29 Extension Fields

While Kronecker's Theorem is powerful, it remains awkward to work explicitly with the language of factor rings. It is more common to speak of *extension fields.* We have already seen that

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

is a field containing $\mathbb{Q}$, so we call it an extension field of $\mathbb{Q}$.

This is an example of a *simple extension,* where we adjoin a single element to a given field and use the field operations to produce as many new elements as possible. We will define these properly in a moment, but first we introduce some terminology.

Definition 29.1. Suppose that $\mathbb{E}$ and $\mathbb{F}$ are fields.
We say that $\mathbb{E}$ is an *extension field* of $\mathbb{F}$ if and only if $\mathbb{F}$ is a subfield of $\mathbb{E}$.
It is common to refer to the *field extension* $\mathbb{E} : \mathbb{F}$. Thus $\mathbb{E} : \mathbb{F} \iff \mathbb{F} \leq \mathbb{E}$.
$\mathbb{E}$ is naturally a vector space[1] over $\mathbb{F}$: the *degree* of the extension is its dimension $[\mathbb{E} : \mathbb{F}] := \dim_{\mathbb{F}} \mathbb{E}$.
$\mathbb{E} : \mathbb{F}$ is a *finite extension* if $\mathbb{E}$ is a finite-dimensional vector space over $\mathbb{F}$: i.e. if $[\mathbb{E} : \mathbb{F}]$ is finite.

This is nothing more than a switch of focus: given $\mathbb{F} \leq \mathbb{E}$, which of the fields do we take as the reference point?

Examples

1. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ since $\{1, \sqrt{2}\}$ is a basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.
2. $\mathbb{C}$ is an extension field of $\mathbb{R}$ and $[\mathbb{C} : \mathbb{R}] = 2$, since $\{1, i\}$ forms a basis of $\mathbb{C}$ over $\mathbb{R}$.
3. $\mathbb{R}$ is an infinite-dimensional vector space over $\mathbb{Q}$ so we write $[\mathbb{R} : \mathbb{Q}] = \infty$. More properly, $[\mathbb{R} : \mathbb{Q}]$ should be an infinite cardinal, but for our purposes it is not worth distinguishing these.
4. Any field $\mathbb{F}$ is an extension of itself, since any field is a subfield of itself. Clearly $[\mathbb{F} : \mathbb{F}] = 1$ and, moreover $[\mathbb{E} : \mathbb{F}] = 1 \iff \mathbb{E} = \mathbb{F}$.

We can now rephrase Kronecker's Theorem.

Theorem 29.2 (Kronecker, mk II)**.** *If $\mathbb{F}$ is a field and $f \in \mathbb{F}[x]$ a non-constant polynomial, then there exists an extension field $\mathbb{E}$ of $\mathbb{F}$ containing a zero of f.*

There is a subtle difference between this statement and the original, where $\mathbb{E}$ was constructed as a quotient ring containing an *isomorphic copy* of $\mathbb{F}$. See the first example below in order to appreciate the triviality of this distinction.[2]

[1] See later for a review of this and the relevant theorems, in particular if you've forgotten the meaning of terms such as *linear independence* and *basis.* The basic idea is that multiplication of elements in $\mathbb{E}$ by those in $\mathbb{F}$ behaves as *scalar multiplication.*

[2] More generally, you should now be comfortable enough with abstract algebra to be willing to engage in this abuse of language: if $\mathbb{E}$ contains a subfield isomorphic to $\mathbb{F}$, it is typical to simply say that $\mathbb{F}$ is a subfield of $\mathbb{E}$. Emphasizing the distinction is usually considered pedantic.

Example $f(x) = x^2 - 2$ is irreducible over $\mathbb{Q}$. Thus f has a zero $\alpha := x + \langle x^2 - 2 \rangle$ in the extension field

$$\mathbb{E} := \mathbb{Q}[x] \Big/ \langle x^2 - 2 \rangle$$

Indeed, $f(\alpha) = x^2 - 2 + \langle x^2 - 2 \rangle = \langle x^2 - 2 \rangle = 0_{\mathbb{E}}$. We of course are imagining α here as being $\sqrt{2}$ in disguise. Indeed, if $g(x) \in \mathbb{Q}[x]$, then the division algorithm says that there exist unique $q, r \in \mathbb{Q}[x]$ such that

$$g(x) = (x^2 - 2)q(x) + r(x), \quad \deg(r) \leq 1$$

There is therefore a unique $\deg \leq 1$ representative in each coset, whence we can write

$$\mathbb{E} = \{a + bx + \langle x^2 - 2 \rangle : a, b \in \mathbb{Q}\}$$

It should be clear that the field $\mathbb{E}$ is a vector space over $\mathbb{Q}$ with basis

$$\{1_{\mathbb{E}}, \alpha\} = \{1 + \langle x^2 - 2 \rangle, x + \langle x^2 - 2 \rangle\}$$

In this language, we may write

$$\mathbb{E} = \{a + b\alpha : a, b \in \mathbb{Q},\ \alpha^2 = 2\}$$

which, much more explicitly, has $\mathbb{Q}$ as a subfield. The point, of course, is that we are viewing $\mathbb{E} : \mathbb{Q}$ as the simple extension $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ in disguise.

Simple extensions

Suppose $\mathbb{E} : \mathbb{F}$ is a field extension and let $\alpha \in \mathbb{E}$. Our goal is construct a new field $\mathbb{F}(\alpha)$ satisfying:

- $\mathbb{F} \leq \mathbb{F}(\alpha) \leq \mathbb{E}$
- $\alpha \in \mathbb{F}(\alpha)$
- $\mathbb{F}(\alpha)$ is the *smallest* field with the above two properties.

Any such field must contain all polynomial expressions in α with coefficients in $\mathbb{F}$: the set of such is naturally denoted $\mathbb{F}[\alpha]$. This is, in fact, the *image* of the evaluation homomorphism $\phi_\alpha : \mathbb{F}[x] \to \mathbb{E}$,

$$\mathbb{F}[\alpha] = \operatorname{Im} \phi_\alpha = \{a_0 + a_1\alpha + \cdots + a_n\alpha^n : a_i \in \mathbb{F},\ n \in \mathbb{N}_0\}$$

and is therefore a subring, indeed an integral subdomain, of the field $\mathbb{E}$. The required definition should now be clear.

Definition 29.3. Let $\mathbb{E} : \mathbb{F}$ be a field extension and $\alpha \in \mathbb{E}$. The *simple extension* $\mathbb{F}(\alpha)$ of $\mathbb{F}$ is the field of fractions

$$\mathbb{F}(\alpha) := \operatorname{Frac}(\mathbb{F}[\alpha]) \leq \mathbb{E}$$

More generally, a field extension $\mathbb{G} : \mathbb{F}$ is *simple* if there exists some $\alpha \in \mathbb{G}$ such that $\mathbb{G} = \mathbb{F}(\alpha)$.

By the Fundamental Homomorphism Theorem, identifying $\mathbb{F}[\alpha] = \operatorname{Im} \phi_\alpha$ amounts to finding $\ker \phi_\alpha$. This depends crucially on whether the element α is algebraic or transcendental. We update this language to our new setting:

Definition 29.4. Let $\mathbb{E}$ be an extension field of $\mathbb{F}$. An element $\alpha \in \mathbb{E}$ is *algebraic over* $\mathbb{F}$ if it is a zero of some polynomial $f \in \mathbb{F}[x]$. Otherwise, the element α is *transcendental over* $\mathbb{F}$.

