# Lecture 17: Rings, Error Correcting Codes

**Summary:**
We introduce rings and their properties and provide some examples. We prove the absorption property and establish that rings are commutative under addition. We then explore error correcting codes, focusing on the k-fold repetition code and its applications in reliable data transmission.

**Topics Covered:** division ring, field, group, k-fold repetition code, monoid, ring

**Definition:**

A ring is a set $R$ with operations $+$ and $\cdot$ such that

1. $(R, +)$ is a group with identity $0 \in R$
2. $(R, \cdot)$ is a monoid with identity $1 \in R$
3. Distributivity
   - $\forall a, b, c \in R.\ a \cdot (b + c) = a \cdot b + a \cdot c$
   - $\forall a, b, c \in R.\ (a + b) \cdot c = a \cdot c + b \cdot c$

**Examples and non-examples:**

- $(\mathbb{Z}, +, \cdot)$
  - Is a ring
- $(\mathbb{Z}_{\geq 0}, +, \cdot)$
  - Is not a ring because $(\mathbb{Z}_{\geq 0}, +)$ is not a group
- $(\mathbb{Z}_m, +, \cdot)$
  - This is a ring

Recall that in the third example, we defined $+$ and $\cdot$ as

$$[a] + [b] = [a + b]$$
$$[a] \cdot [b] = [ab]$$

**Absorption property:**

Let $(R, +, \cdot)$ be a ring. Let $a \in R$. Then,

$$0 \cdot a = a \cdot 0 = 0$$

**Proof:**

Since $0$ is the identity for $+$, then, we have

$$0 + 0 = 0$$

Therefore,

$$\begin{aligned} 0 \cdot a = (0 + 0) \cdot a &= 0 \cdot a + 0 \cdot a \\ \implies 0 \cdot a &= 0 \cdot a + 0 \cdot a \\ \implies 0a + (-(0a)) &= 0a + 0a + (-(0a)) \\ \implies 0 &= 0a \end{aligned}$$

The other statement is very similar.

$$\text{QED}$$

**Proposition:**

Let $(R, +, \cdot)$ be a ring. Then, $\forall a, b \in R.\ a + b = b + a$.

**Proof:**

Let $a, b \in R$. We first show that

$$a + a + b + b = a + b + a + b$$
$$a + a + b + b = 1 \cdot a + 1 \cdot a + 1 \cdot b + 1 \cdot b$$
$$= (1 + 1) \cdot a + (1 + 1) \cdot b$$
$$= (1 + 1)(a + b)$$
$$= 1 \cdot (a + b) + 1 \cdot (a + b) = a + b + a + b$$

Which is what we wanted to show.

Finally, we cancel the $a$ on the left and the $b$ on the right to get

$$a + b = b + a$$
$$\text{QED}$$

**Example:**

Note that for a ring $(R, +, \cdot)$, $(R, \cdot)$ is not necessarily commutative.

Here's an example:

$$(\mathcal{M}_n(\mathbb{R}), +, \cdot)$$

for $n \geq 2$.

Where $+$ is element-wise addition and $\cdot$ is matrix multiplication.

We know that $\cdot$ is not commutative on $\mathcal{M}_n(\mathbb{R})$ when $n \geq 2$.

**Exercise:**

Let $(R, +, \cdot)$ with $0 \in R$ additive identity and $1 \in R$ multiplicative identity and $0 = 1$. Then, $|R| = 1$ and $R = \{0\}$.

**Recall:** In a ring, $+$ is always commutative.

**Definition:**

1. Let $(R, +. \cdot)$ with $a \in R$ and $R \neq \{0\}$. We say that $a$ is invertible in $R$ when $a$ is invertible in the monoid $(R, \cdot)$.
   - Note that we define this notion specifically for $(R, \cdot)$ because $(R, +)$ is a group, Thus, $a$ is always invertible in $(R, +)$.
2. $a$ is a zero-divisor in $R$ when $\exists b \in R, b \neq 0,\ a \cdot b = 0 \text{ or } b \cdot a = 0$

**Example:**

Consider the ring $(\mathbb{Z}_6, +, \cdot)$. Here, the invertible elements are $[a]$ such that $\gcd(a, 6) = 1$ (relatively prime).

**Proposition:**

An element $a$ of a ring $R$ cannot be both a zero divisor and invertible.

**Proof:**

Assume, for contradiction, that $a \in R$ is both a zero divisor and and invertible.

This means

$$a \cdot b = 0$$

for some $b \in R,\ b \neq 0$

Since $a$ is invertible, we know that we can multiply by $a^{-1}$ on both sides. Then, we get

$$b = 1 \cdot b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$$

$$\implies b = 0$$

which contradicts the assumption that $b \neq 0$.

$$\text{QED}$$

Therefore, every $a \in R$ is exactly one of the following:

1. A zero-divisor
2. Invertible
3. Neither

**Definition:**

A division ring is a ring in which every nonzero element is invertible.

**Definition:**

A field is a division ring where, in addition to $+$, $\cdot$ is also commutative.

**Theorem:**

A finite field must have cardinality $q = p^{\alpha}$, where $p$ is a prime number.

# Error correcting codes

We will be working with the field $\mathbb{F}_2 = \{0, 1\}$.

| $+$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $1$ |
| $1$ | $1$ | $0$ |

| $\cdot$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ |

Bob encodes his message as a string of $0$'s and $1$'s.

$$x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$$

We add an extra dimension to $x$ as follows

$$x_{n+1} = \begin{cases} 0 \ ; \ \text{there is an even number of 1s among the } x_1, \ldots, x_n \\ 1 \ ; \ \text{otherwise} \end{cases}$$

Consider the message

$$0110111$$

Here, something went wrong because this encoding doesn't follow the definition for $x_{n+1}$.

Note that, since we are in $\mathbb{F}_2$, we can define $x_{n+1}$ as

$$x_{n+1} = x_1 + \ldots . + x_n$$

Note that

$$x_1 + \ldots . + x_n + x_{n+1} = 0$$

because of the definition of $x_{n+1}$.

$$z = (z_1, \ldots, z_n, z_{n+1})$$

If $z_1 + \ldots + z_n + z_{n+1} \neq 0$, there is an odd number of errors.

If $z - 1 + \ldots + z_n + z_{n+1} = 0$, there are no errors or there is an even number of errors.

**K-fold repetition code:**

Suppose Bob's message is

$$x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$$

Then, we build

$$y = (\underbrace{x, \ldots, x}_{k}) \in \mathbb{F}_2^{kn}$$

Alice gets

$$z \in \mathbb{F}_2^{kn}$$

And Alice decodes to message to be the $z_i$ that appears the most number of times.

Lets assume that $k = 2m + 1$, $m \in \mathbb{Z}_{\geq 0}$, in our k-fold repetition code.

If $z \in \mathbb{F}_2^{kn}$, the word that Alice receives at most $m$ errors. Then, Alice decodes correctly.

Alice can detect up to $k - 1$ errors.