Splitting Fields

Start by waking up the audience:

Q: • What is $k[x]/(p(x))$?

• When is this thing a field ?

• In which examples have you encountered this construction ?

In full generality, k is a ring, $k[x]$ is the polynomial algebra in one variable over k, and $(p(x))$ is a principal ideal in $k[x]$, so $k[x]/(p(x))$ is its quotient ring. We have typically given the coset of x in the quotient a new name, say α, so that in the quotient we have imposed the identity $p(\alpha) = 0$.

The quotient ring is a field if k is a field and $p(x)$ is an irreducible polynomial over k. We have seen two types of example: (1) describing intermediate field extensions generated by an algebraic element, such as

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$$

$\sqrt{2}$ is algebraic over $\mathbb{Q}$ with irreducible polynomial $x^2 - 2$.

So, we have an isomorphism of field extensions

$$\begin{tikzcd} & \mathbb{Q} \arrow[dl, hook] \arrow[dr, hook] & \\ \mathbb{Q}[x]/(x^2-2) \arrow[rr, "\cong"] & & \mathbb{Q}(\sqrt{2}) \subset \mathbb{R} \end{tikzcd};$$

(2) building new (and bigger) fields from old ones, such as

$$\mathbb{C} = \mathbb{R}[x]/(x^2+1)$$

$$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$$

$$\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1) \quad \text{or} \quad \mathbb{F}_2[x]/(x^3+x^2+1) -$$

$$\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)$$

and so on.

Key observation

To make this work, we needed to start with a polynomial $p(x)$ with coefficients in k, and $p(x)$ had to be irreducible.

If, however, we view $p(x)$ as a polynomial with coefficients in the bigger field $K = k[x]/p(x)$, then we have, by construction, at least one root of $p(x)$ in K, namely the coset of x, i.e., $\alpha = x + (p(x)) \in K$.

This allows us to split off a linear factor of the (no longer irreducible) polynomial $p(x)$ over K:

$$p(x) = (x-\alpha)\cdot q(x)$$

inside $K[x]$.

Examples:

$$x^2+1 = (x+i)\cdot(x-i) \quad \text{over } \mathbb{C},\ \mathbb{F}_9$$

$$x^3+x+1 = (x+b)\cdot(x+b^2)\cdot(x+b^2+b) \quad \text{over } \mathbb{F}_8$$

$$x^2+x+1 = (x+a)\cdot(x+a+1) \quad \text{over } \mathbb{F}_4$$

comment on how we got there: we know from the tutorials that b ($=$ coset of x in $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$) and b^2 are roots of x^3+x+1. The third root is obtained by polynomial division (over $\mathbb{F}_8$).
↳ this week's tutorial.

For $\mathbb{F}_4$, it is easier: the polynomial has at least one root over $\mathbb{F}_4$, a, and hence both roots ($\deg = 2$). $\mathbb{F}_4 \setminus \mathbb{F}_2$ has only two elements, a and $a+1$. Either a is a double root (it isn't) or it is as claimed.

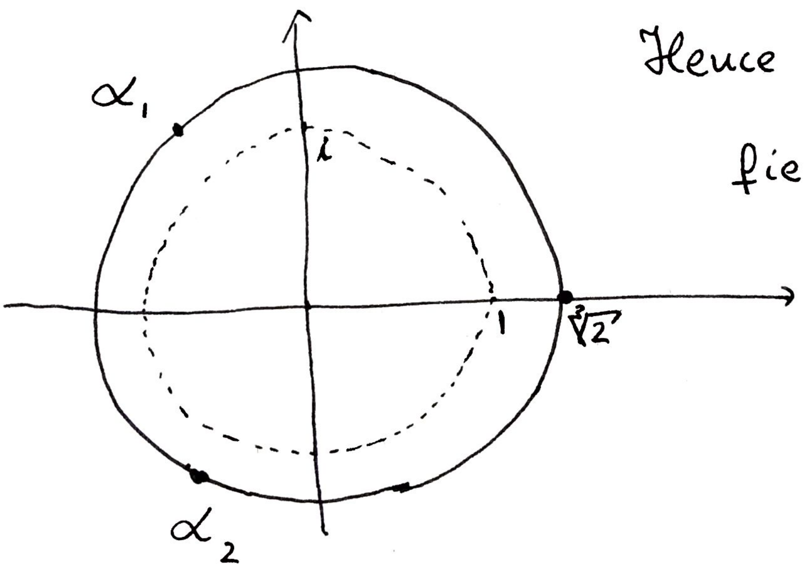
Similarly, $X^2 - 2 = (X+\sqrt{2})(X-\sqrt{2})$ over $\mathbb{Q}(\sqrt{2})$. Indeed, for degree reasons, the polynomial has to split into linear factors over $\mathbb{Q}(\sqrt{2})$, and the second root is easy to find.

