Algebraic field extensions

Recall that if F is a field and E is an extension of F, and $\alpha \in E$, then we write $F(\alpha)$ for the smallest subfield in E which contains F and α.

Of course in this case $F(\alpha)$ is again a field extension of F, and E is an extension of $F(\alpha)$. In short, $F \subset F(\alpha) \subset E$. We call $F(\alpha)$ a *simple extension* of F. We can iterate this notation: for elements $\alpha_1, \ldots, \alpha_n \in E$ we write $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for the smallest field in E containing F and the elements $\alpha_1, \ldots, \alpha_n$.

An element $\alpha \in E$ in an extension field E of F is called *algebraic* over F if there is some polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. Otherwise α is called *transcendental*.

Examples

1. The element $i = \sqrt{-1}$ is algebraic over $\mathbb{Q}$, because it satisfies $f(i) = 0$ where $f(x) = x^2+1$.

2. The elements $\sqrt{2}$, $\sqrt{3}$, $\sqrt{2}+\sqrt{3}$ are algebraic over $\mathbb{Q}$. They first two are roots of x^2-2, x^2-3, respectively. What about the third? Let $\alpha = \sqrt{2}+\sqrt{3}$. We compute

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

$$(\alpha^2-5)^2 = (2\sqrt{6})^2 = 24$$

Thus $\alpha = \sqrt{2}+\sqrt{3}$ satisfies $f(\alpha) = 0$ where $f(x) = (x^2-5)^2 - 24 = x^4 - 10x^2 + 1$.

3. The numbers π and e are transcendental over $\mathbb{Q}$. This is because they are not the roots of any polynomial with coefficients in $\mathbb{Q}$.

4. Any n^{th} root of a rational number p/q is algebraic over $\mathbb{Q}$, since it satisfies $x^n - p/q = 0$. More generally, any number obtained from the rationals via the operations of multiplication, addition, division, and taking various types of n^{th} roots is algebraic over $\mathbb{Q}$. For example,

$$\sqrt[5]{\frac{\sqrt{2}-1}{\sqrt[3]{4+\sqrt{5}}}}$$

is algebraic over $\mathbb{Q}$. This may not be obvious, but it will follow from a result we will prove.

5. All of the above examples are about algebraic and transcendental numbers over $\mathbb{Q}$. The numbers π and e are algebraic over $\mathbb{R}$, because they are in $\mathbb{R}$! Precisely, they satisfy the polynomial equations $x - \pi = 0$ and $x - e = 0$, and these are of course polynomials in $\mathbb{R}[x]$. As another example, $\sqrt{\pi}$ is algebraic over $\mathbb{Q}(\pi)$.

An extension E of a field F is *algebraic* if every $\alpha \in E$ is algebraic over F, and is called *transcendental* otherwise.

▶ **Suppose $\alpha \in E$ is algebraic over F. Then there is a unique monic irreducible polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.**

Proof. Consider the evaluation homomorphism $\phi_\alpha : F[x] \to F(\alpha)$ given by $\phi_\alpha(f(x)) = f(\alpha)$. Since F is a field, $F[x]$ is a PID, and thus the kernel of ϕ_α is an ideal $(f(x))$ where $f(x) \in F[x]$. Note that for a constant polynomial $g(x) = a \in F$ we have $\phi_\alpha(g(x)) = a$, and also for $g(x) = x$ we have $\phi_\alpha(g(x)) = \alpha$. Thus ϕ_α is onto, as the image contains F and α, and $F(\alpha)$ is the smallest field containing F and α. The 1st Isomorphism Theorem then gives an isomorphism between $F[x]/(f(x))$ and $F(\alpha)$, which is a field. Thus $(f(x))$ is a maximal ideal, and $f(x)$ must be an irreducible polynomial. If $f(x)$ is not monic, say $f(x) = a_n x^n + \cdots + a_0$ where $a_n \in F$ is non-zero, then $p(x) = f(x)/a_n$ is a monic irreducible polynomial with $(f(x)) = (p(x))$. Note $p(\alpha) = \phi_\alpha(p(x)) = 0$. Uniqueness is left as an exercise. □

In the above situation, we call $p(x)$ the *minimal polynomial* of α over F. For example, the minimal polynomial of $\sqrt{-1}$ over $\mathbb{Q}$ is $p(x) = x^2 + 1$.