Simple transcendental extensions

We deal with these first as they are (surprisingly) very easy. By definition, if $\alpha \in \mathbb{E}$ is transcendental over $\mathbb{F}$, the evaluation homomorphism has trivial kernel $\ker \phi_\alpha = \{0\}$, whence ϕ_α is *injective* and

$$\mathbb{F}[\alpha] = \operatorname{Im} \phi_\alpha \cong {\mathbb{F}[x]}\Big/_{\ker \phi_\alpha} \cong \mathbb{F}[x]$$

This is merely an integral domain, not a field. Indeed:

Theorem 29.5. *A simple transcendental extension $\mathbb{F} \leq \mathbb{F}(\alpha) \leq \mathbb{E}$ is the subfield of rational expressions in α:*

$$\mathbb{F}(\alpha) = \left\{ \frac{a_0 + a_1\alpha + \cdots + a_n\alpha^n}{b_0 + b_1\alpha + \cdots + b_m\alpha^m} : m, n \in \mathbb{N}_0,\ a_i, b_j \in \mathbb{F},\ b_i \text{ not all zero} \right\} \leq \mathbb{E}$$

This is an infinite-dimensional vector space over $\mathbb{F}$ and is naturally isomorphic to the field of rational fractions $\mathbb{F}(x) = \operatorname{Frac}(\mathbb{F}[x])$ in the indeterminate x. All simple transcendental extensions of a given field $\mathbb{F}$ are therefore isomorphic.

Example e and π are transcendental over $\mathbb{Q}$. The proofs of these facts are hard (π especially) and more difficult than merely showing their irrationality: look them up if you want a challenge…

Simple Algebraic Extensions and Minimal Polynomials

Suppose that $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$ and consider

$$\ker \phi_\alpha = \{f \in \mathbb{F}[x] : f(\alpha) = 0\}$$

Since α is algebraic, there exists at least one non-constant polynomial in $\ker \phi_\alpha$…

Theorem 29.6. *Let $\alpha \in \mathbb{E}$ be algebraic over $\mathbb{F}$. Then:*

1. *There exists a unique monic irreducible $m_{\alpha,\mathbb{F}} \in \mathbb{F}[x]$ such that $\ker \phi_\alpha = \langle m_{\alpha,\mathbb{F}} \rangle$.*
2. *If $\deg(m_{\alpha,\mathbb{F}}) = n$, then $[\mathbb{F}(\alpha) : \mathbb{F}] = n$ so that every simple algebraic extension is finite. Indeed the set $\{1, \alpha, \cdots, \alpha^{n-1}\}$ forms a basis of $\mathbb{F}(\alpha)$ over $\mathbb{F}$ so that*

$$\mathbb{F}(\alpha) = \mathbb{F}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{F}\}$$

Proof. 1. Every ideal in $\mathbb{F}[x]$ is principal; since $\ker \phi_\alpha$ is non-trivial, we see that $\ker \phi_\alpha = \langle m \rangle$ for some non-constant $m \in \mathbb{F}[x]$. Observe that

$$\langle m \rangle = \langle f \rangle \iff f \mid m \text{ and } m \mid f \iff m, f \text{ are associates}$$

We may thus divide m by its leading coefficient to obtain the unique *monic* generator $m_{\alpha,\mathbb{F}}$ of $\ker \phi_\alpha$. If $m_{\alpha,\mathbb{F}}$ were reducible, then some non-constant proper divisor would have α as a zero and thus lie in $\ker \phi_\alpha = \langle m_{\alpha,\mathbb{F}} \rangle$: a contradiction.

2. If $\{1, \alpha, \ldots, \alpha^{n-1}\}$ were linearly dependent, there would exist some non-zero $k \in \ker \phi_\alpha$ with $\deg(k) \leq n-1$. But this contradicts the fact that $n = \deg(m_{\alpha,\mathbb{F}})$ is the minimal degree for a non-zero polynomial in $\ker \phi_\alpha$.

   Now apply the division algorithm: given $f \in \mathbb{F}[x]$, there exist unique $q, r \in \mathbb{F}[x]$ for which

   $$f(x) = q(x)m_{\alpha,\mathbb{F}}(x) + r(x), \quad \deg(r) < n$$

   Clearly $f(\alpha) = r(\alpha)$ so that

   $$\mathbb{F}[\alpha] = \operatorname{Im} \phi_\alpha = \{r(\alpha) : r \in \mathbb{F}[x], \deg(r) < n\}$$

   It follows that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a spanning set and thus a basis of $\mathbb{F}[\alpha]$.

   Finally, the irreducibility of $m_{\alpha,\mathbb{F}}$ means that $\ker \phi_\alpha = \langle m_{\alpha,\mathbb{F}} \rangle$ is a maximal ideal, whence

   $$\mathbb{F}[\alpha] \cong \mathbb{F}[x] \Big/ \langle m_{\alpha,\mathbb{F}} \rangle$$

   is a *field* and thus equals its field of fractions. ∎

Definition 29.7. We call $m_{\alpha,\mathbb{F}} \in \mathbb{F}[x]$ the *minimal polynomial* of α over $\mathbb{F}$ since it is the unique monic polynomial of *least degree* for which α is a zero. The *degree of α over* $\mathbb{F}$ is the degree of its minimal polynomial:

$$\deg_{\mathbb{F}}(\alpha) := \deg(m_{\alpha,\mathbb{F}}) = [\mathbb{F}(\alpha) : \mathbb{F}]$$

The subscripts are often omitted unless one needs to stress the element or field.

Examples

1. $\sqrt{2}$ is algebraic over $\mathbb{Q}$ with minimal polynomial $m = x^2 - 2 \in \mathbb{Q}[x]$, whence $\deg_{\mathbb{Q}}(\sqrt{2}) = 2$.

   $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a simple extension of $\mathbb{Q}$ with degree $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

   We could of course work over $\mathbb{R}$, though it is somewhat silly: $\sqrt{2}$ has minimal polynomial $m_{\sqrt{2},\mathbb{R}} = x - \sqrt{2}$ and $\deg_{\mathbb{R}}(\sqrt{2}) = 1$. Indeed $\mathbb{R}(\sqrt{2}) = \mathbb{R}$, so that $[\mathbb{R}(\sqrt{2}) : \mathbb{R}] = 1$.

2. Repeat the same exercise with $\sqrt[3]{2}$ over $\mathbb{Q}$. Certainly this is a zero of $x^3 - 2 \in \mathbb{Q}[x]$: we claim this is the minimal polynomial m. Indeed,

   - If $\deg(m) = 1$, then $\sqrt[3]{2} \in \mathbb{Q}$.
   - If $\deg(m) = 2$, then $x^3 - 2 \in \ker \phi_{\sqrt[3]{2}} = \langle m \rangle$ would have even degree.

   Both statements are false, whence $\sqrt[3]{2}$ has minimal polynomial $m = x^3 - 2$ over $\mathbb{Q}$ and we have a simple extension

   $$\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}] = \{a + 2^{1/3}b + 2^{2/3}c : a, b, c \in \mathbb{Q}\}$$

   of degree $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

3. The only irreducible quadratic polynomial over the field $\mathbb{Z}_2$ is $f(x) = x^2 + x + 1$. It follows that f has a zero $\alpha = x + \langle x^2 + x + 1 \rangle$ in the extension field

$$\mathbb{F}_4 := \mathbb{Z}_2[x] \Big/ \langle x^2 + x + 1 \rangle$$

The minimal polynomial of α is clearly $m = x^2 + x + 1$, whence $[\mathbb{F}_4 : \mathbb{Z}_2] = 2$ and we can write

$$\mathbb{F}_4 = \{a + b\alpha : a, b \in \mathbb{Z}_2\}$$

We have therefore produced a field with *four* elements, which we may label $0, 1, \alpha, 1 + \alpha$. The addition/multiplication tables are below:

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

where, for example, we compute

$$\alpha(1 + \alpha) = \alpha + \alpha^2 = \alpha - \alpha - 1 = 1$$

using the minimal polynomial for α.
Observe that $(\mathbb{F}_4, +) \cong V$ (the Klein 4-group), while $(\mathbb{F}_4 \setminus \{0\}, \cdot) \cong C_3$ is cyclic. Indeed the first observation shows that $2 \cdot x = 0$ for all $x \in \mathbb{F}_4$, whence $\mathbb{F}_4$ has characteristic 2.

More generally, if $f \in \mathbb{Z}_p[x]$ is irreducible of degree n, then we may construct the finite field $\mathbb{F}_{p^n} = \mathbb{Z}_p[x] \Big/ \langle f(x) \rangle$ with p^n elements and degree $[\mathbb{F}_{p^n} : \mathbb{Z}_p] = p^{n-1}$.

