0.1 Extension fields

Given a polynomial, is it possible to find a field in which that polynomial has a root? For example, consider the polynomial $x^2 + 1$.

Definition 0.1. Let F be a field. If $E \supseteq F$ is a field and the operations of E restricted to F are the same as the operations of F, then E is an **extension field** of F.

If E is an extension field of F, we can say that E is an extension of F, or E extends F. Note the abuse of notation here again: F may not actually be a subset of E, but if it is isomorphic to a subfield of E it is good enough.

Example 0.2. $\mathbb{C}$ is clearly an extension field of $\mathbb{R}$. Additionally, $\mathbb{R}$ is an extension field of $\mathbb{Q}$. //

Example 0.3. Let F be a field and let $p \in F[x]$ be irreducible over F. Then, $F[x]/\langle p \rangle$ is an extension field of F. Notice that we can embed F as a subfield of $F/\langle p \rangle$ by the map

$$x \mapsto x + \langle p \rangle.$$

It is not too hard to see that this map is an isomorphism onto its image. We will use this example to motivate the following theorem. //

Theorem 0.4 (Existence of Extension Fields)**.** Let F be a field and let $f \in F[x]$ be a nonconstant polynomial. Then there exists an extension field E of F such that f has a root in E.

Proof. Let $p(x)$ be an irreducible factor of f. This exists as $F[x]$ is a UFD. It suffices to produce an extension field of F where p has a root in. Let $E = F[x]/\langle p \rangle$. Then F embeds into E. Now, we see that $x + \langle p \rangle$ is a root of p in E. Write $p(x) = \sum_{i=0}^{n} a_i x^i$, then

$$p(x + \langle p \rangle) = \sum_{i=0}^{n} a_i (x + \langle p \rangle)^i = \left(\sum_{i=0}^{n} a_i x^i \right) + \langle p \rangle = \langle p \rangle.$$

□

Note that if D is an integral domain and $p \in D[x]$, then there is an extension field of $Q(D)$ that contains a root of p. This means that there is an extension field that contains D. This need not be true if D is not an integral domain.

Example 0.5. Let $f(x) = 2x + 1$ in $\mathbb{Z}_4[x]$. Then given any ring $R \supseteq \mathbb{Z}_4$, f has no roots in R. //

0.2 Splitting Fields

Definition 0.6. Let F be a field, and let E be an extension of F. Then we *define* $F(a_1, \dots, a_n)$ to be the *smallest* subfield of E that contains F and $\{ a_1, \dots, a_n \}$.

It immediately follows that $F(a_1, \dots, a_n)$ is the intersection of all subfields of E that contain F and $\{ a_1, \dots, a_n \}$. We warn the reader that it is important that we have an extension field to talk about. For example, it is nonsensical to write something like $\mathbb{Q}(\text{apple})$ when we don't have any field that contains apple in it.

Definition 0.7 (Polynomial splitting)**.** Let F be a field and let E be an extension of F. Let $f \in F[x]$. Then f **splits** in E if it can be factorized into linear factors, i.e. we have $a \in F$, $a_i \in E$ such that

$$f(x) = a(x - a_1) \cdots (x - a_n).$$

We say that E is a **splitting field for** f if $E = F(a_1, \dots, a_n)$.

In other words, E is a splitting field for f it is the smallest field that contains F and all roots of f. We remark that whether a polynomial splits depends on which field the polynomial comes from.

Example 0.8. Let $f(x) = x^2 + 1$ in $\mathbb{Q}[x]$. Then $\mathbb{C}$ is *not* a splitting field of f over $\mathbb{Q}$, since we can find a smaller field that still contains roots of f, namely, $\mathbb{Q}[x]/\langle f \rangle$. //

It would be pretty stupid if splitting fields did not exist. Luckily they do.

Theorem 0.9 (Splitting fields exist)**.** Let F be a field and $f \in F[x]$ be nonconstant. Then there is a splitting field of f over F.

The proof of the theorem is simple: induction on $\deg f$ and use Theorem 0.4.

Proof. We go by induction[1] on $\deg f$. If $\deg f = 1$ it is trivial: $f(x) = (x - a)$ for some $a \in F$. Now suppose the theorem is true for all polynomials of degree less than $\deg f$ and all fields. By Theorem 0.4, there is an extension field $E \supseteq F$ such that f has a root in E. Let this root be a_1. Then we factorize f over E, so write $f(x) = (x - a_1)g(x)$, where $g(x) \in E[x]$. Thus there is a splitting field $K \supseteq E$ of g over E. K has all roots of g, say they are $a_2, \ldots, a_n$. Since $E \supseteq F$, K contains a_1, F and $a_2, \ldots, a_n$. So we can take the splitting field to be $F(a_1, \ldots, a_n)$. $\square$

Now we can finally give some examples of splitting fields.

Example 0.10. Let $f(x) = x^2 + 1$, but this time considered as an element of $\mathbb{R}[x]$. Then $\mathbb{C}$ is a splitting field of f over $\mathbb{R}$. Notice that $\mathbb{R}[x]/\langle f \rangle$ also is a splitting field of f. Are these the same splitting field? We will answer this soon. //

[1] Note that strong induction is used here, since $\deg g$ may not necessarily be $\deg f - 1$. If I am wrong, please correct me.