CLASS 1, MONDAY FEBRUARY 5TH: RINGS!

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 0.1. 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**.
- R is said to be a **division ring** if it is unital, $1 \neq 0$, and every element $r \in R$ has a multiplicative inverse: $\frac{1}{r}$ or r^{-1}. Note that we don't need to worry about the side in which we multiply (left/right inverses)!

Most of the time later in this course we will focus on commutative, unital, rings R.

Example 0.2.

- 0: The ring with 1 element 0 is a ring! It is unital $(1 = 0)$, but is not division.
- K: A field is a commutative, unital, division ring! 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 $\pmod n$ 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
- $M_n(K)$: $n \times n$ matrices with coefficients in a field K are a non-commutative unital ring. It is not a division ring, as something not of full rank can not be inverted. However...
- $GL_n(K)$: The **General Linear Group** of full rank $n \times n$ matrices is a subring of $M_n(K)$, which IS a unital division ring!

- $C_i(\mathbb{R})$: 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.

Proof. Exercise done in class. For the first consequence, note that

$$0 \cdot r = (0 + 0) \cdot r = 0 \cdot r + 0 \cdot r$$

so $0 \cdot r = 0$ by subtraction of the left from the right hand side. □

Some ring elements have specific properties. I now list a few of them:

Definition 0.3. 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**.

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 element is a unit. There are many nice properties of non-zero-divisors:

Proposition 0.4. *If a is a non-zero divisor, and $b, c \in R$ are such that $ab = ac$, then $b = c$.*

This was shown using distributivity. Next time we will pick up with this result:

Corollary 0.5. *Any finite integral domain R is a field.*