<u>Example:</u> Consider the polynomial

$$p(x) = X^3 - 2 \quad \text{over } \mathbb{Q}.$$

This is irreducible over $\mathbb{Q}$, has one root ~~over~~ in $\mathbb{R}$, which we will denote $\sqrt[3]{2} \in \mathbb{R}$ and two additional complex roots,

$$\alpha_{1,2} := \sqrt[3]{2} \cdot e^{\pm \frac{2\pi i}{3}} = \frac{\sqrt[3]{2}}{2}\left(-1 \pm i\sqrt{3}\right).$$



Hence, we have field isomorphisms

$$\begin{tikzcd}
 & \mathbb{C} & & \\
\alpha_1 & \mathbb{Q}(\alpha_1) \arrow[u, phantom, "\cup"] & & \\
x \arrow[u, mapsto] \arrow[d, mapsto] & \mathbb{Q}[x]/(x^3-2) \arrow[u, phantom, "\cong"] \arrow[d, phantom, "\cong"] \arrow[r, phantom, "\cong"] & \mathbb{Q}(\sqrt[3]{2}) & x \mapsto \sqrt[3]{2} \\
\alpha_2 & \mathbb{Q}(\alpha_2) & \mathbb{R} \arrow[u, phantom, "\supset"] & \\
 & \mathbb{C} \arrow[u, phantom, "\cup"] & \mathbb{C} \arrow[u, phantom, "\cup"] &
\end{tikzcd}$$

p is the irreducible polynomial of each of the three roots.

Over $\mathbb{R}$ (and hence over $\mathbb{Q}(\sqrt[3]{2})$) the factorization of x^3-2 into irreducible polynomials takes the form

$$x^3 - 2 = (x - \sqrt[3]{2}) \cdot \underbrace{\left(x^2 + \sqrt[3]{2}\,x + (\sqrt[3]{2})^2\right)}_{\substack{\text{irreducible} \\ \text{over} \\ \mathbb{Q}[x]/(x^3-2) \;\cong\; \mathbb{Q}(\sqrt[3]{2}).}}.$$

Our polynomial does not split into linear factors over $\mathbb{Q}[x]/(x^3-2)$, but its irreducible components now have lower degree, so we can iterate. $x^2 + \sqrt[3]{2}\,x + (\sqrt[3]{2})^2$ is the irreducible polynomial of each of the roots α_1 and α_2 over $\mathbb{Q}(\sqrt[3]{2})$.

$$\begin{tikzcd}
 & & & \mathbb{Q}(\sqrt[3]{2})(\alpha_1) \\
\mathbb{Q} \arrow[r, phantom, "\subset"] & \mathbb{Q}(\sqrt[3]{2}) \arrow[r, phantom, "\subset"] & \mathbb{Q}(\sqrt[3]{2})[x]/\left(x^2+\sqrt[3]{2}x+(\sqrt[3]{2})^2\right) \arrow[ur, "\cong", "x \mapsto \alpha_1"'] \arrow[dr, "\cong", "x \mapsto \alpha_2"'] & \\
 & & & \mathbb{Q}(\sqrt[3]{2})(\alpha_2)
\end{tikzcd}$$

$$\underbrace{\mathbb{Q} \underset{\substack{\text{degree 3} \\ \text{extension}}}{\subset} \mathbb{Q}(\sqrt[3]{2}) \underset{\substack{\text{degree 2} \\ \text{extension}}}{\subset} \mathbb{Q}(\sqrt[3]{2})[x]/\left(x^2+\sqrt[3]{2}x+(\sqrt[3]{2})^2\right)}_{\text{degree 6 extension}}$$

But $\alpha_1 + \alpha_2 = -\sqrt[3]{2}$, so the intermediate field extensions of $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{C}$ generated by α_1 and α_2 respectively are equal to each other

$$\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2})(\alpha_1) = \mathbb{Q}(\sqrt[3]{2})(\alpha_2) \subseteq \mathbb{C}.$$

<u>Exercise:</u> (1) Show that $\mathbb{Q}(\sqrt[3]{2})(\alpha_1) = \mathbb{Q}(\sqrt[3]{2}, \alpha_1)$

$= \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) \subset \mathbb{C}$ is the smallest intermediate extension of $\mathbb{Q} \subset \mathbb{C}$ containing the two algebraic elements $\sqrt[3]{2}$ and $i\sqrt{3}$.

(2) How many automorphisms of the field $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ can you construct?