.1 Field extensions, I

Exercise .1.1. Prove that if $k \subseteq K$ is a field extension, then $\operatorname{char} k = \operatorname{char} K$. Prove that the category Fld has no initial object.

Solution. Let $\varphi : k \to K$ be a field extension. If $i : \mathbb{Z} \to k$ is the unique ring homomorphism, we have $\ker i = (\operatorname{char} k)$. Similarly, there is a unique ring homomorphism $i' : \mathbb{Z} \to K$ with $\ker i' = (\operatorname{char} K)$. Since i' is unique, we must have $i' = \varphi \circ i$. We find

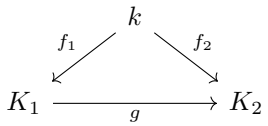
$$\ker(\varphi \circ i) = \{n \in \mathbb{Z} \mid \varphi(i(n)) = 0\}$$

but since φ is injective, $\varphi(i(n)) = 0$ if and only if $i(n) = 0$. That is, $\ker(\varphi \circ i) = \ker(i) = (\operatorname{char} k)$. Thus, we have $\operatorname{char} K = \operatorname{char} k$.

Now suppose Fld has an initial object I. That is, there is a unique homomorphism from I to every field k. But since field extensions preserve characteristic, I cannot exist (indeed, there are fields of characteristic 0 and p for all primes p). □

Exercise .1.2. Define carefully the category Fld_k of extensions of k.

Solution. The objects of Fld_k are pairs of fields and morphisms (K, f) such that $f : k \to K$ is a ring homomorphism. Morphisms in Fld_k are ring homomorphisms $g : K_1 \to K_2$ such that the diagram



commutes. Composition attains a natural definition. Certainly this defines a category as every object has an identity morphism, namely the identity homomorphism $id : K \to K$. Furthermore, associativity is easy to verify. Given morphisms $f : K_1 \to K_2$, $g : K_2 \to K_3$, and $h : K_3 \to K_4$, we find $h \circ (g \circ f) = (h \circ g) \circ f$ based on the associativity of ring homomorphisms. It is also trivial based on the commutativity of the corresponding diagram. □

Exercise .1.3. Let $k \subseteq F$ be a field extension, and let $\alpha \in F$. Prove that the field $k(\alpha)$ consists of all the elements of F which may be written as a rational function in α, with coefficients in k. Why does this *not* give (in general) an onto homomorphism $k(t) \to k(\alpha)$?

Solution. By definition, $k(\alpha)$ is a subfield of F, so every element of this field is an element of F. To have a field structure, it must include all linear combinations

of α and α^{-1} with coefficients in k. These are precisely the rational functions in α with coefficients in k.

If α is transcendental over k, then $[k(\alpha) : k]$ is infinite so by Proposition 1.3, $k(t) \cong k(\alpha)$. However, if α is algebraic, then $k(\alpha)$ is finite-dimensional as a vector space over k. Recall that any homomorphism $k(t) \to k(\alpha)$ is injective; in particular, $k(t)$ is a subfield of $k(\alpha)$. But the former is an infinite-dimensional vector space while the latter is not, so no such homomorphism can exist. In particular, there can be no onto homomorphism $k(t) \to k(\alpha)$. □

Exercise .1.4. Let $k \subseteq k(\alpha)$ be a simple extension, with α transcendental over k. Let E be a subfield of $k(\alpha)$ properly containing k. Prove that $k(\alpha)$ is a finite extension of E.

Solution. Suppose $k \subset E \subseteq k(\alpha)$ and let $\beta \in E \setminus k$. Then

$$\beta = \frac{f(\alpha)}{g(\alpha)}$$

for $f, g \in k[t]$. In particular, we have $f(\alpha) = \beta g(\alpha)$. Now define $p(t) \in E[t]$ to be $p = f - \beta g$. Then $p(\alpha) = 0$. Now it remains to show that $p \neq 0$ everywhere. Indeed, if $p(0) = f(0) - \beta g(0) = 0$, we would find $f(0) = \beta g(0)$, or $\beta = f(0)/g(0) \in k$, contradicting our choice of β. □

Exercise .1.5. (Cf. Example 1.4.)

