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 $+: A \times A \to A$

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 is associative $(ab)c = a(bc) \quad \forall a, b, c \in A$.

- distributive $(a+b)c = ac + bc$, $c(a+b) = ca + cb$.

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

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

We always assume our rings are unital. mostly $\ldots$ commutative.

1.2) Examples & constructions

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

1) Fields = comm. 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., unital) ring.
\[ A[x] := \left\{ \text{polynomials } \sum_{i=0}^{\infty} a_i x^i \mid a_i \in A \right\} \text{, usual addition \& multiplication of polynomials (can take e.g. } A = \mathbb{Q}, \mathbb{C} \text{ or } \mathbb{Z} \text{ etc.)} \]

- more general: \[ A[x_1, \ldots, x_n] \text{ can be obtained by iterating previous constr'n, e.g. } A[x_1, x_2] = A[x_1][x_2] \]
- even more general: for any set \( I \) (finite or infinite) \( \{ \) independent variables \( x_i, i \in I \),

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

4) Products: (commute unital) rings \( A, A_2 \)

- product \( A_1 \times A_2 = \left\{ (a_1, a_2) \mid a_1 \in A_1; \right\} \text{ w. componentwise +, e.g. } (a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \).

- More generally, for a set \( I \) \& rings \( A_i (i \in I) \rightarrow \prod_{i \in I} A_i = \left\{ (a_i)_{i \in I} \right\} \).

5) Subring 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.

- \( \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \) \( \{ \) examples of \( \{ \)

- \( A \subset A[x] \text{ or } A[x_1, \ldots, x_n] \subset A[x_1, \ldots, x_n] \text{ etc.} \) \( \{ \) subrings.

2) Ring homomorphisms

Definition: \( \) Let \( A, B \) be (commute unital) rings

A map \( \psi: A \rightarrow B \) is a (unital ring) homomorphism if
i) \( \varphi(q+2) = \varphi(q) + \varphi(2), \varphi(q_1) = \varphi(q_1) \varphi(q_2) \quad \forall q, q_1, q_2 \in A \).

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

We say that \( B \) is an \textbf{\textit{\textbf{A}}-algebra} if we have fixed a homomorphism \( A \rightarrow B. \)

Rem: zero map \( A \rightarrow B \) satisfies i) but not ii).

- example of algebra: \( A[x] \) is an \( A \)-algebra with homomorph \( a \mapsto a \) (deg 0 polynomial).
- our definition of algebra only works when \( A, B \) commute (will give a more gen'l def'n later)

Examples & constructions:

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

2) How to think about homomorphisms \( \varphi: A[x, \ldots, x_n] \rightarrow B \):
   \[ \varphi = \varphi|_A: A \rightarrow B \text{ homomorphism}; \ b_i = \varphi(x_i), i = 1, \ldots, n. \]
   Conversely, from \( \varphi: A \rightarrow B \) & \( b_1, \ldots, b_n \in B \), uniquely recover \( \varphi: \)
   \[ \varphi(\sum \alpha_{\xi} x_{\xi}^{\xi_1} \cdots x_{\nu}^{\nu_1}) = \sum \varphi(\alpha_{\xi}) b_{\xi_1} \cdots b_{\nu_1}. \]

3) A ring homomorphism \( \mathbb{Z} \rightarrow B \) is unique by \( 1 \mapsto 1. \)

4) Compositions & inverses: \( \varphi: A \rightarrow B, \psi: B \rightarrow C \) homomorphisms
   \[ \Rightarrow \psi \circ \varphi: A \rightarrow C \text{ is also a homomorphism}. \]
   \( \varphi: A \rightarrow B \) a bijective homomorphism \( \Rightarrow \varphi^{-1}: B \rightarrow A \) is also a homomorphism (exercise). Here we say that \( \varphi \) is an \textbf{\textit{\textbf{isomorphism}}.}

3) **Ideals** \( A \) is a commutative unital rng.
3.1) Definition & examples:

**Definition:** 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:**

1) $\varphi: A \to B$ ring homomorphism. 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 $\text{im} \varphi$ is a subring.

