Recap: We've explored these polynomial quotient rings.

- $\mathbb{Z}_3[x]/\langle x^2 \rangle$ is *not* a field.
- $\mathbb{Z}_7[x]/\langle x^2 - 1 \rangle$ is *not* a field.
- $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ is a field, because it's isomorphic to $\mathbb{C}$.

Question: Given $g(x) \in F[x]$, when is $F[x]/\langle g(x) \rangle$ a field? (And why?)

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.

   Example: $g(x) = x^2 - 1 \in \mathbb{Z}_7[x]$, where $g(x) = (x+1)\cdot(x-1)$. Then...

   $$((x+1) + \langle g(x)\rangle)\cdot((x-1) + \langle g(x)\rangle) = g(x) + \langle g(x)\rangle = 0 + \langle g(x)\rangle.$$

   Thus, $\mathbb{Z}_7[x]/\langle g(x)\rangle$ has zero divisors, so it is *not* a field.

2. If $g(x)$ is unfactorable, then $F[x]/\langle g(x)\rangle$ is a field.

   Example: $g(x) = x^2 + 1 \in \mathbb{R}[x]$ is unfactorable. Thus, $\mathbb{R}[x]/\langle g(x)\rangle$ is a field.

Today's goal. To prove this theorem:

- Fix $g(x) \in F[x]$. If $g(x)$ is unfactorable, then $F[x]/\langle g(x) \rangle$ is a field.

Key: We'll use the *structural similarities* between $\mathbb{Z}$ and $F[x]$.

The analogous statement in $\mathbb{Z}$ is:

- Fix $p \in \mathbb{Z}$. If p is prime, then $\mathbb{Z}/\langle p \rangle$ is a field.

Note: Here, $\langle p \rangle = p\mathbb{Z}$, i.e., the set of all multiples of p.

When two cosets are equal

In $\mathbb{Z}/\langle p \rangle$:

$$378 + \langle 5 \rangle = 3 + \langle 5 \rangle \iff 378 - 3 = 375 \in \langle 5 \rangle.$$

$$\alpha + \langle p \rangle = \beta + \langle p \rangle \iff \alpha - \beta \in \langle p \rangle.$$

In $F[x]/\langle g(x) \rangle$:

$$\alpha(x) + \langle g(x) \rangle = \beta(x) + \langle g(x) \rangle \iff \alpha(x) - \beta(x) \in \langle g(x) \rangle.$$

Key proof ingredient: The GCD theorem

Integers: If a and b are relatively prime, then there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Polynomials: If $f(x)$ and $g(x)$ are relatively prime, then there exist $p(x), q(x) \in F[x]$ such that $f(x) \cdot p(x) + g(x) \cdot q(x) = 1$.

(See Chapter 35 reading for their proofs using *ideals*.)

Theorem. Fix $g(x) \in F[x]$. If $g(x)$ is unfactorable, then $F[x]/\langle g(x)\rangle$ is a field.

Proof: Assume $g(x)$ is unfactorable.

Let $\alpha(x) \in F[x]$ such that $\alpha(x) + \langle g(x)\rangle \neq 0 + \langle g(x)\rangle$. Thus, $\alpha(x) \notin \langle g(x)\rangle$.

We will show that $\alpha(x) + \langle g(x)\rangle$ has a multiplicative inverse.

Since $\alpha(x) \notin \langle g(x)\rangle$ and $g(x)$ is unfactorable, they are relatively prime.

Then, there exist $p(x)$, $q(x) \in F[x]$ such that $\alpha(x) \cdot p(x) + g(x) \cdot q(x) = 1$.

Hence, $(\alpha(x) + \langle g(x)\rangle) \cdot (p(x) + \langle g(x)\rangle) = \alpha(x) \cdot p(x) + \langle g(x)\rangle = 1 + \langle g(x)\rangle$,

because $\alpha(x) \cdot p(x) - 1 = -g(x) \cdot q(x) \in \langle g(x)\rangle$.

Thus, $\alpha(x) + \langle g(x)\rangle$ has a multiplicative inverse, namely $p(x) + \langle g(x)\rangle$.

Therefore, $F[x]/\langle g(x)\rangle$ is a field.