# Lecture 1: Rings and ideals.

**Ring**: Abelian group $R$ written additively with an associative distributive multiplication.
**Unital ring**: $\exists 1 \in R$ s.t. $1a = a1 = a \quad \forall a \in R$. 1 is called an identity.
**Commutative ring**: $xy = yx$, $x, y \in R$.

Exer. Identity is unique.

All rings will be commutative unless specified otherwise. Also all of them will have an identity 1.

We allow $1 = 0$, then $R = 0$.

**A unit**: $u \in R$ such that $\exists u^{-1} \in R$ with $uu^{-1} = 1$. I.e., a unit is an invertible element. $u^{-1}$ Also denoted $\frac{1}{u}$, called reciprocal or multiplicative inverse. Units in $R$ form the multiplicative group $R^\times$.

**Ring homomorphism (map)**: $\varphi: R \to R'$ preserving $+, \times$, and 1 (clearly $\varphi(R^\times) \subset R'^\times$). If $\varphi$ is bijective, then it's easy to show that $\varphi^{-1}$ is a homom. as well, and $\varphi$ is called an **isomorphism**.

homom. $\varphi: R \to R$ = endomorphism
isom. = automorphism

$R \subset R'$ **subring** if it's closed under $+, \times$, and contains 1. E.g. if $\varphi: R \to R'$ is a homom. then $\operatorname{Im}\varphi = \varphi(R) \subset R'$ is a subring. (called image of $\varphi$)

**$R$-algebra**: ring $R'$ such that we are given a ring map $\varphi: R \to R'$. Then can multiply elements of $R'$ by elements of $R$.

**$R$-algebra map:** $\psi: R' \to R''$ : a ring map compatible with mult. by $R$ (i.e., $R$-linear). Note: Any ring is a $\mathbb{Z}$-algebra, any ring map is a $\mathbb{Z}$-algebra map.

**Examples.** 1. $\mathbb{Z}$, the ring of integers.

2. $R[X_1, \dots, X_n]$ - ring of polynomials over $R$. E.g. $\mathbb{Z}[X_1, \dots, X_n]$, $\mathbb{C}[X_1, \dots, X_n]$.

**Ideal:** A subgroup $I \subset R$ in a ring $R$ such that $RI \subset I$. I.e. $\forall r \in R, x \in I, rx \in I$.

**Ex.** 1. $n\mathbb{Z} \subset \mathbb{Z}$

2. Let $I \subset \mathbb{Z}[x]$ be the set of polynomials that vanish at 0. Then $I$ is an ideal.

3. $I \subset \mathbb{Z}[x,y]$ polynomials vanishing on the circle $x^2+y^2=1$.

4. $0 \subset R$ is an ideal. Also $R \subset R$.

If $S \subset R$ then the **ideal generated by** $S$ $\langle S \rangle$ is the smallest ideal containing $S$. It consists of linear combinations $\sum_{i=1}^{n} a_i s_i$, where $a_i \in R$ and $s_i \in S$.

E.g. if $S = \{a\}$ then $\langle S \rangle = \langle a \rangle = Ra$ is the **principal ideal** generated by $a$

Universal property of $R[X_1, \ldots, X_n]$:
If $R'$ is an $R$-algebra then
$\mathrm{Hom}_{R\text{-algebras}}(R[X_1, \ldots, X_n], R') = R'^n$.

Indeed, if $\varphi: R[X_1, \ldots, X_n] \to R'$
then $\varphi|_R = \varphi$ and $\varphi(X_i)$ determine $\varphi$,
but they can be prescribed
arbitrarily.

---

Universal mapping property of $R/I$:
It's a ring $S$ together with a
map $\varphi: R \to S$ such that for any
$\psi: R \to T$ such that $\psi(I) = 0$
there exists a unique $\theta: S \to T$ such that
the diagram

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ & \searrow^{\psi} & \downarrow \theta \\ & & T \end{array}$$

is commutative,
$(\psi = \theta \circ \varphi)$

and the correspondence $\psi \leftrightarrow \theta$ is a
bijection.

Prop. $R/I$ is determined by this property.
If have another one $(S', \varphi')$, then
have $R \xrightarrow{\varphi} S \xrightarrow{\theta} S'$, $\theta'$, and $\theta \circ \theta' = \theta' \circ \theta = id$ by
uniqueness.

If $I, J \subset R$ are ideals, can form: new ideals (containing $I, J$).

sum $I+J = \{x+y \mid x \in I, y \in J\}$

intersection $I \cap J = \{x \mid x \in I \text{ and } x \in J\}$.

product $IJ = \{\sum_i x_i y_i, \; x_i \in I, y_i \in J\}$.

