 1 and units $U(n)$.

   Example: $2\mathbb{Z}$ is a commutative ring with no unity.

   Example: $GL_2\mathbb{R}$ is not a ring since addition is not closed.

   Example: $M_2\mathbb{R}$ is a non-commutative ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and units $GL_2\mathbb{R}$.

   Example: The quaternions $\mathbb{H}$ is a non-commutative ring with unity 1 and units all nonzero quaternions.

3. **Theorem (Properties of Multiplication):** If $a,b,c \in R$ then:

   (a) $a0=0a=0$.
   (b) $a(-b)=(-a)b=-(ab)$.
   (c) $(-a)(-b)=ab$.
   (d) $a(b-c)=ab-ac$ and $(b-c)a=ba-ca$.

   In addition if R has a unity 1 then:

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

(f) $(-1)(-1) = 1$.

We really need to stop to consider that these obvious-looking things are not obvious. For example (c) states that the product of the inverses of two elements must equal the product of the two elements and (e) states that the product of the inverse of the unity with an element equals the inverse of that element.

Proof: We'll prove (a) and part of (b).

For (a) note that $0 + a0 = a0 = a(0 + 0) = a0 + a0$ and then we cancel.

For part of (b) note that $a(-b) + ab = a(-b + b) = a(0) = 0$ and so $a(-b) = -(ab)$.

4. **Theorem (Uniqueness of Unity and Multiplicative Inverses):** If a ring has a unity then it is unique. If a ring has a multiplicative inverse then it is unique.
Proof: Just like for groups. $\mathcal{QED}$

5. **Definition:** A subset $S \subseteq R$ of a ring is a *subring* if itself is a ring using R's operations.

6. **Theorem (Subring Test):** A nonempty subset $S \subseteq R$ is a subring if $\forall a, b \in S$ we have $a - b \in S$ and $ab \in S$.
Proof: Straightforward. $\mathcal{QED}$

   Example: $n\mathbb{Z}$ is a subring of $\mathbb{Z}$.

   Example: The set $\mathbb{Z}[i] = \{a + b\,\hat{\imath} \,|\, a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$.