Lecture 2

Let's see some basic properties of a ring R:

(i) $0 \bullet a = a \bullet 0 = 0 \quad \forall a \in R$

Proof. Let a be in R, then:

$$\begin{aligned} 0 = 0 + 0 \Rightarrow & 0 \bullet a = (0+0) \bullet a \\ \Rightarrow & 0 \bullet a = 0 \bullet a + 0 \bullet a \\ \Rightarrow & 0 \bullet a + (-0 \bullet a) = 0 \bullet a + 0 \bullet a + (-0 \bullet a) \\ \Rightarrow & 0 = 0 \bullet a \end{aligned}$$

■

(ii) $(-a) \bullet b = a \bullet (-b) = -(a \bullet b) \quad \forall a, b \in R$

Proof. Let a, b be in R, then:

$$a \bullet b + -(a \bullet b) = 0 \quad \text{(by definition)}$$

then

$$\begin{aligned} a \bullet b + (-a) \bullet b = (a + (-a)) \bullet b = 0 \bullet b = 0 \\ \Rightarrow -(a \bullet b) = (-a) \bullet b \end{aligned}$$

■

(iii) $(-a) \bullet (-b) = a \bullet b \quad a, b \in R$

Proof. Let a, b be in R, then:

$$(-a) \bullet (-b) = -(a \bullet (-b)) = -(-(a \bullet b))$$

But by definition we of additive inverse:

$$-(-(a \bullet b)) + (-(a \bullet b)) = 0$$

So

$$(-a) \bullet (-b) = -(-(a \bullet b)) = a \bullet b$$

■

(iv) If R has 1, then 1 is unique and $(-a) = (-1) \bullet a$

Proof. First, the multiplicative identity. Assume 1 and $1'$ are distinct identities. But

$$1 = 1 \bullet 1' = 1'$$

So, in fact, they are the same and it is unique.
Now, by definition additive inverses are unique, so $-a = (-1) \bullet a$ must both sum with a to 0. We check

$$a + (-1) \bullet a = 1 \bullet a + (-1) \bullet a = (1 + (-1)) \bullet a = 0 \bullet a = 0$$

which confirms it. ■

Definition 2.1: Zero Divisor

We say a non-zero element $a \in R$ is a **zero divisor** if $\exists b \neq 0$ such that $a \cdot b = 0$

Example 2.1 Recall that $M_2(\mathbb{R})$ is the set of 2x2 matrices with real valued entries and $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Then,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

implies $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is a zero divsor.

Example 2.2 Let $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Then

$$\overline{2} \cdot \overline{3} = \overline{0}$$

implies $\overline{2}$ is a zero divisor.

Claim: If $\overline{0} \neq \overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is not a zero divisor, then it is a unit.

Proof. Let $a \in \mathbb{Z}$ with $a \neq 0$ be relatively prime to n. Then Euclid's algorithm (more specifically Bezout's Identity) constructs $x, y \in \mathbb{Z}$ such that

$$a \cdot x + n \cdot y = 1 \implies \overline{a} \cdot \overline{x} = \overline{1}$$

Hence, $\overline{a}$ is a unit.
On the other hand, if $\gcd(a, n) > 1$, then let $\gcd(a, n) = d$. Hence, since n is a multiple d we can write for some $q, k \in Z$

$$n = d \cdot q \quad a = d \cdot k$$

Then,

$$\overline{a} \cdot \overline{q} = \overline{a \cdot q} = \overline{d \cdot k \cdot q} = \overline{n \cdot k} = \overline{n} = \overline{0}$$

Thus, $\overline{a}$ is a zero divisor. ■

Corollary 2.1

If n is prime, then $\mathbb{Z}/n\mathbb{Z}$ is a field.

Proof. If $0 < m < n$ and n is prime, then $\gcd(m, n) = 1$. From the previous claim, this would mean every element is a unit and therefore $\mathbb{Z}/n\mathbb{Z}$ is a field. ■

Example 2.3 $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are fields but $\mathbb{Z}/4\mathbb{Z}$ is not (since $\overline{2} \cdot \overline{2} = \overline{0}$, therefore $\overline{2}$ is a zero divisor and not a unit).

Claim: If $a \in R$ is a zero divisor, then it is not a unit

Proof. Let $b \neq 0$ and $a \bullet b = 0$.
Assume $\exists c \in R$ such that $a \bullet c = 1 = c \bullet a$, then

$$c \bullet a \bullet b = c \bullet (a \bullet b) = c \bullet 0 = 0$$

but similarly,

$$c \bullet a \bullet b = (c \bullet a) \bullet b = 1 \bullet b = b$$

contradicting the fact of $b \neq 0$. Hence our assumption is wrong and a is not a unit. ∎

Definition 2.2: Group of Units

If R is a ring with $1 \neq 0$, we denote the set of units by

$$R^{\times} := \{a \in R | \, \exists b \in R \quad a \bullet b = b \bullet a = 1\}$$

Claim: $(R^{\times}, \bullet)$ is a group.

