Lecture 1.2

Last time:

- A **ring** is a set A with two operations $+$ and $\cdot$ satisfying

(1) $(A, +)$ is an abelian group.

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

(3) $1x = x = x1$ for all $x \in A$.

(4) $x(y+z) = xy + xz$ and $(x+y)z = xz + yz$

for all $x, y, z \in A$.

- The group of units of A is

$$A^\times = \{x \in A \mid xy = 1 = yx \text{ for some } y \in A\}.$$

- The integers form a ring $\mathbb{Z}$.

Def A commutative ring A is:

- an integral domain if $1 \neq 0$ and for any $x, y \in A$ such that $xy = 0$, $x = 0$ or $y = 0$. If there do exist $x, y \neq 0$ with $xy = 0$, x and y are called zero divisors.

- a **field** if $1 \neq 0$ and $A^\times = A \setminus \{0\}$,

  i.e. every nonzero element of A has a

  multiplicative inverse.

Prop Every field is an integral domain.

Proof: Suppose $xy = 0$ but $x \neq 0$. Then

since $A^\times = A \setminus \{0\}$, x has an inverse,

say $x^{-1} \in A^\times$.

Multiplying $xy = 0$ through by x^{-1} gives

definition of $A^\times$: $x^{-1}xy = x^{-1}0$

Exercise 1 below: $1y = 0$

axiom (3): $y = 0$

So A is an integral domain. $\square$

Exercise 1: Use the axioms of a ring to show that in any ring A, $x0 = 0 = 0x$ for all $x \in A$.

Ex ① The integers are a commutative ring: (1) – (5) follow from the axioms of integer arithmetic. Further,

$\mathbb{Z}$ is an integral domain:

if $xy = 0$ for $x, y \in \mathbb{Z}$ then

$x = 0$ or $y = 0$.

Is $\mathbb{Z}$ a field? NO!

$\mathbb{Z}^\times = \{\pm 1\} \neq \mathbb{Z} \setminus \{0\}$.

② One of the most familiar groups is probably $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$. This is a ring under $(x + n\mathbb{Z}) \cdot (y + n\mathbb{Z}) = xy + n\mathbb{Z}$.

Notation: $\bar{x} = x + n\mathbb{Z}$. Eventually, we will

just write x for $x+n\mathbb{Z}$.

First, we need to show this binary operation is well-defined:

if $\bar{x} = \bar{x}'$ then $x = x' + ns$

$\bar{y} = \bar{y}'$ then $y = y' + nt$

want: $\bar{x}\bar{y} = \bar{x}'\bar{y}'$ in $\mathbb{Z}/n\mathbb{Z}$.

Then $xy = (x'+ns)(y'+nt)$

$= x'y' + x'nt + nsy' + n^2st$

$= x'y' + n(x't + y's + nst)$

$\in x'y' + n\mathbb{Z}$.

So $\bar{x}\bar{y} = xy + n\mathbb{Z} = x'y' + n\mathbb{Z} = \bar{x}'\bar{y}'$.

Now let's check the ring axioms.

(1) We already know $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under $+$.

(2) For any $x, y, z \in \mathbb{Z}$,

$$\begin{aligned}((x+n\mathbb{Z})(y+n\mathbb{Z}))(z+n\mathbb{Z}) &= (xy+n\mathbb{Z})(z+n\mathbb{Z}) \\ &= (xy)z + n\mathbb{Z} \\ &= x(yz) + n\mathbb{Z} \\ &= (x+n\mathbb{Z})(yz+n\mathbb{Z}) \\ &= (x+n\mathbb{Z})((y+n\mathbb{Z})(z+n\mathbb{Z})).\end{aligned}$$

(3) A multiplicative identity is $1+n\mathbb{Z}$:

$$(x+n\mathbb{Z})(1+n\mathbb{Z}) = x\cdot 1 + n\mathbb{Z}$$

$$= x + n\mathbb{Z}.$$

(4) $$(x+n\mathbb{Z})\big((y+n\mathbb{Z}) + (z+n\mathbb{Z})\big) =$$

$$(x+n\mathbb{Z})\big((y+z)+n\mathbb{Z}\big) =$$

$$x(y+z)+n\mathbb{Z} = (xy+xz)+n\mathbb{Z}$$

$$= (xy+n\mathbb{Z}) + (xz+n\mathbb{Z}).$$

$$= (x+n\mathbb{Z})(y+n\mathbb{Z}) +$$
$$(x+n\mathbb{Z})(z+n\mathbb{Z}).$$

Is $\mathbb{Z}/n\mathbb{Z}$ a commutative ring? Yes!

$$(x+n\mathbb{Z})(y+n\mathbb{Z}) = xy + n\mathbb{Z}$$

$= yx + n\mathbb{Z}$

$= (y + n\mathbb{Z})(x + n\mathbb{Z})$.

