Last time: Division algorithm

Example  $x^2 - x$ in $\mathbb{Z}/6\mathbb{Z}[x]$

has roots: 0, 1, 3, 4 modulo 6

E.g. $4^2 - 4 = 12 \equiv 0 \mod 6$

Thm A nonzero polynomial of degree $n$ over a field has at most $n$ roots.

Pf: Induction on $n$

Base case: If $f$ has degree 0, then $f$ is a nonzero constant, so $f$ has no roots. ✓

Inductive step: Now assume $f$ has degree $n \geq 1$. If $f$ has no zeros, then we're done.

If $a$ is a zero of $f$, then

* $f(x) = g(x)(x-a)$

where $g(x)$ has degree $n-1$.

Suppose $b$ is another root of $f$. (If $f$ has no other roots, then we're done.)
0 = f(b) = q(b)(b-a)

But b-a \neq 0 \implies q(b) = 0.

Thus all roots of f that are not a, are roots of q.

by Induction: There are n-1 such roots

\implies \text{at most } n \text{ total distinct roots of } f.

Root of a polynomial in \( F \) of \( f(x) \in F[x] \) is an element \( \alpha \) of \( F \) such that \( f(\alpha) = 0 \).

Suppose \( F \subseteq E \) are fields, and \( f(x) \in F[x] \). A root of the polynomial \( f \) in \( E \) is an element \( \alpha \) of \( E \) so that \( f(\alpha) = 0 \).

Example: \( \mathbb{R} \subseteq \mathbb{C} \), \( f(x) = x^2 + 1 \in \mathbb{R}[x] \).

Then \( f \) has no roots in \( \mathbb{R} \), but it has roots \( i, -i \in \mathbb{C} \).

\( f(i) = (-i)^2 + 1 = -1 + 1 = 0 \).

Example: \( \mathbb{Q} \subseteq \mathbb{R} \), \( f(x) = x^2 - 2 \in \mathbb{Q}[x] \).

Then \( f \) has no roots in \( \mathbb{Q} \), but it has roots \( \pm \sqrt{2} \in \mathbb{R} \).

Def: A principal ideal domain is an integral domain \( R \) in which every ideal is principal, i.e. every ideal
In which every ideal is principal, i.e., every ideal has the form \(<a> = \{ra : r \in R\} \) for some \(a \in R\).

**Example:** \(\mathbb{Z}\) is a P.I.D.

**Pf:** If \(I \subseteq \mathbb{Z}\) is an ideal, then \(I = n\mathbb{Z}\) for some \(n \in \mathbb{Z}\).

**Non-example:** \(\mathbb{Z}[x]\) is not a P.I.D.

E.g., \(<2, x> \subseteq \mathbb{Z}[x]\) is not principal.

In general, for a ring \(R\), \(a_1, a_2, \ldots, a_k \in R\) then
\[
<\{a_1, \ldots, a_k\} = \{\sum_{i=1}^{k} r_ia_i : r_1, r_2, \ldots, r_k \in R\}.
\]

**Thm:** If \(F\) is a field, then \(F[x]\) is a P.I.D.

**Pf:** \(F[x]\) is an integral domain.

Now suppose \(I \subseteq F[x]\) is an ideal. If \(I = \{0\}\), then done. Otherwise, let \(g(x) \in I\) be an element of minimum positive degree. We claim: \(I = \langle g \rangle\).

**Pf of Claim:** Suppose \(f \in I\). Have \(f = qg + r\), \(\deg(r) < \deg(g)\). But \(f \in I, g \in I \Rightarrow r \in I\). This implies \(r = 0\) or \(r\) is a nonzero constant.
If $r$ is a $\neq 0$ constant, $I = R - \langle 1 \rangle$.

Otherwise $r = 0 \implies f \divides qg \implies f \in \langle g \rangle$.

**Corollary** Suppose $F$ is a field, $I$ an ideal of $F[x]$, with $I \neq 0$, $I \neq R$. Then $I = \langle g \rangle$ iff $g$ is an element of $I$ with minimum positive degree.

**Pf:** We proved this in the course of proving the above theorem.

**Example** Consider $\phi : (\mathbb{R}[x] \to \mathbb{C}$ defined by $\phi(f) = f(i)$.

Then $x^2 + 1 \in \ker(\phi)$

- $x^2 + 1$ is a polynomial of min degree in $\ker(\phi)$, because any polynomial of smaller degree is of form $at + bx$, $a, b \in \mathbb{R}$

And $\phi(ax + bx) = a + bi \neq 0$ unless $a = b = 0$.

By Corollary, $\ker(\phi) = \langle x^2 + 1 \rangle = (\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$, by the first isom theorem.

I.e. $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \frac{\mathbb{R}[x]}{\langle \ker(\phi) \rangle} \overset{\sim}{\twoheadrightarrow} \phi(\mathbb{R}[x]) = \mathbb{C}$

First Isom Thm

**Then** Suppose $d \in \mathbb{Z}$, and $d$ is not a square. Then $\mathbb{Z}[x]/\langle x^2 - d \rangle \cong \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$. 
\[ \mathbb{Z} \langle x \rangle / \langle x^2 - d \rangle \cong \mathbb{Z}[\sqrt{d}] = \{ a + b \sqrt{d} : a, b \in \mathbb{Z} \} \]

**Lemma:** Suppose \( a + b \sqrt{d} = 0 \), with \( a, b \in \mathbb{Z} \). Then \( a = b = 0 \).

**Pf:** If \( b = 0 \), then \( a = 0 \), so we're done. Otherwise, \( \sqrt{d} = \frac{-a}{b} \implies d = \frac{a^2}{b^2} \implies d \) is a square. \(-x\)

**Pf of Thm:** Define \( \phi: \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{d}] \) as \( \phi(f) = f(\sqrt{d}) \).

Clear that \( \phi \) is a surjective (hence, a ring homomorphism).

**Claim:** \( \ker \phi = \langle x^2 - d \rangle \).

**Pf of Claim:** Suppose \( f(x) = q(x)(x^2 - d) + a + bx \)

Then \( f(\sqrt{d}) = 0 \) \( \implies a + b\sqrt{d} = 0 \) \( \implies a - b = 0 \).

\( \implies a = b = 0 \).

\( \implies f \in \langle x^2 - d \rangle \).

\( \implies \ker \phi = \langle x^2 - d \rangle \).

\( \implies \mathbb{Z}[x] / \langle x^2 - d \rangle \cong \mathbb{Z}[x] / \ker \phi \cong \mathbb{Z}[\sqrt{d}] \). \( \Box \)

**Ex:** \( \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z} \)

\( f \mapsto f(0) \mod 2 \)
\[ f \rightarrow f(0) \mod 2 \]

\[ \ker f = \langle 2, x \rangle, \] which is not principal.