Lecture 1: Rings, ideals & modules I.

1) Rings.
2) Ring homomorphisms.
3) Ideals

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

BONUS: Non-commutative counterparts.

1.1) Definition:

Def: A (unital, associative) ring is a set A together w. two maps, $+, \cdot : A\times A \to A$ (addition & multiplication) s.t.

(i) A is an abelian 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: $(a+b)c = ac+bc$, $c(a+b) = ca+cb$

$\Big\}\ \forall a,b,c\in A$

- has unit: $\exists$ (autom. unique) $1\in A$ s.t. $1a = a1 = a$ $\forall a\in A$.

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

In this course we will mostly consider commutative rings.

1.2) Examples & constructions.

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

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

2) $A=\mathbb{Z}$.

3) Rings of polynomials: A is a (comm've) ring. (can take e.g. $A=\mathbb{Q}, \mathbb{C}$ or $\mathbb{Z}$ etc.)

- $A[x]=\{$polynomials $\sum_{i\geq 0} a_i x^i \mid a_i\in A$, fin. many $\neq 0\}$, usual addition & multiplication of polynomials.

- more general: $A[x_1,\dots,x_n]=\{$polynomials $\sum_{i_1,\dots i_n\geq 0} a_{i_1\dots i_n} x_1^{i_1}\dots x_n^{i_n}$ $a_{i_1,\dots i_n}\in A\}$ can be obtained by iterating the previous constr'n, for example, $A[x_1,x_2]=A[x_1][x_2]$.

- variation: Laurent polynomials $A[x^{\pm 1}]=\{\sum_{i\in\mathbb{Z}} a_i x^i \mid a_i\in A$, fin. many nonzero$\}$.

4) Products: (comm've) 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. $(a_1,a_2)(b_1,b_2)=(a_1b_1, a_2b_2)$.

Def: A subring of a 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 (commutative if A is).

Examples (of subrings)

- $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
- $A \subset A[x]$, $A[x_1, \ldots x_{n-1}] \subset A[x_1, \ldots x_n]$, $A[x] \subset A[x^{\pm 1}]$.

2) Ring homomorphisms

Def: Let A, B be rings. A map $\varphi: A \to B$ is a ring homomorphism if:

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

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

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

Examples & constructions:

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

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

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

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

Conversely, from $\varphi: A \to B$ & $b_1, \dots b_n \in B$, uniquely recover Φ:
$\Phi\left(\sum_{i_1 \dots i_n} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}\right) := \sum_\alpha \varphi(a_\alpha)\, b_1^{\alpha_1} \dots b_n^{\alpha_n}$.

3) A ring homom'm $\mathbb{Z} \to B$ is unique b/c $1 \mapsto 1$, it's given by $n \mapsto n \cdot 1$.

4) Compositions & inverses: • $\varphi: A \to B$, $\psi: B \to C$ homomorphisms $\Rightarrow \psi \circ \varphi: A \to C$ is also a homomorphism.

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

Exer: The image of a ring homomorphism is a subring.

3) Ideals

A is a commive ring

3.1) Definition & examples:

Def. An ideal in A is a subset $I \subset A$ s.t.

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

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

Examples/constructions:

0) $\{0\} \subset A$, $A \subset A$ are ideals.

1) Let $\varphi: A \to B$ be ring homom'm. Then $\ker\varphi$ is an ideal (e.g. $a \in A, b \in \ker\varphi \Rightarrow \varphi(ab) = \varphi(a)\varphi(b) = 0 \Rightarrow ab \in \ker\varphi$).

2) $a_1, \ldots, a_n \in A$. The **ideal generated by $a_1 \ldots a_n$** is defined by $(a_1, \ldots a_n) := \{\sum_{i=1}^{n} b_i a_i \mid b_i \in A\}$. More generally, let X be a set & a_x for $x \in X$ be elements of A. Then the ideal generated by the elements a_x is $(a_x \mid x \in X) := \{\sum_{i=1}^{k} b_i a_{x_i}$ for $k \geq 0$ & $x_1, \ldots x_k \in X\}$ - finite A-linear combinations of el'ts a_x. $(a_x \mid x \in X)$ is the minimal (w.r.t. $\subset$) ideal containing all a_x: if $I \subset A$ is ideal w. $a_x \in I$ $\Rightarrow (a_x \mid x \in X) \subset I$. The proofs are left as exercises.

Definition: An ideal of the form $(a_1, \ldots a_n)$ for some $n \in \mathbb{Z}_{\geq 0}$, equiv. $(a_x \mid x \in X)$ w. X finite, is called **finitely generated**. An ideal of the form (a) is called **principal**.

Rem: In reasonable ("Noetherian") rings <u>all</u> ideals are finitely generated. An example of such a ring is $\mathbb{F}[x_1, \ldots x_n]$, where $\mathbb{F}$ is a field - we'll prove a more general result (Hilbert basis theorem) a bit later in the course. It's quite rare that all ideals are principal. We'll discuss the most important class of rings, where this holds - principal ideal domains - also later in the course.

3) Every ideal in $\mathbb{Z}$ or $\mathbb{F}[x]$, where $\mathbb{F}$ is a field, is principal.

Rem: For an ideal $I \subset A$, the equality $I = A$ is equivalent to $1 \in I$. Further, if I contains an invertible element, say a, then $1 = aa^{-1} \in I \Rightarrow I = A$. In particular, any field $\mathbb{F}$ has exactly 2 ideals, $\{0\}$ & $\mathbb{F}$.

Exercise (to be used later) Let A be a (commutative) ring. Suppose $\{0\}$ & A are the only 2 ideals in A, and they are distinct. Show A is a 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 $\pi : A \to A/I$, $\pi(a) := a + I$.

Proposition: 0) For $a, b \in A$, the element $ab + I \in A/I$ depends only on $a + I$, $b + I$ and not on a, b themselves.

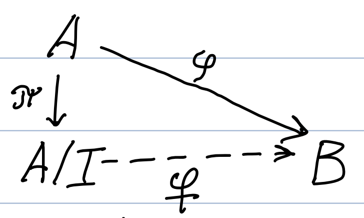
1) The assignment $(a+I)\cdot(b+I) := ab + I$ defines a commutative ring str're on A/I (w. unit $1 + I$).

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

3) "Universal property" for A/I & π:

Let $\varphi : A \to B$ be a ring homom'm s.t. $I \subset \ker\varphi$. Then $\exists!$ (notation means: there's unique) ring homom'm $\bar{\varphi} : A/I \longrightarrow B$ s.t. $\varphi = \bar{\varphi} \circ \pi$.

Equalities of homomorphisms like this are often depicted as "commutative diagrams". The homomorphisms are depicted as arrows and dashed arrows are used for homomorphisms whose existence and uniqueness we seek to establish. For example, the claim of 3) is represented by a commutative diagram as follows:



Proof (of Proposition): exercise.

Exercise 1: Show that φ is surjective $\Leftrightarrow$ $\bar{\varphi}$ is. Further show $\bar{\varphi}$ is injective $\Leftrightarrow$ $\ker\varphi = I$.

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 (assoc've, unital) ring.

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

Exercise: Identify $\operatorname{Mat}_m(\operatorname{Mat}_n(A))$ with $\operatorname{Mat}_{mn}(A)$.

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 $A\langle x_1,..x_n\rangle\to B$ 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.

B2) Ideals in noncommutative rings.

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

Definition: • A left ideal 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: Weyl_1 has a $\mathbb{F}$-basis of <u>ordered</u> monomials $x^i y^j$ $(i,j \in \mathbb{Z}_{\geq 0})$

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