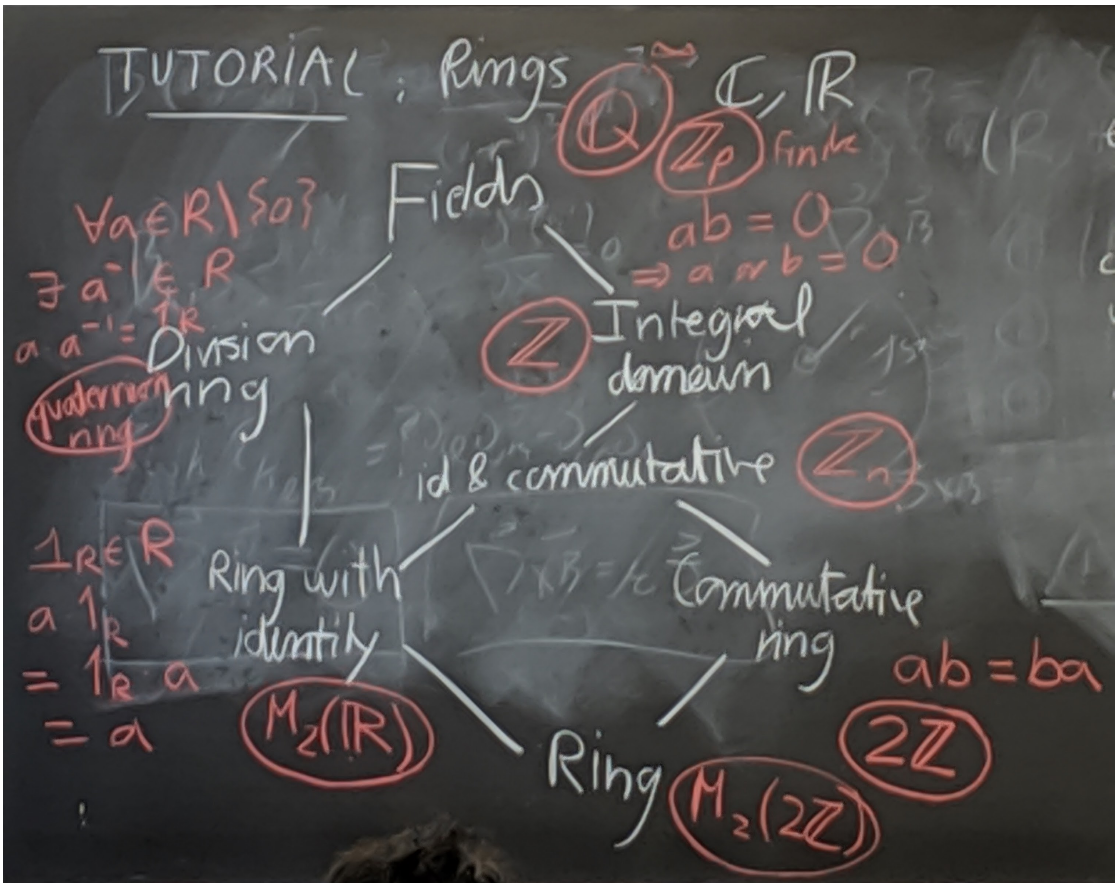
§1 Tutorial 11-15



Definition 1.1. $(R, +, \cdot)$ is a ring if

1. $(R, +)$ is an abelian group.
2. $(ab)c = a(bc)$.
3. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Caution: $(R, \cdot)$ is not a group.

Example 1.2

$(\mathbb{Z}, +, \cdot)$ is a ring.

1. $(\mathbb{Z}, +)$ is an abelian group.
2. 2 is satisfied.
3. 3 is satisfied.

Example 1.3

$(\mathbb{Z}, \cdot)$ is not a group because $\forall n \in \mathbb{Z}$, $n \neq 1, -1$, then $\nexists n^{-1} \in \mathbb{Z}$.

Exercise 1.4. Find an example for each type of ring.

1. Ring: $M_2(2\mathbb{Z})$ doesn't have the identity and isn't commutative.
2. Ring with Identity: $M_2(\mathbb{R})$. Matrix multiplication is not commutative but $M_2(\mathbb{R})$ contains the identity element.
3. Commutative Ring: $2\mathbb{Z}$. Commutative, but doesn't contain the multiplicative identity element.
4. Division Ring: Quaternion Ring
5. Identity and Commutative: $\mathbb{Z}_n$ where n is not prime. It has the identity and multiplication is commutative, but it is not an integral domain.
$$a, b \in \mathbb{Z}_n \text{ where } n = ab$$
but $a, b \neq 0$.
6. Integral Domain: $\mathbb{Z}$ because there is identity, multiplication is commutative, there aren't any zero divisors, but there aren't inverses for all elements.
7. Field: Examples include $\mathbb{Q}$ and $\mathbb{Z}_p$ where p is prime.

Example 1.5

Let R be a ring. $x \in R$ is idempotent if $x^2 = x$. Show that the only idempotent elements in an integral domain are 0 and 1.

