Question:

“Generalize”: Suppose \( f, g \in \mathbb{Z}[x] \) of degree \( n \).
And suppose moreover \( f \) and \( g \) agree at \( n+1 \) distinct integers, i.e., \( \exists \) integers \( a_0, a_1, \ldots, a_n \) all distinct such that \( f(a_j) = g(a_j) \) \( \forall j \). Then prove \( f(x) = g(x) \).

Last time: Irreducibility of polynomials.

A polynomial is reducible if it has a nontrivial factorization.

Claimed:
- \( x^2 + 1 \) is irreducible over \( \mathbb{Z}/3\mathbb{Z} \)
- \( x^2 - 2 \) is irreducible over \( \mathbb{Q} \)

- In general, hard to verify if a polynomial is irreducible.

Thm: Let \( F \) be a field. If \( f(x) \in F[x] \) and \( \deg(f) = 2 \) or \( 3 \), then \( f \) is reducible over \( F \) \( \iff \) \( f(x) \) has a zero in \( F \).

Non-example: \( x^4 + 2x^2 + 1 \in \mathbb{Q}[x] \)

- \( (x^2 + 1)^2 \)
\[ (x^2 + 1)^2 \] so is reducible over \( \mathbb{Q} \)

- Has no roots in \( \mathbb{Q} \), in fact, no roots in \( \mathbb{R} \)

\[ \text{Pf: Suppose first } f \text{ has a zero in } \mathbb{F}_q, \text{ say } f(a) = 0. \]

Then \[ f(x) = (x-a)g(x) \Rightarrow f \text{ is reducible.} \]

Conversely, suppose \( f \) is reducible, so \[ f(x) = g(x)h(x) \]

with \( \deg(g), \deg(h) < \deg(f) \). Then at least one of \( g \) or \( h \) is degree one, say \[ g(x) = ax + b \] with \( a, b \in \mathbb{F}_q \) \( a \neq 0 \). Then \(-a^{-1}b\) is a root of \( g \) and thus of \( f \), so \( f \) has a zero. \( \Box \)

**Ex** \( x^2 + 1 \) has no zeros in \( \mathbb{Z}/32 \) because

\[
\begin{align*}
0^2 + 1 &= 1 \\
1^2 + 1 &= 2 \\
2^2 + 1 &= 5 \equiv 2
\end{align*}
\]

\[ \Rightarrow x^2 + 1 \text{ is irreducible over } \mathbb{Z}/32 \]

**Ex** \( x^2 - 2 \) is irreducible over \( \mathbb{Q} \) because \( 2 \) is not a square in \( \mathbb{Q} \), so there are no zeros in \( \mathbb{Q} \).
However, \(x^2 - 2\) is reducible over \(\mathbb{R}\).

**Thm:** Let \(F\) be a field and \(p(x) \in F[x]\). Then \(\langle p(x) \rangle\) is a maximal ideal in \(F[x]\) \(\iff\) \(p(x)\) is irreducible over \(F\).

**Pf:** Suppose first \(\langle p(x) \rangle\) is maximal, and \(p(x) = g(x)h(x)\). Then \(\langle p(x) \rangle \subseteq \langle g(x) \rangle \subseteq F[x]\).

But \(p(x)\) is maximal \(\Rightarrow\)

\[\langle p(x) \rangle = \langle g(x) \rangle \text{ or } \langle g(x) \rangle = F[x].\]

In this case, \(\deg(p) = \deg(g)\)
\[\overset{\text{??}}{=\rightarrow} h(x)\text{ is a unit.}\]

\[\overset{\text{?}}{=} p(x)\text{ is irreducible.}\]

Suppose conversely \(p(x)\) is irreducible over \(F\), and
\[\langle p(x) \rangle \subseteq I \subseteq F[x]\]
where \(I\) is an ideal.
\[ F[x] \text{ is PID. } \implies I = \langle g(x) \rangle \text{ for some } g. \]

\[ \implies p(x) = g(x)h(x) \text{ for some } h(x) \in F[x]. \]

\[ p(x) \text{ irreducible } \implies \text{ one of } g \text{ or } h \text{ is a unit} \]

\[ \cdot g(x) \text{ a unit } \implies I = \langle g(x) \rangle = F[x] \]

\[ \cdot h(x) \text{ a unit } \implies I = \langle g(x) \rangle = \langle p(x) \rangle \]

\[ \implies \langle p(x) \rangle \text{ is maximal}. \]

\( \square \)

Aside! \( x^2 - 2 \) is irreducible over \( \mathbb{Q} \)

\[ x^2 - 2 = 2 \left( \frac{1}{2} x^2 - 1 \right) \text{ but } 2 \in \mathbb{Q} \text{ is a unit.} \]

**Corollary**

Let \( F \) be a field, \( p(x) \) irreducible polynomial over \( F \).