- Prove that there is exactly one subfield of $\mathbb{R}$ isomorphic to $\mathbb{Q}[t]/(t^2 - 2)$.
- Prove that there are exactly three subfields of $\mathbb{C}$ isomorphic to $\mathbb{Q}[t]/(t^3 - 2)$.

From a 'topological' point of view, one of these copies of $\mathbb{Q}[t]/(t^3 - 2)$ looks very different from the other two: it is not dense in $\mathbb{C}$ but the others are.

Solution. Clearly $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(-\sqrt{2})$ are both subfields of $\mathbb{R}$ isomorphic to $\mathbb{Q}[t]/(t^2 - 2)$. It suffices to show that these subfields are equal. But since $-\sqrt{2} = -1 \cdot \sqrt{2}$ where $-1 \in \mathbb{R}$, we find that $\mathbb{Q}(-\sqrt{2})$ is contained in $\mathbb{Q}(\sqrt{2})$. The reverse inclusion follows similarly, so these two sets are in fact equal.

There are at most three subfields of $\mathbb{C}$ isomorphic to $\mathbb{Q}[t]/(t^3 - 2)$, namely $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\omega\sqrt[3]{2})$, and $\mathbb{Q}(\omega^2\sqrt[3]{2})$ where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Indeed, these are the three possible simple extensions of $\mathbb{Q}$ based on the minimal polynomial. Then we must show that none of these subfields of $\mathbb{C}$ are equal to one another. Clearly $\mathbb{Q}(\sqrt[3]{2})$ is not equal to the other two as it does not contain any element with a factor of i while the other two do. To see that the other two are not equal, suppose for the sake of contradiction that $\mathbb{Q}(\omega\sqrt[3]{2}) = \mathbb{Q}(\omega^2\sqrt[3]{2}) = K$. Consider the element

$$\frac{\omega^2\sqrt[3]{2}}{\omega\sqrt[3]{2}} = \omega \in K$$

which implies that $\omega\sqrt[3]{2}/\omega = \sqrt[3]{2} \in K$. That is, $Q(\sqrt[3]{2}) \subset K$, and this inclusion is proper as we saw above. Then

$$\begin{aligned} 3 &= [K : \mathbb{Q}] \\ &= [K : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \\ &= [K : \mathbb{Q}(\sqrt[3]{2})] \cdot 3 \end{aligned}$$

which implies that $K \cong \mathbb{Q}(\sqrt[3]{2})$, a contradiction. Thus, $\mathbb{Q}(\omega\sqrt[3]{2}) \neq \mathbb{Q}(\omega^2\sqrt[3]{2})$. □

Exercise .1.6. Let $k \subseteq F$ be a field extension, and let $f(x) \in k[x]$ be a polynomial. Prove that $\mathrm{Aut}_k(F)$ acts on the set of roots of $f(x)$ contained in F. Provide examples showing that this action need not be transitive or faithful.

Solution. Given an automorphism $\varphi \in \mathrm{Aut}_k(F)$ and a root α of $f(x)$, we define the action of φ on α to be $\varphi(\alpha)$. To verify that this is in fact an action, note that any field automorphism fixing k sends a root of f to another root of f, $\mathrm{id}_F(\alpha) = \alpha$ and $\varphi(\sigma(\alpha)) = \varphi \circ \sigma(\alpha)$.

From now on, let X denote the set of roots of f contained in F. Recall that an action is transitive if for all $x, y \in X$, there exists a $\varphi \in \mathrm{Aut}_k(F)$ such that $\varphi(x) = y$. Consider the extension $\mathbb{Q} \subseteq \mathbb{C}$ and the polynomial $x^3 - x^2 + x - 1$ which has the roots $\pm i$ and 1. Then there is no automorphism which sends $i \mapsto 1$ since elements of $\mathrm{Aut}_k(F)$ necessarily fix k.

An action is faithful if for all $\varphi \neq \sigma$, there exists an $x \in X$ such that $\varphi(x) \neq \sigma(x)$. Consider the trivial extension $\mathbb{C} \subseteq \mathbb{C}$ and the polynomial $x - 1 \in \mathbb{C}[x]$. Then all automorphisms of $\mathbb{C}$ (and there are distinct ones, namely the identity and the one mapping elements to their conjugate) necessarily send 1 to 1. □

Exercise .1.7. Let $k \subseteq F$ be a field extension, and let $\alpha \in F$ be algebraic over k.

