Example: Find the greatest common divisor of

\[ x^2 + 6x + 5, \quad x^4 + 4x^3 + 6x^2 + 5x + 2, \]

in \( \mathbb{Q}[x] \).

\[ \begin{array}{c}
\begin{array}{c}
\underline{x^2 - 2x + 13} \\
2x^2 + 6x + 5)
\end{array} \\
\begin{array}{c}
x^4 + 4x^3 + 6x^2 + 5x + 2 \\
- x^4 - 6x^3 - 5x^2 \\
\hline
-2x^3 + x^2 + 5x + 2 \\
2x^3 + 12x^2 + 10x
\end{array}
\end{array} \]
\[ \begin{array}{c}
13 x^2 + 15 x + 2 \\
- 13 x^2 - 78 x - 65 \\
\hline
- 63 x - 63 \\
\hline
\end{array} \]

In \( \mathbb{Q}[x] \), 
-63 is a unit (reciprocal \( \frac{1}{63} \))

\( x + 1 \) can replace \(-63x - 63\)

\[ \begin{array}{c}
x^2 + 6x + 5 \\
\hline
x + 1 \\
\hline
\end{array} \]

\[ \begin{array}{c}
x + 5 \\
\hline
x + 1 \quad (x^2 + 6x + 5) \\
\hline
- x^2 - x
\end{array} \]
\[5x + 5 \quad - \quad 3x + 5 \overline{\quad 0}\]

Answer to the problem: \[x + 1\].

Complex conjugation: \[a + bi \mapsto a - bi, \quad a, b \in \mathbb{R}\]

The generator of \(Gal(\mathbb{C}/\mathbb{R}) = \sqrt{2}\).

A polynomial in \(\mathbb{R}[x]\)
with coefficients in \( \mathbb{R} \)

can be considered as a polynomial in \( \mathbb{C}[x] \)

which is left fixed by complex conjugation.

But in \( \mathbb{C}[x] \) the polynomial factors into

linear factors

\[ p(x) = a_m (x - \nu_1) (x - \nu_2) \cdots (x - \nu_m) \]

\( (a_m \neq 0) \)

\( C \subseteq \mathbb{R} \)

\[ \overline{p(x)} = a_m (x - \overline{\nu_1}) (x - \overline{\nu_2}) \cdots (x - \overline{\nu_m}) \]
By uniqueness of factorisation,

\( \alpha_1, \ldots, \alpha_n \) are the same root as

\( \bar{\alpha}_1, \ldots, \bar{\alpha}_n \) (possibly in a different order)

A root can therefore either be a real number, or its complex conjugate is another root.

What about irreducible polynomials over \( \mathbb{R} \)?

an irreducible polynomial \( \in \mathbb{R}[x] \)

with every root \( \alpha \), \( \mathbb{R} \) must have a complex conjugate root \( \bar{\alpha} \). So if \( \alpha \in \mathbb{R} \)
\[ x - v \text{ is a factor of } p(x) = p(x) \text{ is linear} \]
\[ a_1 (x - v) \]

If \( v \) is not real, then,
\[ (x - v)(x - \overline{v}) \text{ is a factor of } p(x) = \]
\[ p(x) = a_2 (x - v)(x - \overline{v}) \]

\[ \therefore \text{ An irreducible polynomial in } \mathbb{R}[x] \text{ is linear or quadratic.} \]

\[ Q(\sqrt{a - \sqrt{b}}) \text{ below or not over } Q? \]
\[ (a - \sqrt{b})(a + \sqrt{b}) = \sqrt{a^2 - b} \text{ must be in the field.} \]
\[ Q(\sqrt{2 - \sqrt{2}}) \text{ yes}, \quad Q(\sqrt{2 - \sqrt{3}}) \text{ no} \]
Example:

\[ \mathbb{Q}[x]/(x^2 + 3) \cong \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\pm \sqrt{3}) \]

\[ (x - r_1) (x - r_2) \]

\[ x^2 + 3 = (x - r_1 \sqrt{3}) (x + r_1 \sqrt{3}) \]

\[ r_2 = -r_1 \]

This is the splitting field of \( x^2 + 3 \) over \( \mathbb{Q} \), because it is quadratic (attacking one root, we also get the other one).

Degree of a splitting field.
\text{Gal}(\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_k})/\mathbb{Q})

\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) = \mathbb{Q}(\sqrt{12}, \sqrt{3})

\left(\sqrt{2}/\sqrt{2}\right)^k = \sqrt[2k]{2 \times \cdots \times 2}

\text{degree} = 2^k

\text{Splitting field of } x^4 - 3 \text{ over } \mathbb{Q}

\text{roots: } \sqrt[4]{3}, -\sqrt[4]{3}, -\sqrt[4]{3}, -\sqrt[4]{3}

\text{Quaternions: } \mathbb{Q}(\sqrt{(2-\sqrt{2})(3-\sqrt{3})})

\text{Splitting field: }
$\mathbb{Q}(\sqrt[4]{3}, i)$

degree 8.

Generators $D_4$ 
($|D_4| = 8$)

(symmetries of a square)
Nested square root:

\[ \sqrt{2 - \sqrt{2}} \cdot \sqrt{2 + \sqrt{2}} = \sqrt{2} \]

\[ \sqrt{2 + \sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2 - \sqrt{2}}} \]

\[ \sqrt{2 - \sqrt{2}} \cdot \sqrt{2 + \sqrt{2}} = \sqrt{2} \]

\[ -\sqrt{2 + \sqrt{2}} \leftrightarrow \sqrt{2 - \sqrt{2}} \]

\[ \sqrt{2} \leftrightarrow -\sqrt{2} \]
\[x = \sqrt{2} - \sqrt{2} \]
\[x^2 - 2 = -\sqrt{2} \quad (x^2 - 2)^2 = 2 \]

\[\begin{align*}
(x^2 - 2)^2 - 2 &= 0 \\
\text{degree 4}
\end{align*} \]

\[\therefore \text{ Galois group has no more element } \cong \mathbb{Z}/4. \]

\[\mathbb{Q}\left( \sqrt{5}, \sqrt{3} \right) \quad (x^2 - 5)(x^2 - 3) \]

\[\begin{align*}
\sqrt{5} & \quad \sqrt{2} \\
-\sqrt{5} & \quad -\sqrt{2}
\end{align*} \]

irreducible over \( \mathbb{Q}(\sqrt{5}) \)
Teaching evaluations, please!

Thank you!