Last time: We completed the proof of...

Theorem. Let F be a field and fix $g(x) \in F[x]$.

1. If $g(x)$ is factorable, then $F[x]/\langle g(x)\rangle$ is *not* a field. ($\mathbb{Z}_7[x]/\langle x^2-1\rangle$)
2. If $g(x)$ is unfactorable, then $F[x]/\langle g(x)\rangle$ is a field. ($\mathbb{R}[x]/\langle x^2+1\rangle$)

Key ingredient: GCD theorem for polynomials, a tool from *number theory*.

Goal: Prove the theorem again, using a tool from *abstract algebra*.

Discuss in your group:

(a) **(Review)** What does it mean that $12\mathbb{Z}$ is an ideal of the ring $\mathbb{Z}$?

$12\mathbb{Z}$ is an additive subgroup of $\mathbb{Z}$ and satisfies product absorption.

(b) Find all ideals A such that $12\mathbb{Z} \subseteq A \subseteq \mathbb{Z}$. (But $A \neq 12\mathbb{Z}, \mathbb{Z}$.)

$A = 6\mathbb{Z},\ 4\mathbb{Z},\ 3\mathbb{Z},\ 2\mathbb{Z}$. ($A$ is *strictly* between $12\mathbb{Z}$ and $\mathbb{Z}$.)

(c) Find all ideals A such that $5\mathbb{Z} \subseteq A \subseteq \mathbb{Z}$. (But $A \neq 5\mathbb{Z}, \mathbb{Z}$.)

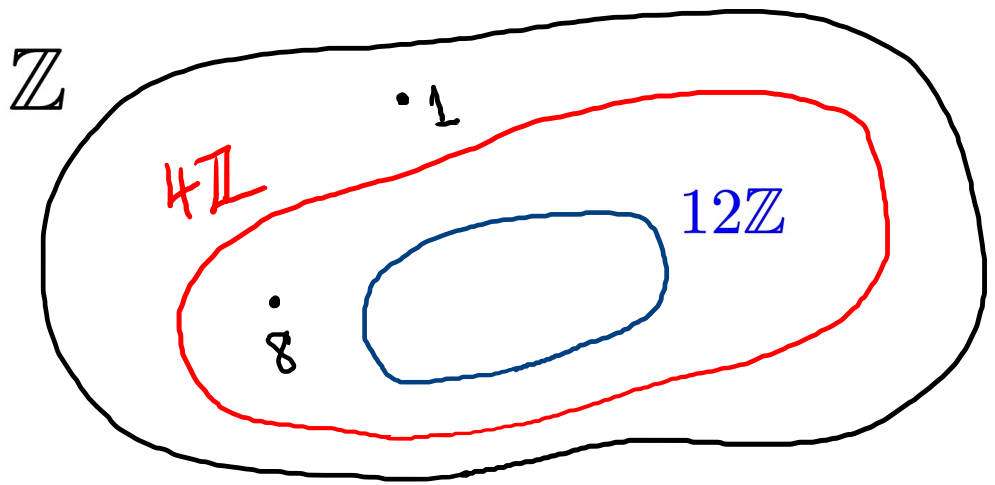
No such ideal A. (We *must* have $A = 5\mathbb{Z}$ or $A = \mathbb{Z}$.)

Example: $5\mathbb{Z}$ is a *maximal* ideal of $\mathbb{Z}$, i.e., there's no ideal "bigger" than $5\mathbb{Z}$.

Definition. Let M be an ideal of a commutative ring R, with $M \neq R$. Then M is *maximal* in R if for any ideal A with $M \subseteq A \subseteq R$, we have $A = M$ or $A = R$.

Remark: Thus, there is no ideal A that is *strictly* between M and R.

Non-Example: The ideal $12\mathbb{Z}$ is *not* maximal in $\mathbb{Z}$, because there is an ideal $4\mathbb{Z}$ such that $12\mathbb{Z} \subsetneq 4\mathbb{Z} \subsetneq \mathbb{Z}$.



Note: $12\mathbb{Z} \subsetneq 4\mathbb{Z}$ means $12\mathbb{Z} \subseteq 4\mathbb{Z}$, but $12\mathbb{Z} \neq 4\mathbb{Z}$. (Similarly for $4\mathbb{Z} \subsetneq \mathbb{Z}$.)