Let $x \in \mathbb{R}$, where R is an integral domain, such that $x^2 = x$.

$$x^2 = x$$
$$\Rightarrow x^2 - x = 0$$
$$\Rightarrow x(x-1) = 0$$

Because R is an integral domain, this implies that x = 0 or x = 1

Note that the following argument would be incorrect because R is not a division ring:

$$x \neq 0$$
$$\Rightarrow x^{-1}x^2 = x^{-1}x$$
$$\Rightarrow x = 1$$

Theorem 1.6
Let R be an integral domain. Then $ab = ac \Rightarrow b = c$.

Example 1.7
In $\mathbb{Z}$ (an integral domain):

$$n \cdot m = n \cdot m'$$
$$\Rightarrow m = m'$$

In $\mathbb{Z}_6$ (not an integral domain):

$$3 \cdot 2 = 3 \cdot 4 = 0$$

but 2 is not equal to 4.

Example 1.8
Prove or disprove: R is a ring with identity 1_R. $S \subset R$ is a subring that has identity 1_S. Then does $1_R = 1_S$?

FALSE. Counter example:

$R = \mathbb{Z}_6$ ring with identity $1_R = 1$ and $S = \{0, 3\}$.

Subring conditions:

1. $S \neq \varnothing$
2. $r - s \in S \ \forall r, s \in S$

$$0 - 0 = 0 \in \mathbb{Z}_6$$
$$0 - 3 = 3 \in \mathbb{Z}_6$$
$$3 = 3 = 0 \in \mathbb{Z}_6$$

3. $r \cdot s \in \S \ \forall r, s \in S$

$$0 \cdot 0 = 0 \in \mathbb{Z}_6$$
$$0 \cdot 3 = 0 \in \mathbb{Z}_6$$
$$3 \cdot 3 = 3 \in \mathbb{Z}_6$$

But $1_R = 1 \neq 3 = 1_S$.

Example 1.9

Is $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ an integral domain?

1. Ring ✓
2. Identity 1 ✓
3. Commutative ✓

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i = (c + di)(a + bi)$$

   Follows because addition and multiplication in $\mathbb{Z}$ are commutative .

4. No zero divisors:

$$\begin{gathered}
\text{Assume } a + bi \neq 0 \\
(a + bi)(c + di) = 0 \\
\Rightarrow (a - bi)(a + bi)(c + di) \\
\Rightarrow \underbrace{(a^2 + b^2)}_{\in \mathbb{Z}}(c + di) \\
\text{Let } n = a^2 + b^2 \in \mathbb{Z} \\
\Rightarrow n(c + di) = 0 \\
\Rightarrow nc + ndi = 0 \\
\Rightarrow \begin{cases} nc = 0 \\ nd = 0 \end{cases} \quad \Rightarrow c = d = 0 \text{ because } \mathbb{Z} \text{ is an integral domain} \\
\Rightarrow c + di = 0
\end{gathered}$$

   Therefore there are no zero divisors because the only way to satisfy the equality is if $(c + di) = 0$.

Definition 1.10 (Ring homomorphism)**.** Ring homomorphism: Let $\varphi : R \to S$ where R, S are rings. Then:

$$\begin{gathered}
\varphi(a + b) = \varphi(a) + \varphi(b) \\
\varphi(ab) = \varphi(a)\varphi(b)
\end{gathered}$$

Definition 1.11 (Ideal)**.** Let $I \subset R$. I is an ideal if it is a subring such that $\forall r \in R$, $rI \subset I$ and $Ir \subset I$.

i.e. $\forall a \in I$, $\forall r \in R$, $ar \in I$ and $ra \in I$.

Example 1.12

Find all possible ring homomorphisms $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_{15}$.

First we will answer the following: what are all the possible group homomorphisms?

$\mathbb{Z}_6 = \langle 1 \rangle$ is cyclic so φ is defined by $\varphi(1)$. i.e.

$$\begin{gathered} 1 \to x \\ \Rightarrow n \to nx \end{gathered}$$

Also,

$$\begin{gathered} 0 = \varphi(0) = \varphi(6) = 6x \in \mathbb{Z}_{15} \\ \Rightarrow [6x]_{15} = 0 \\ \Rightarrow [2x]_5 = 0 \\ \Rightarrow [x]_5 = 0 \end{gathered}$$

So the possible values of x are $x = \{0, 5, 10\}$. Group homomorphisms:

$$\begin{gathered} \varphi_0 : 1 \to 0 \\ \varphi_5 : 1 \to 5 \\ \varphi_{10} : 1 \to 10 \end{gathered}$$

Are these also ring homomorphisms?

1. φ_0. ✓

$$\begin{gathered} 1 \to 0 \\ n \to 0 \\ \varphi(nm) = nm \cdot 0 = 0\varphi(n)\varphi(m) \end{gathered}$$

2. φ_5

$$\begin{gathered} 1 \to 5 \\ n \to 5n \\ \varphi(nm) = 5nm \\ \varphi(n)\varphi(m) = 5n \cdot 5m = 25nm = 10nm \\ 5nm \neq 10nm \text{ so not a ring homomorphism} \end{gathered}$$

3. φ_{10}. ✓

$$\begin{gathered} 1 \to 10 \\ n \to 10n \\ \varphi(nm) = 10nm \\ \varphi(n)\varphi(m) = 10n \cdot 10m = 100nm = 10nm \end{gathered}$$

So the ring homomorphisms from $\mathbb{Z}_6 \to \mathbb{Z}_{15}$ can be described by $\varphi(1) = 0$ and $\varphi(1) = 10$.