# Lecture 1

1) Rings.
2) Ring homomorphisms.
3) Ideals & quotient rings.

References: mostly Section 1,2 in Chapter 1 of [AM] (+examples that are not present there).

## 1) Definition:

Def: • a ring, $A$, is a set w. binary operations $+, \cdot : A\times A \to A$ s.t. (i) $A$ is an abelean group w.r.t. $+$ (in particular, $0\in A$, $a\in A \rightsquigarrow$ opposite $-a\in A$).

(ii) multipl'n $\cdot$ is associative $(ab)c = a(bc)$
• distributive $(a+b)c = ac+bc$, $c(a+b) = ca+cb$ $\forall a,b,c\in A$.

• $A$ is unital: $\exists$ (autom. unique) $1\in A$ s.t. $1a = a1 = a$ $\forall a\in A$.

• $A$ is commutative: $ab=ba$ $\forall a,b\in A$.

We always assume our rings are unital.
mostly — · — · — · — · — · commutative.

## 1.2) Examples & constructions.

0) $A=\{0\}$ $(1=0)$

1) Fields = comm've rings where every $a\neq 0$ has an inverse e.g. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$ etc.

2) $A=\mathbb{Z}$

3) Rings of polynomials: $A$ is a (comm've, unital) ring.

• $A[x] := \{ \text{polynomials } \sum_{i \geq 0} a_i x^i \mid a \in A \}$, usual addition & multiplication of polynomials (can take e.g. $A = \mathbb{Q}, \mathbb{C}$ or $\mathbb{Z}$ etc.)

• more general: $A[x_1, \dots, x_n]$ can be obtained by iterating previous constr'n, e.g. $A[x_1, x_2] = A[x_1][x_2]$

• even more general: for any set $I$ (finite or infinite) $\rightsquigarrow$ independent variables $x_i$, $i \in I$,

$A[x_i]_{i \in I} = \{$ finite $A$-linear combinations of finite monomials in the variables $x_i$, $i \in I \}$

4) Products: (comm've unital) rings $A_1, A_2$

$\rightsquigarrow$ product $A_1 \times A_2 = \{ (a_1, a_2) \mid a_i \in A_i \}$ w. componentwise $+, \cdot$

e.g. $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$.

More generally, for a set $I$ & rings $A_i$ $(i \in I) \rightsquigarrow \prod_{i \in I} A_i = \{ (a_i)_{i \in I} \}$.

5) <u>Subring</u> of a unital ring $A$ is a subset $B \subset A$ s.t.

• $B$ is a subgroup w.r.t. $+$

• $a, b \in B \Rightarrow ab \in B$.

• $1 \in B$

Then $B$ is a ring itself.

$$\left.\begin{array}{l} \text{e.g.} \cdot \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \\ \quad \cdot A \subset A[x] \text{ or } A[x_1, \dots x_{n-1}] \subset A[x_1, \dots x_n] \text{ etc.} \end{array}\right\} \text{examples of subrings.}$$

## 2) Ring homomorphisms

Definition: • Let $A, B$ be (comm've unital) rings

A map $\varphi: A \to B$ is a (unital ring) homomorphism if

i) $\varphi(a_1+a_2)=\varphi(a_1)+\varphi(a_2)$, $\varphi(a_1a_2)=\varphi(a_1)\varphi(a_2)$ $\forall a_1,a_2\in A$.

ii) $\varphi(1)=1$.

- We say that $B$ is an <u>$A$-algebra</u> if we have <u>fixed</u> a homomorphism $A\to B$.

Rem: · zero map $A\to B$ satisfies i) but not ii)

· example of algebra: $A[x]$ is an $A$-algebra with homom'm $a\mapsto a$ (deg 0 polynomial).

· our definition of algebra only works when $A,B$ comm've (will give a more gen'l def'n later)

Examples & constructions:

0) If $B\subset A$ is a subring, then inclusion $B\hookrightarrow A$ is a homom'm.

1) $\pi_i: A_1\times A_2\longrightarrow A_i$, $i=1,2$, $\pi_i(a_1,a_2)=a_i$ : homom'm

2) How to think about homom'ms $\Phi: A[x_1,..x_n]\to B$

$\varphi=\Phi|_A: A\to B$ homom'm; $b_i=\Phi(x_i)$, $i=1,...n$.