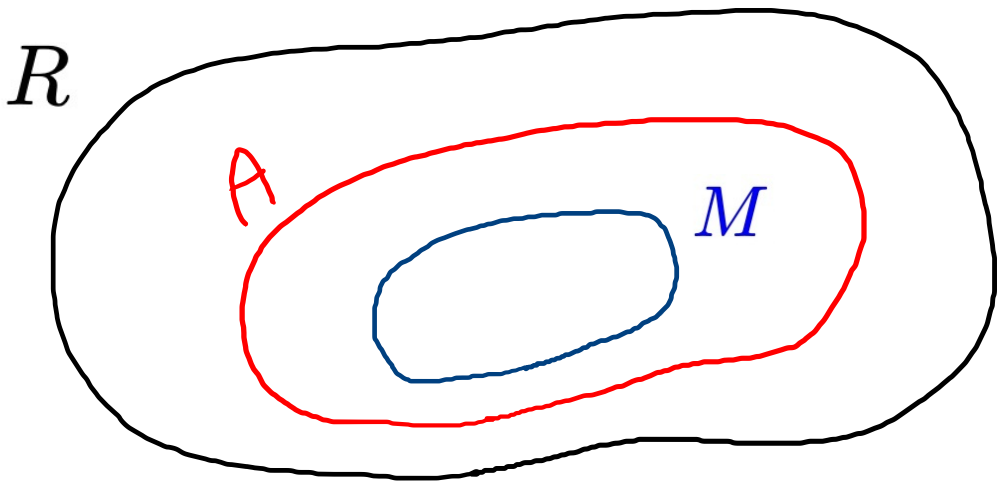
Example: Let $g(x) = x^2 - 1 \in \mathbb{R}[x]$. Then $\langle g(x) \rangle$ is *not* maximal in $\mathbb{R}[x]$, as

$$\langle g(x) \rangle \subsetneq \langle x + 1 \rangle \subsetneq \mathbb{R}[x],$$

$$x^2 - 1 = (x + 1)(x - 1).$$

i.e., $\langle x + 1 \rangle$ is *strictly* between $\langle g(x) \rangle$ and $\mathbb{R}[x]$.

Proof know-how: To show that M is *not* maximal in R, find an ideal A such that $M \subsetneq A \subsetneq R$ (i.e., A is *strictly* between M and R).



Example: Let $g(x) = x^2 + 1 \in \mathbb{R}[x]$. Then $\langle g(x) \rangle$ is maximal in $\mathbb{R}[x]$.

Proof know-how: To show that $\langle g(x) \rangle$ is maximal in $\mathbb{R}[x]$...

- Consider an ideal $\langle p(x) \rangle$ such that $\langle g(x) \rangle \subseteq \langle p(x) \rangle \subseteq \mathbb{R}[x]$.
- Then show that $\langle p(x) \rangle$ must be equal to either $\langle g(x) \rangle$ or $\mathbb{R}[x]$.
- **Conclusion:** Hence $\langle g(x) \rangle$ is maximal in $\mathbb{R}[x]$.
  (There is no ideal strictly between $\langle g(x) \rangle$ and $\mathbb{R}[x]$.)

Theorem. Let F be a field and fix $g(x) \in F[x]$.

1. If $g(x)$ is factorable, then $\langle g(x) \rangle$ is *not* maximal in $F[x]$.

2. If $g(x)$ is unfactorable, then $\langle g(x) \rangle$ is maximal in $F[x]$.

(See Chapter 36 reading for the proof.)

Theorem. Let F be a field and fix $g(x) \in F[x]$.
If $g(x)$ is unfactorable, then $\langle g(x) \rangle$ is maximal in $F[x]$.

- Consider an ideal $\langle p(x) \rangle$ such that $\langle g(x) \rangle \subseteq \langle p(x) \rangle \subseteq F[x]$.
- We will show that $\langle p(x) \rangle = \langle g(x) \rangle$ or $\langle p(x) \rangle = F[x]$.
- Since $g(x) \in \langle g(x) \rangle \subseteq \langle p(x) \rangle$, we have $g(x) = p(x) \cdot q(x)$.
- But $g(x)$ is unfactorable, so either $p(x)$ or $q(x)$ is a nonzero constant.
  - If $p(x)$ is constant, then $\langle p(x) \rangle = F[x]$.
  - If $q(x)$ is constant, then $\langle p(x) \rangle = \langle g(x) \rangle$.

  } See Chapter 36.

- Thus, $\langle g(x) \rangle$ is maximal in $F[x]$, as desired.