NOTES ON RINGS, MATH 369.101

Rings

Often we need to work in a setting where there are not multiplicative inverses (at least for some non-zero elements). For example, the integers $\mathbb{Z}$, polynomials, or matrices.

A **commutative ring** is a set with addition and multiplication which satisfies all the field axioms except (possibly) the existence of multiplicative inverses.

A **ring** is a set with addition and multiplication which satisfies all the commutative ring axioms except (possibly) the commutativity of multiplication.

<u>Examples</u>:

(1) $\mathbb{Z}$: the only thing missing to go from $\mathbb{Z}$ to the field $\mathbb{Q}$ are reciprocals of non-zero numbers (multiplicative inverses). So $\mathbb{Z}$ is a commutative ring.

(2) Every field is a commutative ring. We don't require multiplicative inverses to not be there, they just might not be. Similarly, every commutative ring is a ring.

(3) For any $n > 0$, we have $\mathbb{Z}_n$, integers mod n, which is a commutative ring. If n is a prime, then $\mathbb{Z}_n$ is also a field. If n is not prime, there are still some elements that have a multiplicative inverse (any a with $\gcd(a, n) = 1$), just not every non-zero element. For example:

$$\text{in } \mathbb{Z}_{10}\text{: congruence class of 3 has inverse: } [3][7] = [21] \equiv [1].$$

However, the congruence class of 5 does not, since every multiple of 5 is either congruent to 5 or to 0.

(4) $\mathbb{F}[x]$ is a commutative ring.

(5) $M_n(\mathbb{F})$ which denotes, for $n > 0$, the set of $n \times n$ matrices with entries in a field. This is a ring: addition and multiplication of matrices give you a new matrix; the operations are associative and distributive; the matrix of all zero entries is the additive identity, and the *identity matrix* (with 1 on diagonal, and 0 elsewhere) is the mult. identity; additive inverses are found by negating every entry.

$M_n(\mathbb{F})$ is not a commutative ring.

All the Propositions on addition still work for rings: for example, (additive cancellation) if $a + b = a + c$ then $b = c$ for a, b, c in a ring. And also for any a in a ring, $a \cdot 0 = 0$, and $-(-a) = a$.

Date: Oct. 12 – Oct. 19.

Recall that in $\mathbb{F}[x]$ there is multiplicative cancellation: $f(x) \cdot g(x) = f(x) \cdot h(x)$ implies that $g(x) = h(x)$. Proving this works required the use of the degree of the polynomials.

In a general ring, this doesn't work. For example:
in $\mathbb{Z}_{20}$: $[2][5] = [10] = [2][15]$, but $[5] \neq [15]$ in $\mathbb{Z}_{20}$.