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, $+: A \times A \to A$ (addition & multiplication) s.t.
(i) $A$ is an abelian group w.r.t. $+$ (in particular, $0 \in A$, $a \in A \Rightarrow$ opposite $-a \in A$).
(ii) multiplication, $\cdot$, is

- associative: $(ab)c = a(bc)$
- distributive: $(a+b)c = ac + bc, c(a+b) = ca + cb$
- 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) Field’s = comm’tive 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’tive) ring.
   (can take, e.g., $A = \mathbb{Q}, \mathbb{C}$ or $\mathbb{Z}$ etc.)
   \[ A[x] = \{ \text{polynomials } \sum_{i=0}^{\infty} a_i x^i | a_i \in A \}, \text{ usual addition & multiplication of polynomials}. \]

   • 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)
     ~ independent variables $x_i, i \in I$,
     \[ A[x_i]_{i \in I} = \{ \text{polynomials in finitely many of the} \]
     \[ \text{variables } x_i, i \in I \} \]
     Note that $A[x_i]_{i \in I}$ is comm’tive.

4) Products: (comm’tive) rings $A_1, A_2$

   ~ product $A_1 \times A_2 = \{(a_1, a_2) | a_i \in A_i \}$ w. componentwise $+$.
   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 $A_i (i \in I)$ ~ \[ \prod_{i \in I} A_i. \]
   \[ \{ (a_i)_{i \in I} \mid \sum_i a_i = 0 \} \]
**Def:** A **subring** of a ring $A$ is a subset $B \subseteq A$ 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)
- $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$
- $A \subseteq A[x]$ or $A[x_1, \ldots, x_n] \subseteq A[x_1, \ldots, x_n]$ etc.

2) **Ring homomorphisms**

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

i) $g(a + b) = g(a) + g(b)$, $g(ab) = g(a)g(b) \ \forall a, b \in A$

ii) $g(1) = 1$

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:

1) If $B \subseteq A$ is a subring, then the inclusion $B \rightarrow A$ is a homomorphism.

2) How to think about homomorphisms $\Phi: A[x_1, \ldots, x_n] \rightarrow B$

   $\varphi = \Phi|_A: A \rightarrow B$ is a homomorphism; $b_i = \Phi(x_i), i = 1, \ldots, n$.

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

   $\Phi(\sum a \cdot x_1^{e_1} \cdots x_n^{e_n}) = \sum \varphi(a \cdot) b_1^{e_1} \cdots b_n^{e_n}$.

3) A ring homomorphism $\mathbb{Z} \rightarrow B$ is unique if 1-to-1, it's given by $n \mapsto n \cdot 1$.

4) Compositions & inverses: $\varphi: A \rightarrow B$, $\psi: B \rightarrow C$ homomorphisms

   $\Rightarrow \psi \circ \varphi: A \rightarrow C$ is also a homomorphism.

   $\varphi: A \rightarrow B$ a bijective homomorphism $\Rightarrow \varphi^{-1}: B \rightarrow A$ is also a homomorphism (exercise). Here we say that $\varphi$ is an isomorphism.

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

3) Ideals $A$ is a commutative 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 $I \subseteq A$ 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) $\{0 \}$ and $A$ are ideals.

1) Let $\phi : A \rightarrow B$ be ring homomorphism. Then $\ker \phi$ is an ideal (e.g. $a \in A, b \in \ker \phi \Rightarrow \phi(ab) = \phi(a) \phi(b) = 0 \Rightarrow ab \in \ker \phi$).

2) $a_1, \ldots, a_n \in A$. The ideal generated by $a_1, \ldots, a_n$ is defined by
   
   $$(a_1, \ldots, a_n) = \{ \sum_i b_i a_i \mid b_i \in A \}.$$  
   
   This is the minimal (w.r.t $\subseteq$) ideal containing $a_1, \ldots, a_n$; if $I \subseteq A$ is ideal w. $a_1, \ldots, a_n \in I$ \n   \Rightarrow (a_1, \ldots, a_n) \subseteq I.$

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

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

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**: $I \subseteq A$ ideal in a ring $\rightarrow$ quotient group 

$A/I := \{a+I \mid a \in A\}$ & group homomorphism $\phi: A \rightarrow A/I$, 

$\phi(a) := a + I$.

