Math 222: A Brief Introduction to Rings

We have discussed two fundamental algebraic structures: *fields* and *groups*. A field is a world with two operations (addition and multiplication) which satisfy all the properties we're used to. A group has only one operation which need not be commutative. Somewhere in between these two worlds is a third fundamental structure: a *ring*.

Definition. A *ring* is a set R with two operations $(+, \cdot)$ such that R forms an abelian group under addition and the multiplication is associative and distributes over addition. More precisely, for all $a, b, c \in R$, the following must hold:

(1) $a + b = b + a$.

(2) $(a + b) + c = a + (b + c)$.

(3) There is an element 0 in R such that $a + 0 = a$.

(4) There is an element $-a$ in R such that $a + (-a) = 0$.

(5) $a(bc) = (ab)c$.

(6) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

Clearly any field satisfies all these properties and so is a ring. But, let's look at what properties are NOT assumed for a ring:

- The multiplication is not assumed to be commutative. If it is, the ring is said to be *commutative*. Note: We do not say that a ring is *abelian* – that terminology is reserved for groups.
- The ring need not have a 1, that is a multiplicative identity element. If it does, we say the ring has a *unity* or has an *identity* or has a *one* or the ring is *unital*. If a ring does have a unity, the unity is unique.
- Even if the ring does have a unity, there is no assumption that multiplicative inverses exist. An element of a unital ring which does admit a multiplicative inverse is called a *unit*. If they exist, inverses are also unique in a ring. Further, the set of units in a ring forms a group under multiplication – the *unit group* of the ring.

In this language, a field is a commutative ring with unity in which every non-zero element is a unit. Besides fields, we have already come across many rings in this course:

Example 1. The integers $\mathbb{Z}$ under usual addition and multiplication is a commutative ring with unity – the unity being the number 1. Of course the only units are ± 1.

Example 2. For any positive integer $n > 0$, the integers mod n, $\mathbb{Z}_n$, is a commutative ring with unity. We have seen that the units are those elements which are relatively prime to n. The unit group is denoted $U(n)$. Of course, if n happens to be a prime, then we have a field.

Example 2.1 Consider $\mathbb{Z}_{10}$. The group of units is $U(10) = \{1, 3, 7, 9\}$. Which group of order 4 is this isomorphic to? We have already noticed something "bad" which can happen in rings: both 2 and 5 are non-zero elements of $\mathbb{Z}_{10}$ and yet $2 \cdot 5 = 0 \bmod 10$. The numbers 2 and 5 are called *zero-divisors*. In a field zero is the only zero-divisor. A commutative ring with unity which has NO non-zero zero-divisors is called an *integral domain*. For example, $\mathbb{Z}$ is an integral domain as is any field.

Example 3. Given any ring R, the set of polynomials with coefficients in R:

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : a_i \in R\}$$

under polynomial addition and multiplication is a commutative ring with unity (the constant polynomial 1). We have already observed that most polynomials do not have an inverse. If R has no (non-zero) zero-divisors, then the polynomial ring over R, $R[x]$, has no (non-zero) zero-divisors.

Example 3.1. What are the units in $\mathbb{R}[x]$? $\mathbb{Z}[x]$?

Example 4. The set of even integers $2\mathbb{Z} \subset \mathbb{Z}$ is a ring. Indeed, it is a *subring* of $\mathbb{Z}$ and is of course commutative. Does it have a unity?

Example 5. An important family of non-commutative rings are *matrix rings*. For example, consider the set of all 2×2 matrices with real entries:

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}.$$

This is a ring under matrix addition and multiplication. It has an identity – what is it? But, it is not commutative. Can you give an example? What is the group of units? Note: One can consider matrices of arbitrary size and having entries in any field or ring.

Definition. Two rings R and S are said to be *isomorphic* if there is a map $f : R \to S$ satisfying the following three properties:

- f is one-to-one: For $a, b \in R$, if $f(a) = f(b)$, then $a = b$.
- f is onto: For each $b \in S$, there is $a \in R$ with $f(a) = b$.
- f is a *homomorphism of rings*: For all $a, b \in R$, $f(a+b) = f(a)+f(b)$ and $f(a \cdot b) = f(a) \cdot f(b)$.

Example 6. Consider the fields $F = GF(3, x^2 + x + 2)$ with Galois imaginary α and $F' = GF(3, x^2+2x+1)$ with Galois imaginary β. Both α and β are primitive elements in their respective fields and the map $f : F \to F'$ by $f(\alpha^n) = \beta^n$ for each $0 \leq n \leq 8$ is an isomorphism of rings. Or in this case we would say an isomorphism of fields.

Example 6.1 The map $f : \mathbb{Z} \to 3\mathbb{Z}$ by $f(x) = 3x$ is an isomorphism of groups (under the addition structure) but is NOT an isomorphism of rings since $f(2 \cdot 2) \neq f(2) \cdot f(2)$.

Definition. A subring $S \subset R$ a ring is said to be a (two-sided) *ideal* if for every $s \in S$ and $r \in R$, both rs and sr are in S.

Example 7. The subring $2\mathbb{Z} \subset \mathbb{Z}$ is an ideal. For an element of $2\mathbb{Z}$ is even and multiplying by any other integer, it remains even. Moreover, for any postive integer n, the subset $n\mathbb{Z} \subset \mathbb{Z}$ is an ideal.

Example 8. Consider the polynomial ring $\mathbb{R}[x]$ and let S be the subset of all polynomials with zero constant term. This is a subring and in fact an ideal. It is usually denoted $\langle x \rangle$ and called the ideal generated by x. The point being that every polynomial with zero constant term admits x as a factor; in other words, is a multiple of x.

Example 8.1. Consider the ideal $\langle x^2 \rangle \subset \mathbb{R}[x]$. Can you figure out what this set is? In particular, which of the following polynomials lie in $\langle x^2 \rangle$:

$$x^5 + 2x^3 - x^2, \quad x^2 + 2, \quad 5x^3 + x, \quad 10x^{35} - x^{16} \ ?$$

This notion of an ideal allows one to form so called *factor rings* by "dividing" in some sense a ring by an ideal. This is similar to the notion of a quotient group.