Fermat's Last Theorem

(1633)

There are no positive integers \( x, y, z \geq 2 \) with

\[ x^n + y^n = z^n \quad \text{for some } n \geq 3. \]

\[ 3^2 + 4^2 = 5^2 \]
\[ 5^2 + 12^2 = 13^2 \]

Prop 10.2.2 Let \( F \subseteq E \) be fields with \( x \notin F \)

\[ F[x] = \left\{ f(x) : f(x) \in F[x] \right\} \]

1) is subring of \( E \) containing \( F \) and \( x \)
1. \( F(a) = \{ f(g(x)) : f(x), g(x) \in F[x], g(x) \neq 0 \} \)

2. \( F[a] \) is the smallest such subring

3. \( F \) is a subfield of \( F \) containing \( F \) and \( a \).

4. \( F(a) \) is a subfield

Note: We will see later that \( F[a] = F(a) \).

By 2) Let \( R \subset E \) be another such subring. Since \( a \in R \), \( a^n \in R \) for all \( n > 0 \) and \( \sum_{i=0}^{n} c_i a^i \) with \( c_i \in F \) is in \( R \).

Hence \( R \supset F[a] \)

4) Similar argument. QED
e.g. \( F = \mathbb{Q} \), \( E = \mathbb{R} \), \( \alpha = \sqrt{2} \)

\[
F[\alpha] = \frac{1}{2} \sum_{i=0}^{n} c_i (\sqrt{2})^i \quad c_i \in \mathbb{Q}
\]

\[
= \left\{ a + b \sqrt{2} : a, b \in \mathbb{Q} \right\}
\]

We know

\[
\frac{\alpha + b \sqrt{2}}{(c + d \sqrt{2}) (c - d \sqrt{2})} = \frac{(ac - 2bd) + (bc - ad) \sqrt{2}}{c^2 - 2d^2}
\]

\[
= \alpha + b \sqrt{2} \quad \text{with } a, b \in \mathbb{Q}
\]

Every element in \( F[\alpha] \) has this form.
Hence \( F(x) = F[x] \)

Def \( F \unlhd F(x) \unlhd E \)

\( E \) is a field extension of \( F \)

\( F(x) \) is the field obtained from \( F \) by adjoining \( x \).

Thm 10.2.5 (Kronecker)

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

not a constant. Then there is a field extension \( E \) with \( x \in E \) with \( p(x) = 0 \).
Pf: If \( p(x) \) is irreducible, then let \( E = F[x] / (p(x)) \) and \( \alpha = x \).

If not, then \( p(x) = p_1(x)p_2(x) \ldots \)

where each \( p_i(x) \) is irreducible.

Let \( E = F[x] / (p_i(x)) \) for some \( i \).

\( \alpha = x \)

\( p(\alpha) = p_1(\alpha)p_2(\alpha) \ldots = p_i(\alpha) \) something

\( = 0 \) since \( p_i(\alpha) = 0 \). QED.

Def: \( F \subseteq E \) and \( \alpha \in E \). If there is a monic polynomial \( f(x) \in F[x] \)

with \( f(\alpha) = 0 \), \( \alpha \) is algebraic over \( F \).
If not, \( \alpha \) is transcendental over \( F \), e.g. \( \pi \) and \( e \) are transcendental over \( \mathbb{Q} \).

\( \alpha = \sqrt{2} + \sqrt{3} \) is algebraic.

\[
\alpha^2 = (\sqrt{2} + \sqrt{3})^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6}
\]

\[
\alpha^2 - 5 = 2\sqrt{6}
\]

\[
(\alpha^2 - 5)^2 = (2\sqrt{6})^2
\]

\[
\alpha^4 - 10\alpha^2 + 25 = 24
\]

\[
\alpha^4 - 10\alpha^2 + 1 = 0
\]

Then \( 10, 2, \sqrt{2}, \sqrt{3} \) let \( F \subset E \) with \( \alpha \in E \) algebraic over \( F \). Then \( E \).
monic polynomial \( p(x) \in \mathbb{F}[x] \) with

1) \( p(\alpha) = 0 \)

2) \( p(x) \) is irreducible

3) if \( f(x) \in \mathbb{F}[x] \) with \( f(\alpha) = 0 \)

then \( p(x) \mid f(x) \).

\( p(x) \) is the minimal polynomial of \( \alpha \)

**Proof:** Let \( J = \langle f(x) \rangle \subseteq \mathbb{F}[x] \) s.t. \( f(\alpha) = 0 \).

It is an ideal, let it be principal.

\( J = \langle p(x) \rangle \) with \( p(x) \) monic.

This \( p(x) \) is the minimal poly.
2) Suppose \( p(x) \) is reducible, i.e.
\[
p(x) = p_1(x) p_2(x) \text{ with } \deg p_1(x) < \deg p(x)
\]
\[
0 = p(x) = p_1(x) p_2(x) \in E
\]
Hence either \( p_1(x) = 0 \) or \( p_2(x) = 0 \)
One is in \( \mathbb{F} \), contradiction.

3) Obvious \( \text{QED} \)

Def 10.2.1.0 For \( F \subseteq E \) as above the degree of \( x \) is that of its minimal polynomial.

e.g. \( \sqrt{2} + \sqrt{3} \) has degree 4 / \( \mathbb{Q} \)
Theorem 10.2.11 \[ \text{Let } F \subseteq E \text{ with } \] 
minimal polynomial \( p(x) \) of degree \( N \) 

1) \( F(x) = F[x] / p(x) \) = \( F[x] \) 

2) \( \{1, x, x^2, \ldots , x^{N-1} \} \) is a basis of \( F(x) \) over \( F \) 

3) \( \dim_{F} F(x) = \deg(x) = \deg p(x) = N \) 

Proof 1) Consider the ring homomorphism \( F[x] \rightarrow E \) 

by \( \phi(f(x)) = f(x) \) 

Its image is \( F[x] \) by definition 

Its kernel is \( J = (p(x)) \)
Since \( p(x) \) is in \( F[x] \), \( F[x]/p(x) \) is a field, so \( F(x) = F[x] \).

2) Let \( S = \langle \{1, x, x^2, \ldots, x^{n-1}\} \rangle \)

\[
= \left\{ \sum_{i=0}^{n-1} c_i x^i : c_i \in F \right\}
\]

Clearly \( S \subseteq F[x] \)

To show \( F[x] \subseteq S \), it suffices to show \( x^m \in S \) for all \( m \geq 0 \).

\[ p(x) = x^n - \sum_{i=0}^{n-1} p_i x^i \quad \text{with} \quad p_i \in F \]

This means that \( \in F[x] \).
\[ x^n = \sum_{i=0}^{n-1} \beta_i x^i \in S \]

\[ x^{n+1} = \sum_{i=0}^{n-1} \beta_i x^{i+1} = \beta_n x^n + \sum_{i=0}^{n-2} \beta_i x^i \in S \]

In $S$ by above calculation

\[ x^{n+k} \in S \text{ by induction on } k. \]

Hence $S = F[x]$.

3) Follows from 2)