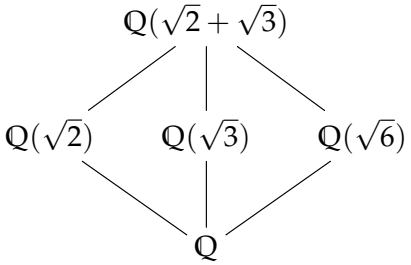
4. $\alpha = \sqrt{2} + \sqrt{3}$ is algebraic over $\mathbb{Q}$: we compute

$$(\alpha - \sqrt{2})^2 = 3 \implies \alpha^2 - 2\sqrt{2}\alpha + 2 = 3 \implies 8\alpha^2 = (1 - \alpha^2)^2$$

whence α is a zero of the polynomial $m = x^4 - 10x^2 + 1$. This is irreducible (exercise!) and is therefore the minimal polynomial of α, whence $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. The standard basis $\{1, \alpha, \alpha^2, \alpha^3\}$ is awkward. Observe that

$$\alpha^2 = 5 + 2\sqrt{6}, \qquad \alpha^3 = 11\sqrt{2} + 9\sqrt{3}$$

from which we see that a simpler basis is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Indeed this shows that the simple extensions $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$ are *intermediate fields* for the extension $\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}$. We can even draw the *subfield diagram* on the right.



The observation that this subfield diagram is similar to the subgroup diagram for the Klein 4-group is central to *Galois Theory.*

5. The real number $\alpha = \sqrt{2+\sqrt[3]{2}}$ satisfies

$$\alpha^2 - 2 = \sqrt[3]{2} \implies (\alpha^2-2)^3 = 2 \implies \alpha^6 - 6\alpha^4 + 12\alpha^2 - 10 = 0$$

The polynomial $x^6 - 6x^4 + 12x^2 - 10 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 2$, whence this is the minimal polynomial of α and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$.

Aside 1: Finding inverses in a simple algebraic extension

There are two standard approaches to this.

Brute Force/Linear Algebra Suppose $[\mathbb{F}(\alpha) : \mathbb{F}] = n$. Given $b_0 + \cdots + b_{n-1}\alpha^{n-1} \in \mathbb{F}(\alpha)$, compute

$$(b_0 + \cdots + b_{n-1}\alpha^{n-1})(c_0 + \cdots + c_{n-1}\alpha^{n-1}) = 1$$

Using $m_{\alpha,\mathbb{F}}$ to evaluate the left hand side as a polynomial in α of degree $< n$ and equating coefficients of α^k, we obtain a linear system of n equations in n unknowns $b_0, \ldots, b_{n-1}$. For example, in $\mathbb{Q}(\sqrt[3]{2})$,

$$(a + 2^{1/3}b + 2^{2/3}c)(d + 2^{1/3}e + 2^{2/3}f) = 1 \iff \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix} \begin{pmatrix} d \\ e \\ f \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

This can be solved via the usual linear algebra methods: for instance

$$(a + 2^{1/3}b + 2^{2/3}c)^{-1} = \frac{(2bc - a^2) + (ab - 2c^2)2^{1/3} + (ac - b^2)2^{2/3}}{6abc - a^3 - 2b^3 - 4c^3}$$

Euclidean Algorithm We state this without proof, though the abstract argument is no harder than in the integers: The Euclidean algorithm works perfectly in $\mathbb{F}[x]$! Let m be the minimal polynomial of α and suppose $r \in \mathbb{F}[x]$ has $0 \leq \deg(r) < \deg(m)$. Apply the division algorithm to divide m by r and repeat:

$$\begin{aligned} m &= q_1 r + r_1, && \deg(r_1) < \deg(r) \\ r &= q_2 r_1 + r_2, && \deg(r_2) < \deg(r_1) \\ r_1 &= q_3 r_2 + r_3, && \deg(r_3) < \deg(r_2) \\ &\vdots \end{aligned}$$

One may prove, exactly as with the integers, that the final non-zero remainder in the sequence $r, r_1, r_2, \ldots$ is a *greatest common divisor* of m and r: that is a polynomial d of maximal degree which divides both m and r. In our case, this is necessarily constant since m is irreducible. Now reverse the steps of the algorithm to see that there exist polynomials $\lambda, \mu \in \mathbb{F}[x]$ such that

$$\lambda(x)m(x) + \mu(x)r(x) = 1$$

It follows that $r(\alpha)^{-1} = \mu(\alpha)$ in $\mathbb{F}(\alpha)$.

Here is an example where we find the inverse of $x^2+3+\langle x^3-2\rangle$ in $\mathbb{Q}[x]\Big/_{\langle x^3-2\rangle}$.

Division Algorithm 1 $\quad x^3-2 = x(x^2+3)-3x-2$

Division Algorithm 2 $\quad x^2+3 = \left(\frac{1}{3}x-\frac{2}{9}\right)(3x+2)+\frac{31}{9}$

Reverse algorithm
$$\begin{aligned}\frac{31}{9} &= x^2+3-\left(\frac{1}{3}x-\frac{2}{9}\right)(3x+2)\\ &= x^2+3+\left(\frac{1}{3}x-\frac{2}{9}\right)\left(x^3-2-x(x^2+3)\right)\\ &= \left(\frac{1}{3}x-\frac{2}{9}\right)(x^3-2)+\left(-\frac{1}{3}x^2+\frac{2}{9}x+1\right)(x^2+3)\\ \implies 1 &= \frac{1}{31}(3x-2)(x^2-2)+\frac{1}{31}(-3x^2+2x+9)(x^2+3)\end{aligned}$$

It follows that $\left(x^2+3+\langle x^3-2\rangle\right)^{-1} = \frac{1}{31}(-3x^2+2x+9)+\langle x^3-2\rangle$, whence, with $\alpha = \sqrt[3]{2}$, we obtain

$$(2^{2/3}+3)^{-1} = \frac{1}{31}(-3\cdot 2^{2/3}+2\cdot 2^{1/3}+9) \in \mathbb{Q}(\sqrt[3]{2})$$

exactly as we'd find using the linear algebra method.

The methods are roughly equivalent: the steps of the Euclidean algorithm are similar to elementary row operations applied to the matrix system; reversing the algorithm is akin to back-substitution. Both methods become significantly slower as the degree of the minimal polynomial increases.

Aside 2: A Primer on Vector Spaces

Definition 29.8. A *vector space* V over a field $\mathbb{F}$ is a set V together with two operations *addition* and *scalar multiplication.* These satisfy the axioms:

1. $(V,+)$ is an abelian group.
2. $\mathbb{F}$ acts on V by scalar multiplication: that is, $\forall \lambda,\mu\in\mathbb{F},\ v,w\in V$,
   - $\lambda v \in V$
   - $\lambda(\mu v) = (\lambda\mu)v$
   - $1v = v$
   - $(\lambda+\mu)v = \lambda v+\mu v$
   - $\lambda(v+w) = \lambda v+\lambda w$

Moreover, a subset $W\leq V$ is a *subspace* of V if it is also a vector space over $\mathbb{F}$.

Examples $\mathbb{R}^n, \mathbb{C}^n$, etc., should be familiar. If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a vector space over $\mathbb{F}$. Most importantly, if $\mathbb{E}:\mathbb{F}$ is a field extension, then $\mathbb{E}$ is a vector space over $\mathbb{F}$: *think about this until it seems obvious!*

Remarks We *don't* denote vectors differently from scalars. This is in part because our main example is that of field extensions, where the base field $\mathbb{F}$ is a subspace of the extension field $\mathbb{E}$.
Following on from this, note that 0 is simultaneously a *scalar* ($0 \in \mathbb{F}$) and the *zero-vector* $0 \in V$.

Lemma 29.9. *1.* $\forall \lambda \in \mathbb{F},\ v \in V$ *we have* $0v = 0$, $\lambda 0 = 0$ *and* $(-\lambda)v = \lambda(-v) = -(\lambda v)$.

