Lecture 2.1

Last time:

- An **integral domain** is a commutative ring with no nontrivial zero divisors:

$$xy = 0 \implies x = 0 \text{ or } y = 0.$$

- A **field** is a commutative ring $\mathbb{F}$ with $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$.

More examples of rings:

(1) $\mathbb{R}$ and $\mathbb{C}$ are fields:

- in technical terms, $\mathbb{R}$ is defined as

the completion of $\mathbb{Q}$ under the absolute value $|\cdot|$, so elements $x \in \mathbb{R}$ are the limit of some Cauchy sequence in $\mathbb{Q}$.

- in $\mathbb{C}$, $z^{-1} = \frac{1}{z} = \frac{1}{x+iy}$

$$= \frac{x-iy}{x^2+y^2} = \frac{\bar{z}}{|z|^2}$$

for all $z \neq 0$, and $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ follows from checking $zz^{-1} = 1$.

(2) Let A be a commutative ring and define

$$M_n(A) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} : a_{ij} \in A \right\}.$$

Then $M_n(A)$ is a ring under

$$+ : M_n(A) \times M_n(A) \longrightarrow M_n(A)$$
$$((a_{ij}), (b_{ij})) \longmapsto (a_{ij} + b_{ij})$$

$$\cdot : M_n(A) \times M_n(A) \longrightarrow M_n(A)$$
$$((a_{ij}), (b_{ij})) \longmapsto (a_{ij})(b_{ij}).$$

For $n \geq 2$, $M_n(A)^\times \neq M_n(A) \setminus \{0\}$,

so $M_n(A)$ is not a field in general.

But more of an obstacle is the fact

that for $n \geq 2$, $M_n(A)$ is not commutative:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}.$$

(3) For a ring A, the set of polynomials

$$A[x] = \left\{ a_0 + a_1 x + \dots + a_n x^n \;\middle|\; \begin{array}{l} a_i \in A, \\ n \geq 0 \\ (n \in \mathbb{Z}) \end{array} \right\}$$

is a ring under polynomial addition

and multiplication (extended FOIL):

$$+ : A[x] \times A[x] \longrightarrow A[x]$$

$$\left(\sum_{i=0}^{n} a_i x^i, \sum_{j=0}^{m} b_j x^j\right) \mapsto \sum_{k=0}^{\max(n,m)} (a_k + b_k) x^k$$

$$\cdot : A[x] \times A[x] \longrightarrow A[x]$$

$$\left(\sum_{i=0}^{n} a_i x^i, \sum_{j=0}^{m} b_j x^j\right) \mapsto \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j}.$$

If A is commutative, so is $A[x]$.

We can also iterate this construction to build rings of multivariable polynomials:

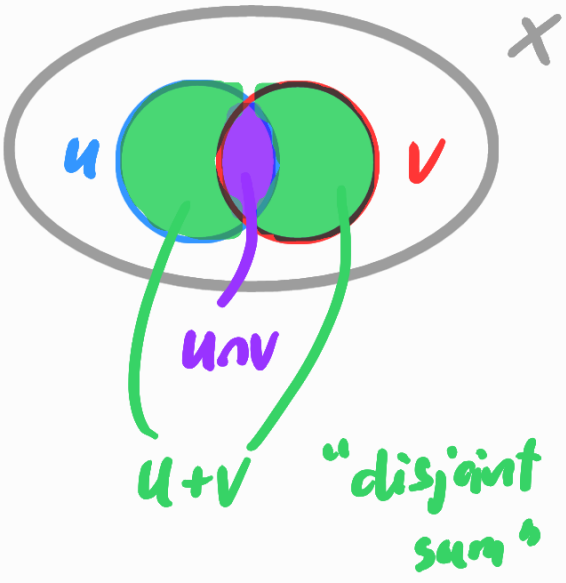
$$A[x_1, \dots, x_r] = A[x_1][x_2] \cdots [x_r].$$

(4) Let X be a set and

$$\mathbb{P}(X) = \{\text{subsets } U \subseteq X\}.$$

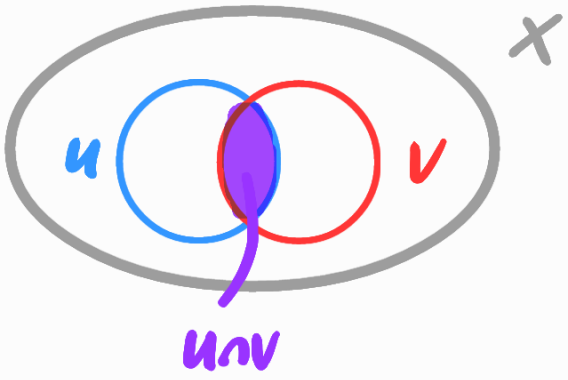
Then $\mathbb{P}(X)$ is a commutative ring under

$$+ : \mathbb{P}(X) \times \mathbb{P}(X) \longrightarrow \mathbb{P}(X)$$
$$(U, V) \longmapsto U \cup V \setminus U \cap V$$



$$\cdot : \mathbb{P}(X) \times \mathbb{P}(X) \longrightarrow \mathbb{P}(X)$$

$$(U, V) \longmapsto U \cap V$$



Here, the 0 element is the empty set $\emptyset$:

$$U + \emptyset = U \cup \emptyset \setminus U \cap \emptyset$$

$$= U \setminus \emptyset = U$$

The multiplicative identity is X itself :

$$X \cdot U = X \cap U = U.$$

Subrings, Homomorphisms and Ideals

We've learned a few examples of rings.