Then \( F[x]/\langle p(x) \rangle \) is field.

This corollary is how one actually constructs new fields from old fields.

**Cor**

Let \( F \) be a field, and \( p(x), a(x), b(x) \in F[x] \).

If \( p(x) \) is irreducible over \( F \) and \( p(x) | a(x)b(x) \) then \( p(x) | a(x) \) or \( p(x) | b(x) \).
Pf: \( \langle p(x) \rangle \) is maximal \( \Rightarrow \) \( \langle p(x) \rangle \) is a prime ideal.

\[ a(x) b(x) \in \langle p(x) \rangle \Rightarrow a(x) \in \langle p(x) \rangle \text{ or } b(x) \in \langle p(x) \rangle. \]

But \( a(x) \in \langle p(x) \rangle \) means \( p(x) \mid a(x) \)
and \( b(x) \in \langle p(x) \rangle \) means \( p(x) \mid b(x) \). \( \square \)

**Examples**

1. \( F = \mathbb{Q} \), \( p(x) = x^2 - 2 \). Then
   \[ \mathbb{Q}[x] / \langle x^2 - 2 \rangle \]

   is a field. In fact,

   \[ \mathbb{Q}[x] / \langle x^2 - 2 \rangle \cong \mathbb{Q}[\sqrt{2}] = \{ a + b\sqrt{2} : a, b \in \mathbb{Q} \} \]

**Idea of proof:** Define \( \phi : \mathbb{Q}[x] \rightarrow \mathbb{Q}[\sqrt{2}] \)

\[ f(x) \mapsto f(\sqrt{2}) \]

- Clearly \( \phi \) is a surj ring homom.
- Can check \( \ker(\phi) = \langle x^2 - 2 \rangle \)
- First Isom Thm \( \mathbb{Q}[x] / \langle x^2 - 2 \rangle \cong \mathbb{Q}[\sqrt{2}] \)

2. \( \mathbb{Z}[i] / \langle 3 \rangle \cong \left( \mathbb{Z}[x] / \langle x^2 + 1 \rangle \right) / \langle 3 \rangle \)

\[ \cong \mathbb{Z}[x] / \langle 3, x^2 + 1 \rangle \]
\[ \mathbb{Z}_3[x] / \langle x^2 + 1 \rangle \]

But \( x^2 + 1 \) is irreducible over \( \mathbb{Z}_3 \)

\[ \mathbb{Z}[x] / \langle 3 \rangle \] is a field.

In fact, this field has \( 9 = 3^2 \) elements.

**Example 3** The polynomial \( x^3 + x + 1 \) is irreducible over \( \mathbb{Z}_2 \)

\[ \mathbb{Z}_2[x] / \langle x^3 + x + 1 \rangle \] is a field.

This field has \( 8 = 2^3 \) elements.

**Lemma** Suppose \( F \) is a field, \( g(x) \in F[x] \) a polynomial.

The polynomials in \( F[x] \) of degree \( \leq \deg(g) \) are a complete set of distinct coset representatives for \( F[x] / \langle g(x) \rangle \).

**Pf:** Suppose \( f(x) \in F[x] \). Then \( f = qg + r \) with \( \deg(r) < \deg(g) \)

\[ \Rightarrow f(x) + \langle g(x) \rangle = f(x) + \langle g(x) \rangle. \]
Conversely, if \( r_1, r_2 \in F(x) \) and \( \deg(r_1), \deg(r_2) < \deg(g) \) then
\[
\text{if } \quad r_1(x) + \langle g(x) \rangle = r_2(x) + \langle g(x) \rangle
\]
\[
\implies g(x) \mid r_1 - r_2
\]
\[
\implies r_1(x) - r_2(x) = 0 \quad \Rightarrow \quad r_1(x) = r_2(x).
\]