2. $W \leq V \iff 0 \in W$ *and* $\lambda_1 w_1 + \lambda_2 w_2 \in W$ *for all* $\lambda, \mu \in \mathbb{F},\ w_1, w_2 \in W$.

We omit the proofs, which should be familiar.

Definition 29.10. Let V be a vector space over $\mathbb{F}$. A *linear combination* is a *finite sum*

$$\lambda_1 v_1 + \cdots + \lambda_n v_n \text{ where } \lambda_i \in \mathbb{F} \text{ and } v_1, \ldots, v_n \in V$$

Let $S \subseteq V$. The *span* of S is the set of all linear combinations of vectors in S

$$\operatorname{Span} S = \{\lambda_1 v_1 + \cdots + \lambda_n v_n : n \in \mathbb{N},\ \lambda_i \in \mathbb{F}, v_i \in S\}$$

The set S is *linearly dependent* if

$$\exists n \in \mathbb{N},\ v_i \in S,\ \lambda_i \in \mathbb{F} \text{ not all zero, such that } \lambda_1 v_1 + \cdots + \lambda_n v_n = 0$$

We call such an equation a *linear dependence.* The set S is *linearly independent* otherwise:

$$\forall n \in \mathbb{N},\ v_i \in S,\ \lambda_1 v_1 + \cdots + \lambda_n v_n = 0 \implies \forall i,\ \lambda_i = 0$$

Lemma 29.11. *Let S be a linearly independent subset of V and let $v \in V$. Then*

$$S \cup \{v\} \text{ is linearly independent} \iff v \notin \operatorname{Span} S$$

Proof. We prove the contrapositive:

$$\begin{aligned} v \in \operatorname{Span} S &\iff \exists \lambda_i \in \mathbb{F},\ v_i \in S \text{ such that } v = \lambda_1 v_1 + \cdots + \lambda_n v_n \\ &\iff v - \lambda_1 v_1 - \cdots - \lambda_n v_n = 0 \qquad (*) \end{aligned}$$

Since the coefficient in front of v is non-zero, this says that $S \cup \{v\}$ is linearly dependent.
Conversely, if one has a linear dependence on the set $S \cup \{v\}$, one may assume the coefficient of v is non-zero, else S would be linearly dependent. Divide out by the coefficient of v to obtain $(*)$. ∎

The Lemma says that we can keep making a linearly independent set larger, provided there exists an element not in its span. This is the rough idea behind…

Definition 29.12. A set S is a *basis of V over* $\mathbb{F}$ if it is a maximal linearly independent subset of V: i.e., for which $\operatorname{Span} S = V$.

Theorem 29.13. *Every vector space has a basis, and all basis sets have the same cardinality.*

Definition 29.14. The *dimension* of a vector space is the cardinality of any (and all) basis sets.

You should see a complete discussion of this topic in an upper-division linear algebra course.

31 Algebraic Extensions

Our goal consider to what extent simple algebraic extensions are sufficient to construct all algebraic extensions. We begin with a critically important result for working with multiple extensions. This result is very similar to that for indices of multiple subgroups, and the proof should seem familiar.

Theorem 31.1 (Tower Law)**.** *If* $\mathbb{E} : \mathbb{F}$ *and* $\mathbb{K} : \mathbb{E}$ *are field extensions, then* $\mathbb{K} : \mathbb{F}$ *is a field extension, and*

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}] \tag{$*$}$$

Moreover, $\mathbb{K} : \mathbb{F}$ *is a finite extension if and only if* $\mathbb{E} : \mathbb{F}$ *and* $\mathbb{K} : \mathbb{E}$ *are.*

Proof. Let $\mathcal{E}_{\mathbb{F}}$ be a basis of $\mathbb{E}$ over $\mathbb{F}$ and $\mathcal{K}_{\mathbb{E}}$ a basis of $\mathbb{K}$ over $\mathbb{E}$. Define

$$\mathcal{B}_{\mathbb{F}} := \{\alpha\beta : \alpha \in \mathcal{E}_{\mathbb{F}}, \beta \in \mathcal{K}_{\mathbb{E}}\}$$

We claim that this is a basis of $\mathbb{K}$ over $\mathbb{F}$.

Linear Independence Suppose that I, J are *finite* indexing sets, that $\alpha_i \in \mathcal{E}_{\mathbb{F}}$, $\beta_j \in \mathcal{K}_{\mathbb{E}}$ and that $f_{ij} \in \mathbb{F}$ are scalars for which

$$\sum_{i\in I}\sum_{j\in J} f_{ij}\alpha_i\beta_j = 0$$

Then

$$\begin{aligned}
\sum_{j\in J}\left(\sum_{i\in I} f_{ij}\alpha_i\right)\beta_j = 0 &\implies \forall j \in J,\ \sum_{i\in I} f_{ij}\alpha_i = 0 && \text{(linear independence of } \mathcal{K}_{\mathbb{E}}\text{)}\\
&\implies \forall j \in J,\ i \in I,\ f_{ij} = 0 && \text{(linear independence of } \mathcal{E}_{\mathbb{F}}\text{)}
\end{aligned}$$

Spanning Set Since $\mathcal{K}_{\mathbb{E}}$ is a basis, every element $x \in \mathbb{K}$ may be written (uniquely) as a finite sum

$$x = \sum_{j\in J} e_j\beta_j \qquad \text{(each } e_j \in \mathbb{E} \text{ and } J \text{ is a finite indexing set)}$$

But each $e_j \in \mathbb{E}$ may be written uniquely as

$$e_j = \sum_{i\in I_j} f_{ij}\alpha_i \qquad \text{(each } f_i \in \mathbb{F} \text{ and } I_j \text{ is a finite indexing set)}$$

Let $I = \bigcup_{j\in J} I_j$ and letting some f_{ij} be zero if necessary, we see that

$$x = \sum_{j\in J}\sum_{i\in I} f_{ij}\alpha_i\beta_j \in \operatorname{Span}\mathcal{B}_{\mathbb{F}}$$

Finally, it should be clear that $\mu : \mathcal{E}_{\mathbb{F}} \times \mathcal{K}_{\mathbb{E}} \to \mathcal{B}_{\mathbb{F}} : (\alpha, \beta) \to \alpha\beta$ is a bijection. ∎

Corollary 31.2. *By induction, if* $(\mathbb{F}_i)_{i=1}^n$ *is a 'tower' of fields (i.e.* $\forall i,\ \mathbb{F}_{i+1} \geq \mathbb{F}_i$*), then*

$$[\mathbb{F}_n : \mathbb{F}_1] = [\mathbb{F}_n : \mathbb{F}_{n-1}] \cdots [\mathbb{F}_2 : \mathbb{F}_1]$$

To obtain examples of multiple extension fields, we extend our notation for simple extensions.

Definition 31.3. Suppose $\mathbb{E} : \mathbb{F}$ and $\alpha_1, \ldots, \alpha_n \in \mathbb{E}$. We define the extension field

$$\mathbb{F}(\alpha_1, \ldots, \alpha_n)$$

to be the smallest subfield (intersection of all subfields) of $\mathbb{E}$ containing $\mathbb{F}$ and the elements $\alpha_1, \ldots, \alpha_n$. By the definition of simple extension, this can be formed as a sequence of simple extensions:

$$\mathbb{F}(\alpha_1, \alpha_2) = \big(\mathbb{F}(\alpha_1)\big)(\alpha_2), \quad \text{etc.},$$

where the order of extension is irrelevant.

Example Consider $\mathbb{Q}(\sqrt{2}, i) = \big(\mathbb{Q}(\sqrt{2})\big)(i)$. Then $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$. The minimal polynomials in each case are

$$m_{\sqrt{2},\mathbb{Q}} = x^2 - 2, \qquad m_{i,\mathbb{Q}(\sqrt{2})} = x^2 + 1$$

It follows that $\{1, \sqrt{2}\}$ is a basis of $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ and $\{1, i\}$ is a basis of $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})$. But then

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$$

and moreover, $\{1, \sqrt{2}, i, \sqrt{2}i\}$ is a basis of $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$. We'll return to this example in a moment.