Conversely, from $\varphi: A\to B$ & $b_1,..b_n\in B$, uniquely recover $\Phi$:

$$\Phi\Big(\sum_\alpha a_\alpha x_1^{\alpha_1}\cdots x_n^{\alpha_n}\Big):=\sum_\alpha \varphi(a_\alpha)\, b_1^{\alpha_1}\cdots b_n^{\alpha_n}.$$

3) A ring homom'm $\mathbb{Z}\to B$ is unique b/c $1\mapsto 1$.

4) Compositions & inverses: · $\varphi: A\to B$, $\psi: B\to C$ homomorphisms $\Rightarrow \psi\circ\varphi: A\to C$ is also a homom'm

· $\varphi: A\to B$ a bijective homom'm $\Rightarrow \varphi^{-1}: B\to A$ is also a homom'm (exercise). Here we say that $\varphi$ is an <u>isomorphism</u>.

## 3) Ideals

$A$ is a comm've unital ring.

## 3.1) Definition & examples:

**Definition:** An ideal in $A$ is a subset $I \subset A$ s.t.

(i) $I$ is an abelian subgroup of $A$ w.r.t $+$, and

(ii) $\forall\, a \in A,\ b \in I \Rightarrow ab \in I$.

Examples/constructions:

1) $\varphi: A \to B$ ring homom'm. Then $\ker\varphi$ is an ideal (e.g. $a \in A, b \in \ker\varphi \Rightarrow \varphi(ab) = \varphi(a)\varphi(b) = 0 \Rightarrow ab \in \ker\varphi$); while $\operatorname{im}\varphi$ is a subring

2) $a_1, \dots, a_n \in A$. The ideal generated by $a_1 \dots a_n$: $(a_1, \dots a_n) = \{\sum_{i=1}^{n} b_i a_i \mid b_i \in A\}$. This is the minimal (w.r.t. $\subset$) ideal containing $a_1 \dots a_n$: if $I \subset A$ is ideal w. $a_1 \dots a_n \in I$ $\Rightarrow (a_1, \dots, a_n) \subset I$.

3) Every ideal in $\mathbb{Z}$ has the form $(n)$ for some $n \in \mathbb{Z}$.

Rem: an ideal $I$ isn't a subring unless $1 \in I \Leftrightarrow I = A$

Q: What are ideals in a field? A: $\{0\}$ or entire field b/c $a \in I \Rightarrow a^{-1}a \in I \Rightarrow 1 \in I \Rightarrow I$ coincides w. the whole field.

## 3.2) Quotient rings:

$I \subset A$ ideal in a ring $\rightsquigarrow$ quotient group $A/I = \{a + I \mid a \in A\}$ & group homom'm $\pi: A \to A/I$, $\pi(a) = a + I$.

depends only on $a+I, b+I$

Proposition: 1) The assignment $(a+I)\cdot(b+I) := \boxed{ab+I}$ defines a comm've unital ring str're on $A/I$ (w. unit $1+I$)

2) $\pi: A \to A/I$ is a ring homomorphism (moreover, the ring str're on $A/I$ is unique s.t. $\pi$ is a ring homomorphism)

3) Universal property for $A/I$ & $\pi$:

let $\varphi: A \to B$ be a ring homom'm s.t. $I \subset \ker\varphi$. Then $\exists!$ ring homom'm $\bar{\varphi}: A/I \longrightarrow B$ s.t. $\varphi = \bar{\varphi}\circ\pi$ i.e. the following diagram is comm've:

there's unique.

$$\begin{tikzcd} A \arrow[d, "\pi"'] \arrow[dr, "\varphi"] & \\ A/I \arrow[r, dashed, "\bar{\varphi}"'] & B \end{tikzcd}$$

Proof: exercise.

Examples: 1) $A = \mathbb{Z}$, $I = (n)$ $(= n\mathbb{Z})$, $A/I = \mathbb{Z}/n\mathbb{Z}$ - residues mod $n$.

2) $A = \mathbb{Z}[x]$, $d \in \mathbb{Z}$ not a complete square, $I := (x^2 - d) \subset A$.