Proof. We check the properties of a group

(i) $1 \in R^{\times} \quad (1 \bullet 1 = 1)$

(ii) $\forall a \in \mathbb{R}^{\times}$, $a \bullet 1 = 1 \bullet a = a$

(iii) Associativity follows since $\bullet$ is associative in R

(iv) $\forall a \in R^{\times}$, by the definition of $R^{\times}$ there exists $b \in R$ such that

$$a \bullet b = b \bullet a = 1$$

but this is the same as

$$b \bullet a = a \bullet b = 1$$

hence b, the inverse of a, is also a unit and therefore $b \in R^{\times}$.

∎

A field F is a commutative ring with $1 \neq 0$ such that $F^{\times} = F \setminus \{0\}$

Definition 2.3: Integral Domain

We say a commutative ring R with $1 \neq 0$ is an **integral domain** if it has no zero divisors

Example 2.4 $\mathbb{Z}/4\mathbb{Z}$ is **not** an integral domain. ($\overline{2} \bullet \overline{2} = \overline{0} \implies \overline{2}$ is a zero divisor)

Example 2.5 $M_2(\mathbb{R})$ is **not** an integral domain. Then,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

implies $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is a zero divsor.

Example 2.6 $\mathbb{Z}$ is an integral domain

Proposition 2.1: Cancellation Law

Let R be a ring and $a, b, c \in R$.
Suppose a is not a zero divisor, then

$$ab = ac \implies b = c$$

Proof. If $a \neq 0$, then $a \cdot (b - c) = 0$. Since we supposed a is not a zero divisor then it must be

$$b - c = 0 \implies b = c$$

■

Example 2.7 To show why a must **not** be a zero divisor, consider $\mathbb{Z}/4\mathbb{Z}$. We have $\overline{2} \cdot \overline{2} = \overline{0}$ and $\overline{2} \cdot \overline{0} = \overline{0}$. So

$$\overline{2} \cdot \overline{2} = \overline{2} \cdot \overline{0}$$

but

$$\overline{2} \neq \overline{0}$$

Corollary 2.2

If R is a finite (as a set) integral domain then R is a field

Proof. Fix $a \in R$ and $a \neq 0$. Then define a map

$$\begin{aligned} f_a : & R \to R \\ & x \mapsto a \cdot x \end{aligned}$$

<u>Claim:</u> f_a is an injective map by cancellation

> ***Proof.*** Suppose $f_a(x) = f_a(y)$, then
>
> $$a \cdot x = a \cdot y \implies x = y$$
>
> hence, it is injective. ■

By the Pigeonhole Principle f_a is also surjective. This bijection implies that there exists $x \in R$ such that $a \cdot x = 1$. Hence, a is a unit and is an element of the group of units, i.e $a \in R^{\times}$.
Since every non-zero a is shown to be in $R^{\times}$ this way, they are all units, and hence R is a field (since every element in the ring has a multiplicative inverse). ■

Definition 2.4: Subring

A subring S of a ring R is a subgroup that is closed under multiplication. That is $S \subset R$ such that $\forall a, b \in S$,

$$\left.\begin{array}{ll} \text{(i) } a+b \in S & \text{(closure under } +) \\ \text{(ii) } 0 \in S & \text{(additive identity)} \\ \text{(iii) } -a \in S & \text{(additive inverse)} \end{array}\right\} S \text{ is a subgroup}$$
$$\begin{array}{ll} \text{(iv) } a \bullet b \in S & \text{(closure under } \bullet) \end{array}$$

Proposition 2.2: Subgroup Criterion

If $S \subset R$ is a subset of a ring such that $\forall a, b \in S$

(i) $S \neq \emptyset$
(ii) $a - b \in S$
(iii) $a \bullet b \in S$

then S is a subring.

Proof. Suppose $a, b \in S$ and the conditions above are true, then

(i) $a - a = 0 \in S$
(ii) $0 - a = -a \in S$
(iii) $a - b = a + (-b) \in S$
(iv) $a \bullet b \in S$

thus satisfying the definition of a subring. ■

Example 2.8 $\mathbb{Z} \subset \mathbb{Q}, \mathbb{Q} \subset \mathbb{R}, \mathbb{Z} \subset \mathbb{R}$ are all subrings.

Example 2.9 $2\mathbb{Z} \subset \mathbb{Z}$ is a subring and more generally $n\mathbb{Z} \subset \mathbb{Z}$ is a subring.

Example 2.10 $C[0,1] \subset \mathcal{F} \coloneqq \{f : [0,1] \to \mathbb{R}\}$ is a subring.

Definition 2.5: Subfield

If F is a field and $F' \subset F$ is a subring such that

(i) $1 \in F'$
(ii) $\forall a \in F', a^{-1} \in F'$

then we say F' is a **subfield** of F.

Warning: Not all subrings of fields are subfields! (e.g $\mathbb{Z} \subset \mathbb{R}$)

Claim: If $R \subset F$ is a subring of a field with $1 \in R$, then R is an integral domain.