Definition 31.4. An field extension $\mathbb{E} : \mathbb{F}$ is *algebraic* if every element of $\mathbb{E}$ is algebraic over $\mathbb{F}$.

Theorem 31.5. *Let $\mathbb{E} : \mathbb{F}$ be a finite extension (includes every simple algebraic extension). Then:*

1. *$\mathbb{E} : \mathbb{F}$ is algebraic.*
2. *If $\beta \in \mathbb{E}$, then $\deg_{\mathbb{F}}(\beta)$ divides $[\mathbb{E} : \mathbb{F}]$.*

Proof. Let $[\mathbb{E} : \mathbb{F}] = n$ be finite and let $\beta \in \mathbb{E}$. Then the simple extension $\mathbb{F}(\beta)$ is a subfield of $\mathbb{E}$, whence

$$[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{F}(\beta)][\mathbb{F}(\beta) : \mathbb{F}]$$

In particular, $\mathbb{F}(\beta)$ is a finite extension of $\mathbb{F}$. Theorem 29.5 says that β cannot be transcendental over $\mathbb{F}$, whence it must be algebraic. Moreover,[3] $\deg_{\mathbb{F}}(\beta) = [\mathbb{F}(\beta) : \mathbb{F}]$ divides n. ∎

[3]It is worth seeing a more constructive elementary partial argument which only shows that $\deg_{\mathbb{F}}(\beta) \leq n$. Since $\beta \in \mathbb{E}$ and $[\mathbb{E} : \mathbb{F}]$ has dimension n, the cardinality-$(n+1)$ set

$$\{1, \beta, \ldots, \beta^n\} \subseteq \mathbb{F}(\beta)$$

is linearly dependent over $\mathbb{F}$, whence $\exists b_i \in \mathbb{F}$ not all zero for which $b_0 + b_1\beta + \cdots + b_n\beta^n = 0$. Otherwise said,

$$f(x) := b_0 + b_1 x + \cdots + b_n x^n \in \mathbb{F}[x]$$

is a non-zero polynomial with β as a zero, whence β is algebraic over $\mathbb{F}$. Moreover, $f \in \left\langle m_{\beta,\mathbb{F}} \right\rangle$, whence

$$\deg_{\mathbb{F}}(\beta) = \deg(m_{\beta,\mathbb{F}}) \leq \deg(f) \leq n = [\mathbb{E} : \mathbb{F}]$$

Examples

1. Let $\beta = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. By the Theorem, β is algebraic over $\mathbb{Q}$: we find its minimal polynomial.

   - Clearly $\beta \in \mathbb{Q} \iff b = 0 \iff \deg_{\mathbb{Q}}(\beta) = 1$. In this case $m_\beta = x - \beta$.
   - Observe that

     $$(\beta - a)^2 = 2b^2 \implies \beta^2 - 2a\beta + a^2 - 2b^2 = 0$$

     Thus $m_\beta = x^2 - 2ax + a^2 - 2b^2$ is the minimal polynomial[4] of β over $\mathbb{Q}$.

2. Every element $\beta \in \mathbb{Q}(\sqrt{2}, i)$ is algebraic over $\mathbb{Q}$ and, moreover, $\deg_{\mathbb{Q}}(\beta)$ must divide 4. For example,

   $$\begin{aligned} \beta = \sqrt{2} - 3i &\implies -9 = (\beta - \sqrt{2})^2 = \beta^2 - 2\sqrt{2}\beta + 2 \\ &\implies (2\sqrt{2}\beta)^2 = (\beta^2 - 2)^2 \implies 8\beta^2 = \beta^4 - 4\beta^2 + 4 \qquad (*) \\ &\implies \beta^4 - 12\beta^2 + 4 = 0 \end{aligned}$$

   It can be checked that $m_{\beta,\mathbb{Q}} = x^4 - 12x^2 + 4$ is irreducible over $\mathbb{Q}$ (e.g. consider it modulo 3).

   Now consider finding the degree of any $\beta \in \mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$. There are three cases:

   - $\deg_{\mathbb{Q}}(\beta) = 1 \iff \beta \in \mathbb{Q}$ whence $m_\beta = x - \beta$.
   - If $\beta \in \mathbb{Q}(\sqrt{2}) \setminus \mathbb{Q}$ then $\deg_{\mathbb{Q}}(\beta) = 2$ as seen in the previous example. More generally, write $\beta = \xi + i\eta$ where $\xi, \eta \in \mathbb{Q}(\sqrt{2})$ and $\eta \neq 0$. We see if β can be made to satisfy a quadratic polynomial:

     $$\begin{aligned} \beta^2 + p\beta + q = 0 &\iff (\xi^2 - \eta^2 + p\xi + q) + i(2\xi + p)\eta = 0 \\ &\iff p = -2\xi,\ q = \eta^2 + \xi^2 \end{aligned}$$

     For this polynomial to have rational coefficients, we require $\xi \in \mathbb{Q}$ and $\eta^2 \in \mathbb{Q}$. Putting it all together, we see that

     $$\deg_{\mathbb{Q}}(\beta) = 2 \iff \beta = a + b\sqrt{2},\ a + bi, \text{ or } a + b\sqrt{2}i$$

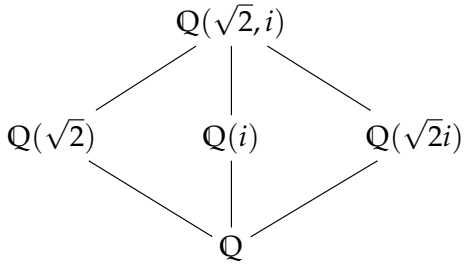
     where $a, b \in \mathbb{Q}$ and $b \neq 0$. The minimal polynomial can be found by computing $(\beta - a)^2 \ldots$
   - $\deg_{\mathbb{Q}}(\beta) = 4$ otherwise. In this case β has minimal polynomial

     $$m_{\beta,\mathbb{Q}(\sqrt{2})} = x^2 - 2\xi x + \eta^2 + \xi^2 \quad \text{over } \mathbb{Q}(\sqrt{2})$$

     All $\sqrt{2}$ terms can be taken to one side as in $(*)$ before squaring both sides to obtain a degree 4 monic polynomial over $\mathbb{Q}$: this will be $m_{\beta,\mathbb{Q}}$.

[4] We needn't check explicitly that this is irreducible, though you should do so: Theorem 31.5 guarantees that m_β exists and has degree 2, while Theorem 29.6 shows that this is the *only* degree 2 monic polynomial for which β is a zero.

We can summarize this using a subfield diagram:



where every extension has degree 2. By the above analysis, the three simple extensions $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2}i)$ are the *only* intermediate fields of the extension $\mathbb{Q}(\sqrt{2},i):\mathbb{Q}$.

As a final observation, note that if $\beta=\sqrt{2}+i$, then $\sqrt{2}=\frac{\beta^2+3}{2\beta}$ and $i=\frac{\beta^2-3}{2\beta}$, whence $\mathbb{Q}(\sqrt{2},i)$ is in fact a simple extension $\mathbb{Q}(\sqrt{2}+i)$!

3. Review our earlier discussions of the simple extension $\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}$ and check that everything is in accordance with the theorems. In particular, check, as we did above, that the only elements of $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ with degree 2 over $\mathbb{Q}$ are the irrationals in the intermediate fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, so that these really are the *only* intermediate fields of this extension.