$A/I = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ (remark $\sqrt{d} = \pi(x)$)

Formally, $A/I = \mathbb{Z}[\sqrt{d}]$ is a consequence of (3):

$$\begin{tikzcd} \mathbb{Z}[x] \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & \mathbb{Z}[\sqrt{d}] \\ & \mathbb{Z}[x]/(x^2-d) \arrow[u, dashed, "\bar{\varphi}"'] \end{tikzcd}, \quad x \mapsto \sqrt{d} \Rightarrow \varphi(x^2 - d) = 0$$

Exercise: $\bar{\varphi}$ is surjective & injective

Injectivity: every coset $a + \mathbb{Z}[x](x^2-d)$ has a unique repres've of the form $a + bx$.

Remarks (added 9/3) : I) $\bar{\varphi}$ is surj've $\Leftrightarrow$ $\varphi$ is surj've

$\bar{\varphi}$ is injective $\Leftrightarrow$ $\ker\varphi = I$.

II) $\exists$ natural bijections between:

$$\begin{array}{ccc} \pi^{-1}(\underline{J}) \in \{\text{ideals } J\subset A \mid J\supset I\} \ni J \\ \uparrow & & \downarrow \\ \underline{J} \in \{\text{ideals } \underline{J}\subset A/I\} \ni \pi(J)=J/I \end{array}$$

Useful when we study inclusions $I\subset J$ - ideals in $A$. For some questions we encounter, can replace $I\subset J\subset A$ w. $\{0\}\subset J/I\subset A/I$.

BONUS: noncommutative counterparts, part 1.

Nonunital (but commutative) rings are not particularly important so we do not consider them. But noncommutative (unital) rings are of great importance. In this bonus & 2 subsequent ones, I'll explain how various constructions in the main body of the lectures work in the noncommutative setting.

B1) Examples. Below $A$ stands for a unital ring.

1) Fix $n\in\mathbb{Z}_{>0}$. We can consider the ring $Mat_n(A)$ of $n\times n$ matrices w. coefficients in $A$ w. usual matrix addition & multiplication.

Exercise: Identify $Mat_m(Mat_n(A))$ with $Mat_{mn}(A)$.

2) Noncommutative polynomials:

Let $x_1,..x_n$ be variables. By a noncommutative monomial we mean a word in the alphabet $x_1,..x_n$. They are multiplied by concatenation. The ring $A\langle x_1,..x_n\rangle$ of noncommutative polynomials consists of $A$-linear combination of noncommutative monomials w. natural addition & multiplication (elements of $A$ commute with the $x$'s).

Exercise: Give a description of homomorphisms $A\langle x_1,\dots x_n\rangle \to B$ similarly to what was done in the lecture for the usual polynomials.

3) Group ring: let $A$ be commutative. Take a group $G$. The group ring $AG$ by definition consists of finite linear combinations $\sum_{g\in G} a_g g$, $a_g \in A$, w. natural addition, and with multipl.n extending that in $G$ by distributivity. This construction is very important in the study of representations of $G$ (take MATH 353 in the Spring for more on this).

B2) Ideals in noncommutative rings.

The multiplication is no longer commutative so we get three versions of ideals.

Definition: • A <u>left ideal</u> in $A$ is a subset $I\subset A$ s.t.

1) $I$ is an abelian subgroup of $A$ (w.r.t. $+$)

2) $\forall\, a\in A, b\in I \Rightarrow ab\in I$.

• A right ideal is a similar thing but in 2) we require $ba\in I$.

• A two-sided ideal is a subset that is both left & right ideal.

Exercise: Let $\varphi: A\to B$ be a ring homomorphism. Then $\ker\varphi$ is a two-sided ideal.

For a two-sided ideal $I\subset A$ can form the quotient ring

A/I. It enjoys properties analogous to Proposition from Sect. 3.2.

Example (of importance for Quantum Physics). The (first) Weyl algebra; let $\mathbb{F}$ be a field. Then we consider

$$\mathrm{Weyl}_1 := \mathbb{F}\langle x,y\rangle / (xy-yx-1)$$

2-sided ideal generated by $xy-yx-1 \in \mathbb{F}\langle x,y\rangle$.

Premium exercise: $\mathrm{Weyl}_1$ has a $\mathbb{F}$-basis of ordered monomials $x^i y^j$ ($i,j \in \mathbb{Z}_{\geq 0}$)

"Premium": to be tried at your own risk.