2) $q_1, \ldots, q_n \in A$. The ideal generated by $q_1, \ldots, q_n$:

$\langle q_1, \ldots, q_n \rangle = \{ \sum_{i=1}^{n} b_i q_i \mid b_i \in \mathbb{Z} \}$. This is the minimal (w.r.t. $\subseteq$) ideal containing $q_1, \ldots, q_n$: if $I \subseteq A$ is ideal w. $q_1, \ldots, q_n \in I \Rightarrow \langle q_1, \ldots, q_n \rangle \subseteq I$.

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: $\langle 0 \rangle$ or entire field $\mathbb{C}$.

$a \in I \Rightarrow a^{-1} a \in I \Rightarrow 1 \in I \Rightarrow I$ coincides w. the whole field.

3.2) Quotient rings: $I \subseteq A$ ideal in a ring $\Rightarrow$ quotient group

$A/I = \{a + I \mid a \in A\}$ & group homomorphism $\pi: A \to A/I$, $\pi(a) = a + I$ (depends only on $a + I, b + I$)

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

2) $\pi: A \to A/I$ is a ring homomorphism (moreover, the ring structure on $A/I$ is unique s.t. $\pi$ is a ring homomorphism).
3) Universal property for \( A/I \& \phi \):

Let \( \phi : A \rightarrow B \) be a ring homomorphism such that \( I \subseteq \ker \phi \). Then there exists a unique ring homomorphism \( \overline{\phi} : A/I \rightarrow B \) s.t. \( \phi = \overline{\phi} \circ \pi \), where \( \pi \) is the natural projection from \( A \) to \( A/I \).

\[
\begin{array}{ccc}
A & \xrightarrow{\phi} & B \\
\pi \downarrow & & \downarrow \\
A/I & \xrightarrow{\overline{\phi}} & B
\end{array}
\]

Proof: exercise.

Examples:
1) \( A = \mathbb{Z} \), \( I = (n) \ (\text{a prime}) \), \( A/I = \mathbb{Z}/n\mathbb{Z} \) - residues modulo \( n \).

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

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

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

\[
\begin{array}{ccc}
\mathbb{Z}[x] & \xrightarrow{\phi} & \mathbb{Z}[\sqrt{d}] \\
\downarrow & & \downarrow \phi \\
\mathbb{Z}[x]/(x^2 - d) & \xrightarrow{\bar{\phi}} & \mathbb{Z}[\sqrt{d}]
\end{array}
\]

Exercise: \( \phi \) is surjective & injective.

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

Remarks (added 9/3):
1) \( \phi \) is surjective \( \Leftrightarrow \phi \) is surjective

\( \phi \) is injective \( \Leftrightarrow \ker \phi = I \).

II) \( \exists \) natural bijections between:
\[ x^y \in \{ \text{ideals } J \subseteq A \mid J \supseteq I \} \]

Useful when we study inclusions \( I \subseteq J \) - ideals in \( A \). For some questions we encounter, can replace \( I \subseteq J \subseteq A \) w. \( \exists J/I \subseteq A/I \).

**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 \( n \in \mathbb{N} \). 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 \( x_1, x_2 \) be variables. By a noncommutative monomial we mean a word in the alphabet \( x_1, x_2 \). They are multiplied by concatenation. The ring \( A\langle x_1, x_2 \rangle \) of noncommutative polynomials consists of \( A \)-linear combination of noncommutative monomials w. natural addition & multiplication (elements of \( A \) commute.)
Exercise: Give a description of homomorphisms $A(x_1, \ldots, x_n) \rightarrow B$ 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 $\sum_{g \in G} a_g g$, $a_g \in A$, with natural addition, and with multiplication extending that in $G$ by distributivity. This construction is very important in the study of representations of $G$ (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 left ideal in $A$ is a subset $I \subseteq A$ s.t.

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

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

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 $\phi: A \rightarrow B$ be a ring homomorphism. Then $\ker \phi$ is a two-sided ideal.

For a two-sided ideal $I \subseteq A$ 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

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

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

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