4. Let $\alpha=\sqrt[3]{1+\sqrt{7}}$. Certainly

$$\alpha^3=1+\sqrt{7}\implies(\alpha^3-1)^2=7\implies\alpha^6-2\alpha^3-6=0$$

The polynomial x^6-2x^3-6 is irreducible over $\mathbb{Q}$ by Eisenstein with $p=2$: it is therefore the minimal polynomial of α, whence $[\mathbb{Q}(\alpha):\mathbb{Q}]=6$.
We also have the intermediate field $\mathbb{Q}(\sqrt{7})$, where

$$m_{\sqrt{7},\mathbb{Q}}=x^2-7,\qquad m_{\alpha,\mathbb{Q}(\sqrt{7})}=x^3-1-\sqrt{7}$$

corresponding to the tower

$$[\mathbb{Q}(\alpha):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{7})][\mathbb{Q}(\sqrt{7}):\mathbb{Q}]=3\cdot2$$

We therefore have bases $\{1,\sqrt{7}\}$ of $\mathbb{Q}(\sqrt{7})$ over $\mathbb{Q}$, and $\{1,\alpha,\alpha^2\}$ of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}(\sqrt{7})$. It follows that we have a basis

$$\left\{1,\sqrt{7},(1+\sqrt{7})^{1/3},\sqrt{7}(1+\sqrt{7})^{1/3},(1+\sqrt{7})^{2/3},\sqrt{7}(1+\sqrt{7})^{2/3}\right\}$$

of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

5. $\mathbb{Q}(\sqrt[3]{\pi^3+1})$ is a transcendental extension of $\mathbb{Q}$. If it were algebraic and $\alpha=\sqrt[3]{\pi^3+1}$, then $\pi^3=\alpha^3-1\in\mathbb{Q}(\alpha)$ lies in an algebraic extension of $\mathbb{Q}$ and so π^3 would be algebraic (be a zero of some polynomial) over $\mathbb{Q}$. But then π would be algebraic over $\mathbb{Q}$: contradiction.

Finite Algebraic Extensions

All examples of algebraic extensions that we've seen thusfar have been constructed using (a sequence of) simple algebraic extensions. This is, in fact, sufficient, to describe every *finite* algebraic extension.

Theorem 31.6. *Let* $\mathbb{E} : \mathbb{F}$ *be an algebraic extension. Then*

$$\mathbb{E} : \mathbb{F} \text{ is finite } \iff \exists \alpha_1, \ldots, \alpha_n \in \mathbb{E} \text{ such that } \mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$$

Proof. ($\Rightarrow$) Suppose $\mathbb{E} : \mathbb{F}$ is finite. Choose $\alpha_1 \in \mathbb{E} \setminus \mathbb{F}$. Then $\mathbb{F} \leq \mathbb{F}(\alpha_1) \leq \mathbb{E}$. If $\mathbb{F}(\alpha_1) = \mathbb{E}$, we're done. Otherwise repeat:

$$\alpha_2 \in \mathbb{E} \setminus \mathbb{F}(\alpha_1) \implies \mathbb{F} \leq \mathbb{F}(\alpha_1) \leq \mathbb{F}(\alpha_1, \alpha_2) \leq \mathbb{E}$$

This process must eventually terminate, since each intermediate extension has degree

$$[\mathbb{F}(\alpha_1, \ldots, \alpha_{i+1}), \mathbb{F}(\alpha_1, \ldots, \alpha_i)] \geq 2$$

and eventually $2^n > [\mathbb{E} : \mathbb{F}]$.

($\Leftarrow$) Let $\mathbb{F}_i = \mathbb{F}(\alpha_1, \ldots, \alpha_i)$ for each $i = 1, \ldots, n$, with $\mathbb{E} = \mathbb{F}_n$. By the tower law,

$$[\mathbb{E} : \mathbb{F}] = [\mathbb{F}_n : \mathbb{F}_{n-1}] \cdots [\mathbb{F}_2 : \mathbb{F}_1][\mathbb{F}_1 : \mathbb{F}]$$

Since $\mathbb{E}$ is algebraic, all α_i are algebraic over $\mathbb{F}$, whence the above is finite. ∎

It can be shown that every finite (algebraic) extension of $\mathbb{Q}$ is in fact simple: i.e. given $\mathbb{E} : \mathbb{Q}$ finite, $\exists \alpha \in \mathbb{E}$ (a 'primitive element') such that $\mathbb{E} = \mathbb{Q}(\alpha)$. These extensions are called *algebraic number fields,* and are of great importance to Number Theory. The same is true for finite extensions of finite fields. There certainly exist examples of finite extensions which are *not* simple, but exploring this would take us too far afield.

Infinite Algebraic Extensions

The gaping hole in our description of algebraic extensions is that we've seen no examples of *infinite degree* algebraic extensions. Examples of these typically require a little work.

Example For each $n \in \mathbb{N}_{\geq 2}$ define the finite algebraic extension $\mathbb{Q}_n := \mathbb{Q}(2^{1/2}, 2^{1/3}, 2^{1/4}, \ldots, 2^{1/n})$ of $\mathbb{Q}$. We'd somehow like to take the 'limit' of this process. Here is one possibility: define

$$\mathbb{E} := \bigcup_{n=1}^{\infty} \mathbb{Q}_n$$

We claim this is an infinite-dimensional algebraic field extension of $\mathbb{Q}$.

- $\mathbb{E}$ *a field?* Let $\alpha, \beta \in \mathbb{E}$, then $\alpha \in \mathbb{Q}_n$ and $\beta \in \mathbb{Q}_m$ for some m, n. WLOG $m \leq n$, whence α, β *lie in the same field* $\mathbb{Q}_n$. But then $\alpha \pm \beta$, $\alpha\beta$ and α^{-1} (if $\alpha \neq 0$) lie in $\mathbb{Q}_n$ and thus in $\mathbb{E}$.
- $\mathbb{E} : \mathbb{Q}$*?* This is clear since $\mathbb{Q} \leq \mathbb{Q}_1 \leq \mathbb{E}$.
- $\mathbb{E} : \mathbb{Q}$ *algebraic?* If $\alpha \in \mathbb{E}$, then $\alpha \in \mathbb{Q}_n$ for some n, whence α is algebraic over $\mathbb{F}$.
- $[\mathbb{E} : \mathbb{F}] = \infty$*?* If $[\mathbb{E} : \mathbb{F}] = m$ were finite, then every $\alpha \in \mathbb{E}$ would have $\deg_{\mathbb{Q}}(\alpha) \mid m$. The polynomial $x^{m+1} - 2$ is irreducible (Eisenstein with $p = 2$) and thus is the minimal polynomial of $2^{\frac{1}{m+1}} \in \mathbb{E}$. Contradiction.

This 'limit' process whereby we define $\mathbb{E}$ as the union of an infinite ascending chain of algebraic field extensions can be used to create other examples. We'll see another approach in a moment. Now that we have an example of an infinite algebraic extension, it is worth doing a little bookkeeping:

Lemma 31.7. *If $\mathbb{E} : \mathbb{F}$ and $\mathbb{F} : \mathbb{G}$ are algebraic, so is $\mathbb{E} : \mathbb{G}$.*

Proof. Suppose $\alpha \in \mathbb{E}$. Then $\sum_{k=1}^{n} f_k \alpha^k = 0$ for some $f_k \in \mathbb{F}$. It follows that α is algebraic over the finite algebraic extension $\mathbb{G}(f_1, \ldots, f_n)$ of $\mathbb{G}$. But then

$$[\mathbb{G}(\alpha, f_1, \ldots, f_n) : \mathbb{G}] = [\mathbb{G}(\alpha, f_1, \ldots, f_n) : \mathbb{G}(f_1, \ldots, f_n)][\mathbb{G}(f_1, \ldots, f_n) : \mathbb{G}]$$

is finite. Since $\mathbb{G}(\alpha) \leq \mathbb{G}(\alpha, f_1, \ldots, f_n)$, we see that $\mathbb{G}(\alpha) : \mathbb{G}$ is finite, whence α is algebraic over $\mathbb{G}$. ∎

Algebraic Closures

Our current practice of constructing algebraic extensions using repeated simple extensions has certain weaknesses. It *pre-supposes* the existence of an extension $\mathbb{E}$ in which each new element α already lives. For a particular finite extension, a repeated application of Kronecker's Theorem is sufficient to construct a suitable extension $\mathbb{E}$. Trying to do this for *all* (even finite) algebraic extensions simultaneously seems impossible.