Is $\mathbb{Z}/n\mathbb{Z}$ an integral domain?

what if $\bar{x}\bar{y} = \bar{0}$?

$\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\bar{2} \cdot \bar{3} = \bar{0}$ but 

$\bar{2} \neq \bar{0}$, $\bar{3} \neq \bar{0}$.

$\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\bar{2} \cdot \bar{2} = \bar{0}$ 

$\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$1 \cdot 1 = 1$

$1 \cdot 2 = 2$

$1 \cdot 3 = 3$

$1 \cdot 4 = 4$

$2 \cdot 1 = 2$

$2 \cdot 2 = 4$

$2 \cdot 3 = 1$

$2 \cdot 4 = 3$

$3 \cdot 1 = 3$

$3 \cdot 2 = 1$

$3 \cdot 3 = 4$

$3 \cdot 4 = 2$

$4 \cdot 1 = 4$

$4 \cdot 2 = 3$

$4 \cdot 3 = 2$

$4 \cdot 4 = 1$

Do you see a pattern? If not, try some more examples til you spot one.

Theorem $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is a prime number.

and only if n is a prime number.

Pf: First, if $n=1$ then

$$\mathbb{Z}/n\mathbb{Z} = \{0\}$$ ← the trivial ring

so $1=0$. ✗

Next, suppose $n = ab$, where $a, b \geq 2$.

Then $a, b < n$ so $a+n\mathbb{Z} \neq n\mathbb{Z}$ and

$b+n\mathbb{Z} \neq n\mathbb{Z}$, but

$$(a+n\mathbb{Z})(b+n\mathbb{Z}) = \bar{a}\cdot\bar{b} = \bar{n} = \bar{0} = n\mathbb{Z}.$$

Therefore $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain.

Finally, suppose $n=p$ is prime and

$$(x + p\mathbb{Z})(y + p\mathbb{Z}) = p\mathbb{Z}.$$

This means $xy + p\mathbb{Z} = p\mathbb{Z}$, i.e. $xy \in p\mathbb{Z}$.

That is, $p \mid xy$ so because p is prime, $p \mid x$ or $p \mid y$.

In other words, $x \in p\mathbb{Z}$ or $y \in p\mathbb{Z}$ which says $x + p\mathbb{Z} = p\mathbb{Z}$ or $y + p\mathbb{Z} = p\mathbb{Z}$. □

Recall that a field is an integral domain $\mathbb{F}$ where $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$.

Do we think $\mathbb{Z}/p\mathbb{Z}$ (p prime) is also a field?

Theorem For any prime number p, $\mathbb{Z}/p\mathbb{Z}$ is a field, written $\mathbb{F}_p$.

"the field with p elements"

Pf: Switching back to bar notation, take $\bar{x} = x + p\mathbb{Z}$ such that $\bar{x} \neq \bar{0}$.

Then $p \nmid x$ so since p is prime,

$$\gcd(p, x) = 1.$$

By definition, ← did you cover this in Algebra I?

$$\mathbb{Z} = \gcd(p,x)\mathbb{Z} = p\mathbb{Z} + x\mathbb{Z}$$

so we can write $1 \in \mathbb{Z}$ as

$$1 = ap + bx \quad \text{for } a, b \in \mathbb{Z}.$$

Now what should $\bar{x}^{-1}$ be?

$$\bar{x}^{-1} = \bar{b} = b + p\mathbb{Z}$$

Let's finish the proof:

Then $$\bar{x}\bar{b} = (x + p\mathbb{Z})(b + p\mathbb{Z})$$

$$= bx + p\mathbb{Z}$$

Since $1 - bx = ap \in p\mathbb{Z}$,

$$1 + p\mathbb{Z} = bx + p\mathbb{Z}$$

So $\bar{x}\bar{b} = bx + p\mathbb{Z} = 1 + p\mathbb{Z} = \bar{1}$. □

Corollary (Fermat's Little Theorem) Let p be a prime number. Then for any $x \in \mathbb{Z}$ such that $x \notin p\mathbb{Z}$,

$$x^{p-1} \equiv 1 \pmod{p}.$$

Pf: This is equivalent to proving

$$\bar{x}^{p-1} = \bar{1} \quad \text{in } \mathbb{F}_p.$$

Since $\mathbb{F}_p$ is a field, $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{\bar{0}\}$ is a group with $p-1$ elements.