Note that $IJ \subset I \cap J$, but in general $IJ \neq I \cap J$.

Ex. $I = m\mathbb{Z} \subset \mathbb{Z}$, $J = n\mathbb{Z} \subset \mathbb{Z}$
$IJ = \langle mn \rangle$, $I \cap J = \langle LCM(m,n) \rangle$
$I + J = \langle GCD(m,n) \rangle$

Proper ideal: $I \neq R$.

$I = R \iff I$ contains a unit $(\iff I$ contains $1)$.

If $\varphi: R \to R'$ and $I \subset R$ then $R'\varphi(I) \subset R'$ extension of $I$, and for $I' \subset R'$, $\varphi^{-1}(I')$ contraction of $I'$

$\ker(\varphi)$ is an ideal. Conversely, $\forall I \subset R$, $R/I = R'$ is a ring, and (quotient ring, residue ring) $I = \ker\varphi$, $\varphi: R \to R'$, so any ideal is a kernel.

If $J \subset \ker\varphi$ then $\varphi$ descends to $\overline{\varphi}: R/J \to R'$. Univ. property: $\mathrm{Hom}(R/I, R') = \{\varphi: R \to R' \mid \varphi(I) = 0\}$.

We have an isom $\tilde{\varphi}: R/\ker\varphi \xrightarrow{\sim} \mathrm{Im}\,\varphi$.

Prop: $R$ a ring, $P \in R[X]$ the polynomial ring in 1 variable, $a \in R$, $\pi: P \to R$ ring map defined by $\pi(X) = a$. Then $\ker\pi = (X-a)$, so $R[X]/(X-a) \cong R$.

**Proof.** Given $f \in P$, the division algorithm gives $f(x) = g(x)(x-a) + b$, where $g \in P$ and $b \in R$. Then $\pi(f) = b$.

Hence $\ker \pi = (x-a)$, and

$R[x]/(x-a) \cong R$.

---

$R \supset I$ $\quad \pi : R \to R/I$. $\quad I \subset J$.

$J/I \subset R/I$ ideal

$R/J \cong \dfrac{R/I}{J/I}$.

---

**Idempotent:** $e \in R$, $e^2 = e$.

$Re \subset R$ is a ring with unit $e$ (not a subring in the usual sense!).

$e' = 1 - e$ also an idempotent.

It is called **complementary** to $e$.

So $e + e' = 1$, $ee' = 0$.

Conversely, if $e_1, e_2$ are idemp. s.t. $e_1 + e_2 = 1$ then $e_1 e_2 = 0$ and they are complementary.

**Product of rings:** $R \times S = \{(x,y) \mid x \in R, y \in S\}$ with the obvious operation (also denoted $R \oplus S$)

Let $R$ be a ring with complementary idempotents $e_1, e_2$. Let $R_1 = Re_1$ and $R_2 = Re_2$. Let $\varphi: R \to R_1 \times R_2$, $\varphi(x) = (xe_1, xe_2)$. Then $\varphi$ is a ring isomorphism.

Pf. It's clear that $\varphi$ is a homom. since $\varphi: R \to Re$, $\varphi(x) = xe$ is a homom. Now, $\varphi$ is injective since $xe_1 + xe_2 = x$. Also $\varphi$ is surjective since $\varphi(xe_1) = (xe_1, 0)$ and $\varphi(xe_2) = (0, xe_2)$, so $\varphi(xe_1 + ye_2) = (xe_1, ye_2)$.

Main example of a ring:

Let $f_1, \ldots, f_m$ be polynomials in $x_1, \ldots, x_n$ over $\mathbb{C}$.
We can consider algebraic set $X$ defined by $f_1(x_1, \ldots, x_n) = 0$

$$\vdots$$

$$f_m(x_1, \ldots, x_n) = 0.$$

Let $R = \mathcal{O}(X)$ be the ring of polynomial functions on $X$. (i.e. restrictions of polynomials to $X$).

Then $\mathcal{O}(X) = \mathbb{C}[x_1, \ldots, x_n]/I$, where $I = I(X)$ is the ideal of polynomials vanishing at $X$.

The ideal $I' = \langle f_1, \ldots, f_m \rangle$ is contained in $I$, but in general $I' \neq I$. Ex: $f = x^2$.

Hilbert's Nullstellensatz which we will discuss later states that

$$\sqrt{I'} = \{ f \mid f^N \in I' \text{ for some } N \}.$$