**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 $(a + I), (b + I) := ab + I$ 
defines a commutative ring structure on $A/I$ (w. unit 1+I). 
2) $\phi: A \rightarrow A/I$ is a ring homomorphism (moreover, the ring structure on $A/I$ is unique s.t. $\phi$ is a ring homomorphism). 
3) Universal property for $A/I$ & $\phi$: 

let $g: A \rightarrow B$ be a ring homomorphism s.t. $I \subseteq \ker g$. Then 

$\exists!$ (notation means: there's unique) ring homomorphism $\bar{g}: A/I \rightarrow B$ s.t. $g = \bar{g} \circ \phi$.

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 fellows:

$\begin{array}{cccc}
A & \xrightarrow{\phi} & A/I & \xrightarrow{\bar{g}} & B \\
\phi \downarrow & & \phi & & \\
A/I & \rightarrow & B
\end{array}$

**Proof (of Proposition)**: exercise.

**Exercise**: Show that $g$ is surjective $\iff \bar{g}$ is. Further
show \( \varphi \) is injective \( \iff \) \( \ker \varphi = I \).

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 \( \mathbb{Z}[\sqrt{d}] := \{ a + b\sqrt{d} | a, b \in \mathbb{Z} \} \) of \( \mathbb{C} \).

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

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

\[
\begin{align*}
\pi : \{ \text{ideals } J \subset A \mid J \supset I \} & \cong J \\
\uparrow \\
\{ \text{ideals } J \subset A/I \} & \cong \pi^{-1}(J) = J/I
\end{align*}
\]

The last exercise is often useful when we study inclusions of ideals \( I \subseteq J \subset A \). We could try to replace this triple \( \{0\} \subseteq J/I \subset A/I \) & assume the smaller ideal is zero.
Exercise: Let \( \varphi: A \rightarrow B \) be a ring homomorphism & \( F_1, \ldots, F_m \in A[x_1, \ldots, x_n] \). Then to give a ring homomorphism \( \tilde{\varphi}: A[x_1, \ldots, x_n]/(F_1, \ldots, F_m) \rightarrow B \) s.t. the composition \( A \rightarrow A[x_1, \ldots, x_n] \rightarrow A[x_1, \ldots, x_n]/(F_1, \ldots, F_m) \varphi \rightarrow B \) is \( \varphi \) (here we usually view \( B \) as an \( A \)-algebra via \( \varphi \) so \( \varphi \) has to be an \( A \)-algebra homomorphism) is equivalent to picking elements \( b_1, \ldots, b_n \in B \) s.t. \( \varphi_i(b_1, \ldots, b_n) = 0 \forall i = 1, \ldots, m \). Here \( \varphi_i \in B[x_1, \ldots, x_n] \) is obtained from \( F_i \in A[x_1, \ldots, x_n] \) by applying \( \varphi \) 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 (associative, unital) ring.

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

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

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

Exercise: Give a description of homomorphisms $A\langle x_1, \ldots, x_n \rangle \rightarrow B$ 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 $\sum g_j a_j, a_j \in A$, with natural addition, and with multiplication 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 $I \subseteq A$ s.t.

1) $I$ is an abelian subgroup of $A$ (wrt. $+$)

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

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

9}
A two-sided ideal is a subset that is both left and right ideal.

Exercise: Let \( g: A \to B \) be a ring homomorphism. Then \( \ker g \) 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 \( F \) be a field. Then we consider

\[
\text{Weyl}_1 = F \langle x, y \rangle / (xy - yx - 1)
\]

2-sided ideal generated by

\[
xy - yx - 1 \in F \langle x, y \rangle.
\]

Premium exercise: Weyl has a \( F \)-basis of ordered monomials \( x^iy^j \) \((i,j \in \mathbb{Z}_0)\).

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