12. Splitting fields

Let k be a field and let $f(x)$ be a nonzero polynomial with coefficients in k. Is there necessarily some larger field in which f splits into linear factors? You might be used to using the Fundamental Theorem of Algebra to say that the complex numbers have this property but that doesn't answer the questions like: "Is there a field containing $\mathbb{Z}_5$ where $x^3 - x + 2$ splits into linear factors?" Today's goal is to prove that the answer is yes:

We say that f ***splits in*** L if f factors as $c\prod_{j=1}^{d}(x-\theta_j)$ in L. We will say that L is a ***splitting field*** for f if f splits in L and $L = k[\theta_1, \dots, \theta_d]$. Here is today's goal:

Theorem Let k be a field and let $f(x)$ be a degree d nonzero polynomial with coefficients in k. Then there is a splitting field for f.

We start with examples.

Problem 12.1. Let ζ be a primitive n-th root of unity. Show $\mathbb{Q}[\zeta]$ is a splitting field for $x^n - 1$ over $\mathbb{Q}$.

Problem 12.2. Show that $\mathbb{Q}(\sqrt[3]{2})$ is **not** a splitting field for $x^3 - 2$ over $\mathbb{Q}$.

Problem 12.3. As usual, let $\omega = \frac{-1+\sqrt{-3}}{2}$. Show that $\mathbb{Q}[\omega, \sqrt[3]{2}]$ is a splitting field for $x^3 - 2$ over $\mathbb{Q}$.

We now move to generalities:

Problem 12.4. Let k be a field and let $f(x)$ be a degree d nonzero polynomial with coefficients in k. Let $m(x)$ be an irreducible factor of $f(x)$ and let $k_1 = k[t]_{m(t)}$. Show that the polynomial $f(x)$ has a root in k_1. There is very little to say here; this is about understanding the notation.

Problem 12.5. Prove the Theorem at the top of the page, by induction on $\deg(f) - \#(\text{roots of } f \text{ in } k)$.

Readers with some mathematical sophistication may wonder whether splitting fields are unique. The answer is essentially yes, but we first need to set up the vocabulary to answer the question.