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).

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, special cases & 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 $\sum_{i \geq 0} a_i x^i \mid a \in A\}$, usual addition & multiplication of polynomials.

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

• even more general: for any set I (finite or infinite)
$\rightsquigarrow$ independent variables x_i, $i \in I$,
$A[x_i]_{i \in I} = \{$ polynomials in finitely many of the variables x_i, $i \in I\}$
Note that $A[x_i]_{i \in I}$ is comm've.

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. $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$.
More generally, for a set I & rings A_i $(i \in I) \rightsquigarrow \prod_{i \in I} A_i$.
$= \{(a_i)_{i \in I}\}$.

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)
- $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
- $A \subset A[x]$ or $A[x_1, \dots x_{n-1}] \subset A[x_1, \dots x_n]$ etc.

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)

Def: Suppose A & B are commutative. We say that B is an A-algebra if we have fixed a homomorphism $A \to B$.

For example, $A[x]$ is an A-algebra via the homomorphism $a \mapsto a$ (deg 0 polynomial).

Later, we will generalize this definition to the case when B doesn't need to be commutative.

Examples & constructions:

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

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

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

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

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

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

3) A ring homom'm $\mathbb{Z} \to B$ is unique b/c $1 \mapsto 1$, 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 comm've ring (in general, the situation is more complicated, we'll consider it in the Bonus section).

3.1) Definition & examples:

Def. 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:

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

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

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 $\pi: A \to A/I$, $\pi(a) := a+I$.

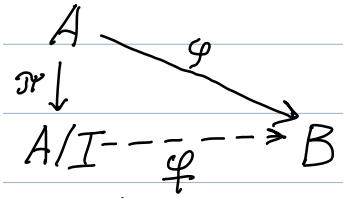
Proposition: 0) For $a, b \in A$, the element $ab+I \in A/I$ depends only on $a+I$, $b+I$ and not on a, b themselves.

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 $\bar{\varphi}: A/I \to B$ s.t. $\varphi = \bar{\varphi} \circ \pi$.

Equalities of homomorphism 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: Show that φ is surjective $\Leftrightarrow$ $\bar{\varphi}$ is. Further

show φ is injective $\Leftrightarrow \ker\varphi = I$.

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, $I:=(x^2-d)\subset A$. Then A/I is naturally identified with the subring $\mathbb{Z}[\sqrt{d}]:=\{a+b\sqrt{d} \mid a,b\in\mathbb{Z}\}$ of $\mathbb{C}$.

Exercise: Deduce an isomorphism $A/I\simeq\mathbb{Z}[\sqrt{d}]$ by using 3) of Proposition. Namely, consider the homomorphism $\varphi: \mathbb{Z}[x]\longrightarrow\mathbb{Z}[\sqrt{d}]$ given by $f(x)\mapsto f(\sqrt{d})$. Show that φ from 3) is an isomorphism by checking that it's surjective & injective.

Exercise: Here we compare sets of ideals in A & in A/I. Namely show that the following maps are mutually inverse bijections:

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

The last exercise is often useful when we study inclusions of ideals $I\subset J\subset A$. We could try to replace this triple w. $\{0\}\subset J/I\subset A/I$ & assume the smaller ideal is zero.

Exercise: Let $\varphi: A \to B$ be a ring homomorphism & $F_1 \dots F_m \in A[x_1 \dots x_n]$. Then to give a ring homomorphism $\Phi: A[x_1 \dots x_n]/(F_1 \dots F_m) \to B$ s.t. the composition $A \to A[x_1 \dots x_n] \twoheadrightarrow A[x_1 \dots x_n]/(F_1 \dots F_m) \xrightarrow{\Phi} B$ is φ (here we usually view B as an A-algebra via φ so Φ has to be an A-algebra homomorphism) is equivalent to picking elements $b_1 \dots b_n \in B$ s.t. ${}^{\varphi}F_i(b_1 \dots b_n) = 0 \ \forall\, i = 1, \dots m$. Here ${}^{\varphi}F_i \in B[x_1 \dots x_n]$ is obtained from $F_i \in A[x_1 \dots x_n]$ by applying φ component-wise. This generalizes Example 2 from Section 2.

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 $\mathrm{Mat}_n(A)$ of $n \times n$ matrices w. coefficients in A w. usual matrix addition & multiplication.

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

2) Noncommutative polynomials:

Let $x_1 \dots x_n$ be variables. By a noncommutative monomial we

mean a word in the alphabet $x_1, \dots x_n$. They are multiplied by concatenation. The ring $A\langle x_1, \dots x_n\rangle$ 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.

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

$$Weyl_1 := \mathbb{F}\langle x,y\rangle/(xy-yx-1)$$

$\leftarrow$ 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 ordered monomials $x^i y^j$ $(i,j \in \mathbb{Z}_{\geq 0})$

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