By Lagrange's Theorem, the order of any $\bar{x} \in \mathbb{F}_p^\times$ divides $p-1$, so $\bar{x}^{p-1} = \bar{1}$ in $\mathbb{F}_p^\times$. □

Ex ③ If A, B are rings, then $A \times B$ is also a ring under

$$+ : (A \times B)^2 \longrightarrow A \times B$$
$$((a,b),(a',b')) \longmapsto (a+a', b+b')$$

$$\cdot : (A \times B)^2 \longrightarrow A \times B$$
$$((a,b),(a',b')) \longmapsto (aa', bb').$$

For example, $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is a

ring for all $n, m \geq 1$.

Claim: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not an integral domain.

Exercise 2: Prove it! Are any of the rings $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ integral domains?

equivalence classes: $\frac{a}{b} \sim \frac{c}{d}$ if and only if $ad = bc$

(4) $\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0 \right\}$ is a field:

$$+ : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$$

$$\left(\frac{a}{b}, \frac{c}{d}\right) \longmapsto \frac{ad + bc}{bd}$$

$$\bullet : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$$

$$\left(\frac{a}{b}, \frac{c}{d}\right) \longmapsto \frac{ac}{bd}$$

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \quad \text{if} \quad a, b \in \mathbb{Z} \setminus \{0\}.$$

In fact, $\mathbb{Q}$ is the smallest field containing $\mathbb{Z}$ (it's the "field of fractions" of $\mathbb{Z}$).

Exercise 3: Carefully check that $\mathbb{Q}$ is a field, i.e. a commutative ring with $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

(5) $\mathbb{R}$ 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 $zz^{-1} = 1$.

⑥ 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:

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

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

(7) 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:

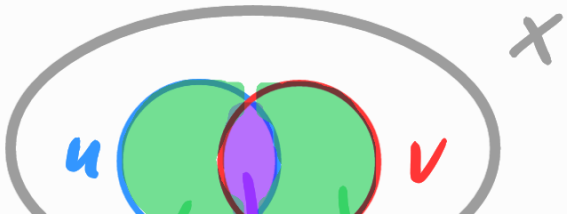
$$A[x_1, \dots, x_r] = A[x_1][x_2] \cdots [x_r].$$

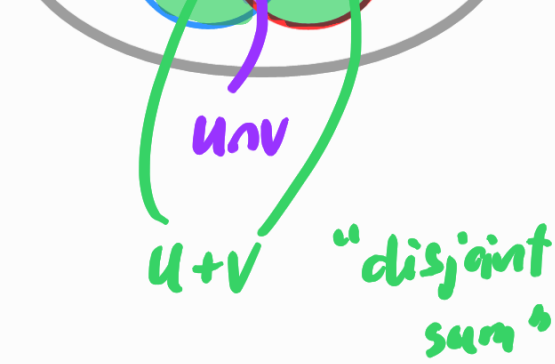
(8) Let X be a set and

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

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

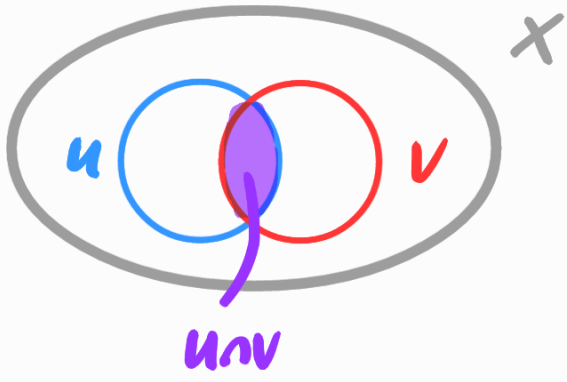
$$+ : \mathbb{P}(X) \times \mathbb{P}(X) \longrightarrow \mathbb{P}(X)$$
$$(U, V) \longmapsto U \cup V \setminus U \cap V$$





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

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



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:

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

Next time: subrings, homomorphisms, ideals.