▶ **Let E be a field extension of F and $\alpha \in E$.**

(i) If α is algebraic with minimal polynomial $p(x)$, then $F(\alpha) \cong F[x]/(p(x))$.

(ii) If α is transcendental, then $F(\alpha) \cong \mathbf{Frac}(F[x])$.

Proof. (i) Suppose α is algebraic. Let $\phi_\alpha : F[x] \to F(\alpha)$ be the evaluation homomorphism. From the proof of the previous result, ϕ_α is onto and $\ker(\phi_\alpha) = (p(x))$ where $p(x)$ is the minimal polynomial of α. The 1st Isomorphism Theorem then proves (i).

(ii) Now suppose α is transcendental. Then ϕ_α has trivial kernel. Indeed, if $f(x) \in \ker(\phi_\alpha)$ then $f(\alpha) = 0$; and if $f(x)$ is a non-zero polynomial in $F[x]$ this would contradict the assumption that α is transcendental. Next, we can extend ϕ_α to a homomorphism

$$\psi : \mathrm{Frac}(F[x]) \longrightarrow F(\alpha)$$

by setting $\psi(f(x)/g(x)) = f(\alpha)/g(\alpha)$. This makes sense because $f(x)/g(x) \in \mathrm{Frac}(F[x])$ has $g(x)$ a non-zero polynomial, and $g(\alpha) \neq 0$ because α is transcendental. The map ψ is 1-1 because the domain is a field, and is onto because ϕ_α is onto. Thus ψ is an isomorphism. □

▶ **Let F be a field and $f(x) \in F[x]$ a non-constant polynomial. Then there is an extension E of F that contains some $\alpha \in E$ such that $f(\alpha) = 0$.**

Proof. If $f(x)$ is not irreducible, let $p(x)$ be an irreducible polynomial which divides $f(x)$. Then set $E = F[x]/(p(x))$. This is a field, and F naturally is included into it. The equivalence class of x serves as the element α. □

One of the most important tools in field theory is linear algebra. As you have already taken a linear algebra course, we only briefly review some of the basics.

Review of some linear algebra

A *vector space* over a field F is an abelian group V equipped with an operation

$$F \times V \longrightarrow V$$

written $(a, v) \longmapsto av$, called scalar multiplication, which satisfies for all $a, b \in F$ and $v, w \in V$:

$$\begin{aligned} a(bv) &= (ab)v \\ (a+b)v &= av + bv \\ a(v+w) &= av + aw \\ 1v &= v \end{aligned}$$

Elements of V are called vectors, and elements of F in this context are often called scalars. A subset $S \subset V$ is *linearly independent* if when $v_1, \ldots, v_m \in S$ satisfy

$$a_1 v_1 + \cdots + a_m v_m = 0$$

then we must have $a_1 = \cdots = a_m = 0$. Suppose S is a maximal linearly independent subset of V. This means that if $S \subset T$ and T is a linearly independent subset of V, then $S = T$. In this case S is called a *basis* for V, and the *dimension* of V is given by

$$\dim_F V = \#S = \text{ size of a maximal linearly independent subset}$$

If S is a finite set, then $\dim_F V$ is finite, and V is called *finite-dimensional*. Otherwise, V is *infinite-dimensional*. A linearly independent subset $S \subset V$ is a basis if and only if it spans V, i.e. any element of V can be written as a linear combination of elements in S.

Degrees of field extensions

Now let us return to our previous setup, where F is some field, and E is an extension field of F. Then E is a vector space over F: indeed, the scalar multiplication map $E \times F \longrightarrow F$ is just the multiplication of field elements, all of which may be viewed as inside E. We define

$$[E : F] = \dim_F E$$

and call this the *degree* of the field extension E of F. In the next lecture we will study the degrees of field extensions and their relation to algebraicity.