Last time: factor rings

\( R \) ring
\( A \subseteq R \) an ideal

\( R/A \) is a ring via the multiplication

\[(a + A)(b + A) = ab + A.\]

**Def.** \( R \) commutative ring. A *prime ideal* \( A \) of \( R \) is a proper ideal of \( R \) satisfying \( ab \in A \Rightarrow a \in A \) or \( b \in A \).

A *maximal ideal* \( A \) of \( R \) is a proper ideal for which \( B \supseteq A \) and \( B \) an ideal \( \Rightarrow B = A \) or \( B = R \).

**Ex.** \( n \mathbb{Z} \subseteq \mathbb{Z} \). \( n \mathbb{Z} \) is a prime \( (=) n \) is prime. \( (n \geq 1 \) pos int \)

\( \mathbb{p} \) prime: \( ab \in \mathbb{p} \mathbb{Z} \Rightarrow p|ab \Rightarrow p|a \) or \( p|b \)

\( \frac{\text{multiples}}{\mathbb{p}} \Rightarrow \mathbb{a} \in \mathbb{p} \mathbb{Z} \) or \( \mathbb{b} \in \mathbb{p} \mathbb{Z} \)

**Ex.** \( R \) integral domain. Then \( \mathfrak{p} \mathfrak{o} \mathfrak{s} \) is prime.

**PF:** \( ab \in \mathfrak{p} \mathfrak{o} \mathfrak{s} \) means \( ab = 0 \Rightarrow a = 0 \) or \( b = 0 \) \( \frac{\text{b/c } R \text{ an integral domain}}{\Rightarrow \mathbb{a} \in \mathfrak{p} \mathfrak{o} \mathfrak{s} \text{ or } \mathbb{b} \in \mathfrak{p} \mathfrak{o} \mathfrak{s}} \)
Note: The prime ideals of \( \mathbb{Z} \) are precisely the ideals \( \mathbb{Z} \) and \( \langle p \rangle \), prime number.

Ex 3  \( R = \mathbb{Z}[x] \). Then \( \langle x \rangle \) is prime.

Let \( f = a_0 + a_1 x + \ldots + a_m x^m \) and suppose \( f \cdot g \in \langle x \rangle \).
\[ g = b_0 + b_1 x + \ldots + b_n x^n \]
\[ fg = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \ldots + a_m b_n x^{m+n} \]
\[ fg \in \langle x \rangle \] means \( a_0 b_0 = 0 \) \( \Rightarrow \) \( a_0 = 0 \) or \( b_0 = 0 \)
\[ \Rightarrow f \in \langle x \rangle \text{ or } g \in \langle x \rangle \]

\( \langle x \rangle \) is not maximal because \( \langle x \rangle \nsubseteq \langle x, 2 \rangle \)

\( \langle 2, x \rangle \) is maximal

[Aside: can imagine \( \langle 2, x, x^2 + 1 \rangle \nsubseteq \langle 2, x \rangle \) is proper.]

But in fact, \( \langle 2, x, x^2 + 1 \rangle = \mathbb{Z}[x] \)

Suppose \( A \nsubseteq \langle 2, x \rangle \) is an ideal. Suppose \( f \in A \) and \( f \notin \langle 2, x \rangle \).

Then \( f \) has odd constant term, because we proved before that
\( \langle 2, x \rangle \) precisely consists of the polynomials with even constant term.

\[ f = 2m + 1 + x \cdot h(x) \text{ for } m \in \mathbb{Z}, h(x) \in \mathbb{Z}[x] \]
\[ 1 = \frac{f - 2m}{\in A} - \frac{h}{\in A} \implies 1 \in A. \]

\[ \Rightarrow A = \mathbb{Z}[x]. \]

**True:** \( A \triangleleft R \) is an ideal and \( A \) contains a unit of \( R \) then \( A = R \). (HW question)

**Ex:** \( (x^2 + 1) \subseteq (R[x]) \) is maximal.

**Pf:** Suppose \( A \supsetneq (x^2 + 1) \) is an ideal strictly containing \( (x^2 + 1) \).

Then \( \exists f \in A, f \notin (x^2 + 1) \).

Have
\[
f(x) = q(x)(x^2 + 1) + r(x), \quad \text{where} \quad q(x) \in (R[x]) \quad \text{and} \quad r(x) \neq 0.
\]

\[ f(x) = (a + bx)(a - bx) = a^2 - b^2 x^2 = a^2 - b^2 (x^2 + 1) - 1 \]

\[ = a^2 + b^2 + b^2 (x^2 + 1) \implies a^2 + b^2 = (a + bx)(a - bx) - b^2 (x^2 + 1) \in A. \]

\[ \implies A \text{ contains a unit} \implies A = (R[x]). \]

**Thm** \( R \), commutative ring w/ unity and \( A \triangleleft R \) is an
Thm. \( R \) commutative ring w/ unity and \( A \subseteq R \) is an ideal. Then \( R/A \) is an integral domain (\( \Rightarrow \) \( A \) is prime).

**Pf.** Suppose \( A \) is prime.

- Suppose \((a+A)(b+A)=0\) in \( R/A \).

Then \( ab+A=0+A \)

\[ \Rightarrow ab \in A \Rightarrow a \in A \ \text{or} \ b \in A \]

\[ \Rightarrow a+A=0 \ \text{in} \ R/A \quad \text{or} \quad b+A=0 \ \text{in} \ R/A \quad \Rightarrow R/A \ \text{is an integral domain.} \]

Conversely, suppose \( R/A \) is an integral domain, and \( ab \in A \).

Then

\[ 0 = ab+A = (a+A)(b+A) \]

\[ \Rightarrow a+A=0 \ \text{in} \ R/A \Rightarrow a \in A \]

\[ \text{or} \ b+A=0 \ \text{in} \ R/A \Rightarrow b \in A \quad \Rightarrow A \ \text{is a prime ideal.} \]

Thm. \( R \) commutative ring w/ unity and \( A \subseteq R \) an ideal.

Then \( R/A \) is a field (\( \Rightarrow \) \( A \) is a maximal ideal)

**Pf.** Suppose \( A \) max'0 ideal. If \( b \notin A \), need to prove that

\( b+A \) has a multiplicative inverse in \( R/A \).

But \( \langle b \rangle + A = \{ \sum br + a : r \in R, a \in A \} \) is an ideal
But $\langle b \rangle + A = \left\{ br + a : r \in R, a \in A \right\}$ is an ideal strictly containing $A$.

$\implies \langle b \rangle + A = R \implies 1 \in \langle b \rangle + A$.

$\implies 1 = br + a \quad \text{for some } r \in R, a \in A$

$\implies (b + A)(r + A) = br + A = 1 - a + A = 1 + A$

$\implies r + A \text{ is the desired mult. inverse.}$