MATH 369 Fall 2025 - Class Notes

11/12/2025

Scribe: Lola Scannell

Summary: Today we reviewed rings and commutative rings, saw several examples and non-examples (including $\mathbb{Z}$, $F[X]$, $2\mathbb{Z}$, and a subset of $\mathbb{Z}_{12}$), and proved basic facts like $0 \cdot a - 0$ in a ring. Then we defined zero divisors and subrings, stated and proved a subring test, and studied units in a ring. We finished with the definitions of a domain and an integral domain, then proved that a unit can be a zero divisor.

Notes:

Rings:

A *ring* is a set R with two binary operations $+$ (additions) and $\cdot$ (multiplication) such that:

1. $(R, +)$ is an abelian group.
2. Multiplication is associative:

$$a(bc) = (ab)c \quad \text{for all } a, b, c \in R.$$

3. There is a multiplication identity $1 \in R$ such that

$$1a = a1 = a \quad \text{for all } 0a \in R.$$

4. Distributive laws hold:

$$a(b + c) = ab + ac, \qquad (b + c)a = ba + ca \quad \text{for all } a, b, c \in R.$$

Unlike a field, we do *not* require that every nonzero element have a multiplicative inverse, and multiplication in a ring need not be commutative.

Commutative Rings:

A ring R is *commutative* if

$$ab = ba \quad \text{for all } a, b \in R.$$

Examples

- $\mathbb{Z}$ with usual addition and multiplication is a commutative ring.

- If F is a field, then $F[x]$ is a commutative ring of polynomials.
- $M_n(F)$, the $n \times n$ matrices over a field F, form a ring that is usually *not* commutative.

Subrings:

Let R be a ring with identity 1_R. A subset $S \subseteq R$ is a *subring* if S is a ring under the inherited operations and its multiplicative identity equals 1_R.

Examples (Ring but not subring)

In $\mathbb{Z}_{12}$ let

$$S = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}.$$

Then S is closed under addition and multiplication mod 12, and $[9]_{12}$ acts as a multiplicative identity on S, so S is a ring. However $[1]_{12} \notin S$, so S is *not* a subring of $\mathbb{Z}_{12}$.

Unit: In a commutative ring R, an element a is a *unit* if there exists $b \in R$ with $ab = 1$. We then write $b = a^{-1}$.

Domain and Integral Domain

- A ring with no zero divisors is called a *domain*.
- A commutative ring with no zero divisors is called an *integral domain*.

Theorems and Proofs:

Theorem 1. *Let R be a ring and $a \in R$. Then $0 \cdot a = a \cdot 0 = 0$.*

Proof. Using distributivity,

$$0 \cdot a = (0 + 0)a = 0a + 0a.$$

Subtract $0a$ from both sides in the additive group $(R, +)$ to get

$$0 = 0a.$$

Similarly $a \cdot 0 = 0$. □

Theorem 2 (Subring Test)**.** *Let R be a ring with identity 1_R and $S \subseteq R$. Suppose:*

1. *S is closed under addition and multiplication;*
2. *for every $a \in S$, the additive inverse $-a$ is in S;*
3. *$1_R \in S$.*

Then S is a subring of R.

Proof. Since S is closed under $+$ and contains additive inverses, $(S, +)$ is a subgroup of $(R, +)$, hence an abelian group. The multiplication and distributive laws are inherited from R, and closure under multiplication is assumed, so S is a ring. Because 1_R lies in S and serves as the multiplicative identity there as well, S is a subring of R. □

Lemma 1. *In a ring R, the multiplicative identity is unique.*

Proof. Since S is closed under $+$ and contains additive inverses, $(S, +)$ is a subgroup of $(R, +)$, hence an abelian group. The multiplication and distributive laws are inherited from R, and closure under multiplication is assumed, so S is a ring. Because 1_R lies in S and serves as the multiplicative identity there as well, S is a subring of R. □

Lemma 2. *In a ring R, the multiplicative identity is unique.*

Proof. Suppose 1 and $1'$ are both multiplicative identities in R. Then

$$1 = 1 \cdot 1' = 1',$$

so they must be equal. □

Theorem 3. *If a is a unit in a ring R, then a is not a zero divisor.*

Proof. Assume a is a unit and suppose for contradiction that there exists $b \neq 0$ with $ab = 0$. Let a^{-1} be the inverse of a. Multiply $ab = 0$ on the left by a^{-1}:

$$a^{-1}ab = a^{-1}0 \quad \Rightarrow \quad 1 \cdot b = 0 \quad \Rightarrow \quad b = 0,$$

which contradicts $b \neq 0$. Hence a cannot be a zero divisor. □