CLASS 1, FEBRUARY 4TH: RINGS AND IDEALS

A ring is one of the most fundamental objects in algebra. It has more structure than a group does, which allows for more interesting analysis. When initially realized, the axioms listed below were made up to encapsulate the structure of the integers in a more flexible framework.

Definition 1.1. A ring $(R, +, \cdot)$, more commonly displayed simply as R, is a set R together with two binary operations

$$+, \cdot : R \times R \to R$$

satisfying the following properties:

1) $(R, +)$ is an Abelian (commutative) group. Expanded, this means that there exists an identity, 0, an inverse for any element, $-r$, and that addition is associative.
2) $\cdot$ is an associative operation: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3) The distributive law holds: $a \cdot (b + c) = a \cdot b + a \cdot c$

Some additional considerations can also be made:

- If $\cdot$ is commutative, $a \cdot b = b \cdot a$, then we call R **commutative**.
- If there exists an identity element for $\cdot$, 1, the R is said to be **unital**.

We will assume throughout (with few exceptions) all rings are commutative and unital.

Example 1.2.

- 0: The ring with 1 element 0 is a ring! It is even unital with $1 = 0$.
- K: A field is a non-zero, commutative, unital ring in which $K^\circ = K \setminus \{0\}$ is a group under $\cdot$. Examples are $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{F}_{p^n}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $K(x)$, etc.
- $\mathbb{Z}$: The integers satisfy these properties, as are thus a commutative unital ring, but NOT a division ring.
- $n\mathbb{Z}$: Does satisfy the properties of being a ring, but has no unit if $n \neq 1$.
- $\mathbb{Z}/n\mathbb{Z}$: The integers $(\mathrm{mod}\, n)$ are a ring! If n is not prime, then it is commutative and unital, but NOT division.
- $K[x]$: Let K be a field (or even any ring!). Then $K[x]$ is notation for polynomials in the variable x with coefficients in K. Then $K[x]$ is a commutative, unital ring which again are NOT division rings.
- $K[\![x]\!]$: The power series in the variable x are also commutative, unital rings which are NOT division rings
- $C_i(\mathbb{R})$: If $i = 0$, the continuous functions from $\mathbb{R}$ to $\mathbb{R}$ form a ring. In addition, if $i > 0$, the i-times differentiable functions also form a ring!

Some immediate consequences of the properties of rings are the following:

- $0 \cdot r = r \cdot 0 = 0$ for any $r \in R$.
- $(-r)s = r(-s) = -(rs)$ for any $a, b \in R$.
- $1 \in R$ is unique, if it is exists.

Ring elements may have specific properties. I now list a few of them:

Definition 1.3. An non-zero element $r \in R$ is called a **zero-divisor** if there exists $s \neq 0$ such that $r \cdot s = 0$. Otherwise r is said to be a **non-zero-divisor**, or **n.z.d.**.

If R has no zero-divisors, and $1 \neq 0$, then R is said to be an **integral domain**.

An element $u \in R$ is called a **unit** if $1 \neq 0$ in R, and there exists $s \in R$ such that $u \cdot s = 1$.

Thus a field is a commutative unital ring in which every non-zero element is a unit.

Next up, we study **Ideals**. They are often used to describe the structure of R in commutative algebra and algebraic geometry.

Definition 1.4. A proper subset $I \subsetneq R$ is called an **ideal** if

1) $(I, +)$ is a closed subgroup of R.
2) I is strongly closed under multiplication: For any element $r \in R$ and $\alpha \in I$, we have that $r \cdot \alpha \in I$.

Example 1.5.
- $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.
- $xK[x]$ is an ideal of $K[x]$.
- Sums of elements divisible by x **or** y form an ideal of $K[x, y]$.

There is a theme here of divisibility: We can think of all of these ideals as being **generated** by a given element (the smallest ideal containing a given element). In this case, we often refer to them as $\langle n \rangle$, $\langle x \rangle$, or $\langle x, y \rangle$ in the previous cases.

In general,

$$\langle f_1, \ldots, f_n \rangle := \left\{ \sum_{i=1}^{n} r_i \cdot f_i \mid r_i \in R \right\}$$

Next up, I bring up the relationship between ring homomorphisms and ideals. Recall the definition of a ring homomorphism:

Definition 1.6. Let R and S be rings. A map $\varphi : R \to S$ is said to be a **ring homomorphism** if the following criteria are met for any $r, r' \in R$:

1) $\varphi(r + r') = \varphi(r) + \varphi(r')$.
2) $\varphi(r \cdot r') = \varphi(r) \cdot \varphi(r')$.
3) $\varphi(1) = 1$.

The collection (group) of all homomorphisms from R to S is denoted by $\mathrm{Hom}(R, S)$.

This is a very reasonable definition, as it makes addition and multiplication in R compatible with that in S. Additionally, the kernel is defined as in linear algebra.

Definition 1.7. The **kernel** of φ, denoted $\ker(\varphi)$ is the set

$$\ker(\varphi) = \{r \in R \mid \varphi(r) = 0\} \subseteq R$$

The relationship between the 2 ideas is now stated as follows (c.f. Homework 1 #1):

Proposition 1.8. *The kernel of a ring homomorphism is an ideal. Additionally, every ideal is the kernel of some homomorphism.*