Most of our examples have involved extensions of $\mathbb{Q}$, where there is an easy work-around: every algebraic extension of $\mathbb{Q}$ can be viewed as a subfield of $\mathbb{C}$! You have been using the critical result for years:

Theorem 31.8 (Fundamental Theorem of Algebra)**.** *Every non-constant $f \in \mathbb{C}[x]$ has a zero in $\mathbb{C}$. By the factor theorem, f splits over $\mathbb{C}$ (factors completely into linear factors).*

While there are algebraic proofs of this result (for instance using Galois Theory), most proofs depend heavily on analysis. We'll give two sketches later. We are more concerned with the immediate corollary: if $\mathbb{F} \leq \mathbb{C}$ and $f \in \mathbb{F}[x]$, then any zero of f may be viewed as a complex number. That is:

Corollary 31.9. *Every algebraic extension of a subfield of $\mathbb{C}$ is isomorphic to some subfield of $\mathbb{C}$.*

The complex numbers thus act as a *universe* within which all algebraic extensions of subfields can be assumed to exist. It would be nice if this sort of thing were possible in general:

> Given a general field $\mathbb{F}$, can we find some 'universal' algebraic extension $\overline{\mathbb{F}}$ such that *every* algebraic extension of $\mathbb{F}$ can be viewed as a subfield of $\overline{\mathbb{F}}$?

The answer is yes, but it will take us some time: we first need some terminology.

Definition 31.10.

1. A field $\mathbb{F}$ is *algebraically closed* if every non-constant $f \in \mathbb{F}[x]$ has a zero in $\mathbb{F}$. Equivalently, f splits over $\mathbb{F}$.
2. A field $\overline{\mathbb{F}}$ is an *algebraic closure of* $\mathbb{F}$ if
   (a) Every non-constant $f \in \mathbb{F}[x]$ splits over $\overline{\mathbb{F}}$.
   (b) $\overline{\mathbb{F}} : \mathbb{F}$ is an algebraic extension.

Remarks

- The Fundamental Theorem of Algebra states that $\mathbb{C}$ is *algebraically closed*. Certainly $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$.
- If $\mathbb{F}$ is algebraically closed then it is an algebraic closure of itself: $\overline{\mathbb{F}} = \mathbb{F}$.
- An algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$ can be viewed as containing precisely those elements which are algebraic over $\mathbb{F}$. More generally, if $\mathbb{E} : \mathbb{F}$ is an algebraic extension, then $\mathbb{E}$ is isomorphic to a subfield of $\overline{\mathbb{F}}$. We can therefore treat any given $\overline{\mathbb{F}}$ as a universal algebraic extension of $\mathbb{F}$: any algebraic $\mathbb{E} : \mathbb{F}$ can be viewed as a subfield of $\overline{\mathbb{F}}$.
- By the previous remark, an algebraic closure $\overline{\mathbb{F}}$ is unique up to isomorphism. It remains to show that such an extension exists!

Lemma 31.11. *If $\overline{\mathbb{F}}$ is an algebraic closure of $\mathbb{F}$, then $\overline{\mathbb{F}}$ is algebraically closed.*

Proof. Let α be algebraic over $\overline{\mathbb{F}}$ and consider an extension $\overline{\mathbb{F}}(\alpha)$. Then $\overline{\mathbb{F}}(\alpha) : \overline{\mathbb{F}}$ and $\overline{\mathbb{F}} : \mathbb{F}$ are algebraic, whence (Lemma 31.7) so is $\overline{\mathbb{F}}(\alpha) : \mathbb{F}$. But then α is algebraic over $\mathbb{F}$ and so $\alpha \in \overline{\mathbb{F}}$. ∎

Theorem 31.12. *If $\mathbb{K} : \mathbb{F}$ is an extension where $\mathbb{K}$ is algebraically closed, then we can define an algebraic closure of $\mathbb{F}$ via:*

$$\overline{\mathbb{F}} := \{x \in \mathbb{K} : x \text{ is algebraic over } \mathbb{F}\}$$

Proof. *$\overline{\mathbb{F}} : \mathbb{F}$ is an algebraic extension* Let $\alpha, \beta \in \overline{\mathbb{F}}$. Both α, β are algebraic, whence the field $\mathbb{F}(\alpha, \beta)$ is a finite, algebraic extension of $\mathbb{F}$, and a subfield of $\mathbb{K}$. Since $\alpha \pm \beta, \alpha\beta, \alpha^{-1}$ (if $\alpha \neq 0$) all lie in $\mathbb{F}(\alpha, \beta)$, all are algebraic over $\mathbb{F}$ and lie in $\mathbb{K}$. It follows that $\overline{\mathbb{F}}$ is a field, and an algebraic extension of $\mathbb{F}$.

Every non-constant $f \in \mathbb{F}[x]$ splits over $\overline{\mathbb{F}}$ Let $f \in \mathbb{F}[x]$ be non-constant. Since $\mathbb{F} \leq \mathbb{K}$ we see that $f \in \mathbb{K}[x]$, whence f splits over $\mathbb{K}$: write

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n), \qquad a \in \mathbb{F},\ \alpha_i \in \mathbb{K}$$

Certainly each α_i is algebraic over $\mathbb{F}$, whence $\alpha_i \in \overline{\mathbb{F}}$. ∎

Examples

1. The most well-known example of an algebraic closure is the set of *algebraic numbers*

   $$\overline{\mathbb{Q}} = \{x \in \mathbb{C} : x \text{ is algebraic over } \mathbb{Q}\}$$

   This is now seen to be a field. Indeed it is an *infinite degree algebraic extension of* $\mathbb{Q}$, which follows immediately from our example on page 13. Indeed it can be shown that $\overline{\mathbb{Q}}$ is a countable set, whence the degree is in fact $[\overline{\mathbb{Q}} : \mathbb{Q}] = \aleph_0$.

2. More generally, any algebraic extension of $\mathbb{Q}$ has the same algebraic closure: e.g. $\overline{\mathbb{Q}(\sqrt{2})} = \overline{\mathbb{Q}}$.

3. $\mathbb{R}$ has algebraic closure $\overline{\mathbb{R}} = \mathbb{C}$: this is a simple algebraic extension $\mathbb{C} = \mathbb{R}(i)$.

Existence of an Algebraic Closure: Zorn's Lemma and Maximal Ideals

As seen in Theorem 31.12, to show that a field $\mathbb{F}$ has an algebraic closure, it is enough to show that it has an algebraically closed extension $\mathbb{K}$. Showing that such exists is the last major goal in our discussion of field extensions.

There immediate difficulty involves producing a field which is large enough! It is impractical to consider applying Kronecker's Theorem infinitely many times: keeping track of the required identifications (cosets of cosets, etc.) would quickly become impossible. The standard way to get round issues like this is to appeal to a heavyweight piece of mathematics: Zorn's Lemma.

Before we can state this, and thence provide a sketch proof of our main result, we require some preliminaries.

Definition 31.13. A *partially ordered set* is a set $\mathcal{U}$ together with a binary relation $\leq$ which satisfies:

Reflexivity $\forall a \in \mathcal{U}, a \leq a$,

Anti-symmetry $\forall a, b \in \mathcal{U},\ a \leq b$ and $b \leq a \implies a = b$,

Transitivity $\forall a, b, c \in \mathcal{U},\ a \leq b$ and $b \leq c \implies a \leq c$.

A *chain* in $(\mathcal{U}, \leq)$ is a subset $\mathcal{C} \subseteq \mathcal{U}$ such that every pair $a, b \in \mathcal{C}$ is comparable: i.e.

$$\forall a, b \in \mathcal{C},\ a \leq b \text{ or } b \leq a$$

An element $c \in \mathcal{U}$ is an *upper-bound* for a chain $\mathcal{C}$ if $\forall a \in \mathcal{C}$ we have $a \leq c$.
An element $m \in \mathcal{U}$ is *maximal* if there are no elements $a \in \mathcal{U}$ for which $m < a$.