Let's next investigate how to compare rings.

Def A **subring** of a ring A is a subset $B \subseteq A$ that is a ring under the same operations as A. That is,

(1) $(B, +)$ is a subgroup of the

abelian group $(A, +)$.

(2) For all $x, y \in B$, $xy \in B$.

(3) $1 \in B$ or $B = \{0\}$.

Ex (5) I mentioned last time that $2\mathbb{Z} \subseteq \mathbb{Z}$ is not a ring, so it can't be a subring. In fact, because $\mathbb{Z} = 1\mathbb{Z}$, any subring of $\mathbb{Z}$ is either 0 or $\mathbb{Z}$ itself.

(6) For the same reason,

$$\mathbb{Z}/n\mathbb{Z} = 1\mathbb{Z}/n\mathbb{Z}$$

implies that the only subrings of $\mathbb{Z}/n\mathbb{Z}$ are 0 and $\mathbb{Z}/n\mathbb{Z}$.

(7) The only nontrivial subring of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is

$$\langle (1,1) \rangle = \{(0,0), (1,1)\}.$$

As an abelian group, $\langle (1,1) \rangle \cong \mathbb{Z}/2\mathbb{Z}$ so we can view this as a copy

of $\mathbb{Z}/2\mathbb{Z}$ inside $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$1 \longmapsto (1,1)$

Question: what do we want in a ring homomorphism $\varphi: A \to B$?

Def A function $\varphi: A \to B$ between two rings is a **ring homomorphism** if:

(1) φ is a homomorphism of abelian groups $\varphi: (A,+) \longrightarrow (B,+)$, i.e.

$$\varphi(x+y) = \varphi(x) + \varphi(y) \quad \text{for all } x, y \in A.$$

(2) $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in A$.

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

Exercise 1: prove that $\varphi(A^\times) \subseteq B^\times$.

Ex (8) The quotient map

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$x \longmapsto \bar{x}$$

is a ring homomorphism for all $n \geq 1$.

(9) Similarly, for $d \mid n$ the map

$$\varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}$$
$$\bar{x} \longmapsto \bar{x}$$

is a ring homomorphism.

(10) Let $A[x]$ be the polynomial ring over some ring A and pick any element $a \in A$. Then the map

$$\begin{aligned} ev_a : A[x] &\longrightarrow A \\ f(x) &\longmapsto f(a) \end{aligned}$$

is a ring homomorphism:

Pick $f(x) = \sum_{i=0}^{n} c_i x^i$, $g(x) = \sum_{i=0}^{n} d_i x^i$.

(1) $ev_a(f(x) + g(x)) = (f+g)(a)$

$$= f(a) + g(a)$$

$$= ev_a(f(x)) + ev_a(g(x)).$$

(2) $$ev_a(f(x)g(x)) = ev_a\left(\sum_{i=0}^{n}\sum_{j=0}^{n} c_i d_j x^{i+j}\right)$$

$$= \sum_{i=0}^{n}\sum_{j=0}^{n} c_i d_j a^{i+j}$$

$$= \left(\sum_{i=0}^{n} c_i a^i\right)\left(\sum_{j=0}^{n} d_j a^j\right)$$

$$= f(a)\, g(a)$$

$$= ev_a(f(x))\, ev_a(g(x)).$$

(3) $$1(a) = 1.$$

So ev_a is a ring homomorphism.

Lemma For any ring A, there exists a unique ring homomorphism $\varphi: \mathbb{Z} \to A$.

Pf: We must have $\varphi(1) = 1$, and this determines $\varphi(n)$ for any $n \in \mathbb{Z}$:

$$\varphi(n) := \underbrace{\varphi(1) + \dots + \varphi(1)}_{n \text{ times}}.$$

If follows that $\varphi(n+m) = \varphi(n) + \varphi(m)$ and $\varphi(nm) = \varphi(n)\varphi(m)$ for any $n, m \in \mathbb{Z}$. $\square$

Remark: This says that $\mathbb{Z}$ is the **initial** ring: it "comes first" and has arrows pointing at every other ring.

Since $\varphi: \mathbb{Z} \to A$ is an abelian group homomorphism, it has a kernel

$$\ker(\varphi) \leq \mathbb{Z}.$$

In particular, $\ker(\varphi) = n\mathbb{Z}$ for some $n \geq 0$. This number n is called the **characteristic** of A, written $\operatorname{char} A$.

Ex (11) For $A = \mathbb{Z}$ itself, φ is the identity $n \longmapsto n$ and this has kernel $0\mathbb{Z}$, so $\operatorname{char} \mathbb{Z} = 0$.

(12) For any $n \geq 1$ and $A = \mathbb{Z}/n\mathbb{Z}$, φ is the quotient map

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

which has kernel $n\mathbb{Z}$. So $\mathbb{Z}/n\mathbb{Z}$ has characteristic n.

We will see shortly that any field has

either characteristic 0 or p for a prime p.

If $\mathbb{F}$ has characteristic p, we call $\mathbb{F}_p$ its

prime subfield.

Next time: ideals.