Example Consider the power set (set of subsets) of $\mathbb{R}$ partially ordered by $\subseteq$, and the chain

$$\mathcal{C} = \{A_1, A_2, A_3, \ldots\} \quad \text{where} \quad A_n = \left\{0, \frac{1}{2}, \frac{2}{3}, \ldots, \frac{n-1}{n}\right\}$$

Clearly $A_m \subseteq A_n \iff m \leq n$ so this is a chain. This chain is bounded above, for example, by the infinite set

$$C := \bigcup_{n \in \mathbb{N}} A_n = \left\{0, \frac{1}{2}, \frac{2}{3}, \ldots\right\}$$

Note the similarity with how we constructed the infinite algebraic extension on page 13. The following results will use the same trick.

Axiom (Zorn's Lemma)**.** *If every chain in a partially ordered set $\mathcal{U}$ has an upper bound in $\mathcal{U}$, then $\mathcal{U}$ has a maximal element.*

Zorn's Lemma is essentially an axiom of set theory, being equivalent to the famous Axiom of Choice. While strange sounding, the idea is very simple. You can imagine a chain as like a sequence of branches coming off a tree-trunk, except where there might be infinitely many branches in a chain and that chains can separate or recombine as one moves away from the trunk. If every sequence of branches is bounded, then at least one of these bounds will have no branches beyond it.

Theorem 31.14. *Every proper ideal of a ring with unity R is contained in some maximal ideal.*

Proof. Let N be a proper ideal of R and let $\mathcal{U}$ be the set of all proper ideals of R containing N. This is partially ordered by the subring relation. Suppose $\mathcal{C}$ is a chain in $\mathcal{U}$ and define

$$K := \bigcup_{I \in \mathcal{C}} I$$

We check that this is an upper bound for $\mathcal{C}$:

- Clearly $0 \in K$, since $0 \in I$ for all $I \in \mathcal{C}$.
- Let $a, b \in C$ and $r \in R$, then $\exists I, J \in C$ such that $a \in I$, $b \in J$. Since $\mathcal{C}$ is a chain, WLOG $I \leq J$. But then $a - b \in J$ and $ra, ar \in J$, whence all three expressions lie in K. Thus K is an ideal of R.
- If $1 \in K$, then $1 \in I$ for some $I \in \mathcal{C}$, whence $I = R$ is non-proper. Thus $1 \notin K$ and so K is a proper ideal of R.
- Since $N \subseteq I$ for all $I \in \mathcal{C}$ we have $N \subseteq K$.

By Zorn's Lemma, there exists a maximal $M \in \mathcal{U}$, necessarily a maximal ideal containing N. ∎

The same argument applied to the set $\mathcal{U}$ of linearly independent subsets of a vector space V shows that every vector space has a basis (the existence part of Theorem 29.13).

Theorem 31.15. *Every field $\mathbb{F}$ has an extension $\mathbb{K}$ which is algebraically closed and thus an algebraic closure*

$$\overline{\mathbb{F}} := \{x \in \mathbb{K} : x \text{ algebraic over } \mathbb{F}\}$$

Sketch Proof.

- Let $P = \{f \in \mathbb{F}[x] : f \text{ irreducible and monic}\}$. For each $f \in P$, let x_f be a separate indeterminate and define the polynomial ring over $\mathbb{F}$ with all these indeterminates

  $$\mathcal{F} := \mathbb{F}[x_f : f \in P]$$

- Let N be the ideal of $\mathcal{F}$ generated by the expressions $f(x_f)$. N is proper,[5] whence it is contained in a maximal ideal M.
- $\mathbb{F}_1 := \mathcal{F}/M$ is a field containing a zero $x_f + M$ of every non-constant polynomial over $\mathbb{F}$.
- Repeat the construction: $\mathbb{F} \leq \mathbb{F}_1 \leq \mathbb{F}_2 \leq \cdots$ where every polynomial over $\mathbb{F}_n$ has a zero in $\mathbb{F}_{n+1}$. Now define $\mathbb{K} := \bigcup_{n=1}^{\infty} \mathbb{F}_n$. We claim this is the required field:
- ($\mathbb{K}$ is an extension field of $\mathbb{F}$) This is identical to the example on page 13: given any $\alpha, \beta \in \mathbb{K}$, *both* lie in some $\mathbb{F}_n$ whence so do $\alpha \pm \beta$, etc. Moreover $\mathbb{F} \leq \mathbb{F}_1 \leq \mathbb{K}$.
- ($\mathbb{K}$ is algebraically closed) Let $f \in \mathbb{K}[x]$. Then every coefficient a_j of f lies in some $\mathbb{F}_{n_j}$, whence $f \in \mathbb{F}_m[x]$ where $m = \max\{n_j\}$. But then f has a zero $\alpha \in \mathbb{F}_{m+1} \leq \mathbb{K}$. ∎

The upshot of all this is that we can always assume that algebraic extensions of a field $\mathbb{F}$ have a common universe, just as we do when working with subfields of $\mathbb{C}$.

[5] The general element of N is $\lambda_1 f_1(x_{f_1}) + \cdots + \lambda_n f_n(x_{f_n})$ where each $\lambda_i \in \mathcal{F}$. If this equals 1, then the same is true in any extension field $\mathbb{E}$ of $\mathbb{F}$ containing a zero $\alpha_1, \ldots, \alpha_n$ of each f_k. Evaluate at $x_{f_k} = \alpha_k$ to see that $0_{\mathbb{E}} = 1_{\mathbb{E}}$: a contradiction. Thus $1 \notin N$ and N is proper.

Example The algebraic closure $\overline{\mathbb{Z}_2}$ of $\mathbb{Z}_2$ can be seen to be an infinite field (homework). Since it is an extension field of $\mathbb{Z}_2$, any element $x \in \overline{\mathbb{Z}_2}$ can be written as a finite linear combination

$$x = a_1 + \cdots + a_n$$

where $a_1, \ldots, a_n$ are linearly independent over $\mathbb{Z}_2$. But then

$$2 \cdot x = (2 \cdot 1)a_1 + \cdots + (2 \cdot 1)a_n = 0$$

Thus $\overline{\mathbb{Z}_2}$ is an infinite field of characteristic 2.

Aside: The Fundamental Theorem of Algebra

The fact that $\mathbb{C}$ is algebraically closed might be the Fundamental Theorem of Algebra, but its proofs tend to depend heavily on *analysis.* Here are two sketch proofs which depend on ideas from complex or multi-variable analysis.

Sketch Proof 1. Suppose $p \in \mathbb{C}[x]$ has no zero in $\mathbb{C}$. Since $|p(z)| \geq m > 0$ for some m, it follows that $\frac{1}{p(z)}$ is an analytic function on the entire complex plane which is bounded above by $\frac{1}{m}$. Liouville's theorem from complex analysis says that any such function is constant. ∎

Sketch Proof 2. Suppose $p(z) \in \mathbb{C}[x]$ has no zero, then $|p(z)|$ has a minimal value m and attains its minimum at some value $z = a$.
Write $p(z) = c_0 + c_k(z-a)^k + \cdots + c_n(z-a)^n$ as a polynomial centered at $z = a$, where $k \in \mathbb{N}$ is minimal such that $c_k \neq 0$. We evaluate $p(z)$ on a small circle radius r centered at $z = a$:

$$\begin{aligned}\left|p(a + re^{i\theta})\right|^2 &= (c_0 + c_k r^k e^{ik\theta} + \cdots)(\overline{c_0 + c_k r^k e^{ik\theta} + \cdots}) \\ &= |c_0|^2 + \left(c_0\overline{c_k}e^{-ik\theta} + \overline{c_0}c_k e^{ik\theta}\right) r^k + O(r^{k+1}) \\ &= m^2 + 2b\cos(\psi - k\theta)r^k + O(r^{k+1})\end{aligned}$$

where $c_0\overline{c_k} = be^{i\psi}$. Now choose $\theta = \frac{1}{k}(\pi - \psi)$ to obtain

$$\left|p(a + re^{i\theta})\right|^2 = m^2 - 2br^k + O(r^{k+1})$$

For small r we clearly have $\left|p(a + re^{i\theta})\right| < m$: contradiction. ∎