- Suppose $p(x) \in k[x]$ is an irreducible monic polynomial such that $p(\alpha) = 0$; prove that $p(x)$ is the minimal polynomial of α over k, in the sense of Proposition 1.3.
- Let $f(x) \in k[x]$. Prove that $f(\alpha) = 0$ if and only if $p(x) \mid f(x)$.
- Show that the minimal polynomial of α is the minimal polynomial of a certain k-linear transformation, in the sense of Definition VI.6.12.

Solution. Since α is algebraic, $k \subseteq k(\alpha)$ is a finite degree extension. Then by Proposition 1.3, $k(\alpha) \cong k[t]/(q(t))$ for a unique monic irreducible nonconstant polynomial $q \in k[t]$ such that $q(\alpha) = 0$. Thus, $q = p$.

For the second point, suppose $f(\alpha) = 0$. In particular, f is in the kernel of the evaluation homomorphism from $k[x] \to F$, but this kernel is exactly $(p(x))$, so

$p(x) \mid f(x)$. Now suppose $p(x) \mid f(x)$ so $f(x) \in (p(x))$ which is the kernel of the evaluation homomorphism. Thus, $f(\alpha) = 0$.

I did not read VI.6.12 yet so I will not answer this for now. □

Exercise .1.8. Let $f(x) \in k[x]$ be a polynomial over a field k of degree d, and let $\alpha_1, \ldots, \alpha_d$ be the roots of $f(x)$ in an extension of k where the polynomial factors completely. For a subset $I \subseteq \{1, \ldots, d\}$, denote by α_I the sum $\sum_{i \in I} \alpha_i$. Assume that $\alpha_I \in k$ only for $I = \emptyset$ and $I = \{1, \ldots, d\}$. Prove that $f(x)$ is irreducible over k.

Solution. We prove the contrapositive. Suppose that $f(x)$ is reducible, say $f(x) = g(x) \cdot h(x)$ where $g, h \in k[x]$ and g is monic. Let

$$g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Let I_g denote the set of indices such that α_i is a root of g. Then we can express g as

$$g(x) = \prod_{i \in I_g} (x - \alpha_i) = x^n - (\alpha_1 + \alpha_2 + \cdots + \alpha_n)x^{n-1} + \cdots + (-1)^n(\alpha_1\alpha_2 \cdots \alpha_n).$$

Comparing coefficients of the term x^{n-1}, we find that

$$\alpha_1 + \alpha_2 + \cdots + \alpha_n = -a_{n-1}.$$

But $-\alpha_{n-1} \in k$, so $\alpha_{I_g} \in k$. □

Exercise .1.9. Let k be a finite field. Prove that the order of $|k|$ is a power of a prime integer.

Solution. Let p be the characteristic of the field; then p is prime. That is $\mathbb{F}_p \subseteq k$ is a field extension so k is a $\mathbb{F}_p$-vector space. In particular, $k \cong \mathbb{F}_p^n$ for some $n \geq 1$ so $|k| = p^n$. □

Exercise .1.10. Let k be a field. Prove that the ring of square $n \times n$ matrices $\mathcal{M}_n(k)$ contains an isomorphic copy of every extension of k of degree $\leq n$. (Hint: If $k \subseteq F$ is an extension of degree n and $\alpha \in F$, then 'multiplication by α' is a k-linear transformation of F.)

Solution. To do. □

Exercise .1.11. Let $k \subseteq F$ be a finite field extension, and let $p(x)$ be the characteristic polynomial of the k-linear transformation of F given by multiplication by α. Prove that $p(\alpha) = 0$.

This gives an effective way to find a polynomial satisfied by an element of an extension. Use it to find a polynomial satisfied by $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$, and compare this method with the one used in Example 1.19.

Solution. To do. □

Exercise .1.12. Let $k \subseteq F$ be a finite field extension, and let $\alpha \in F$. The *norm* of α, $N_{k\subseteq F}(\alpha)$, is the determinant of the linear transformation of F given by multiplication by α.

Prove that the norm is multiplicative: for $\alpha, \beta \in F$,

$$N_{k\subseteq F}(\alpha\beta) = N_{k\subseteq F}(\alpha)N_{k\subseteq F}(\beta).$$

Compute the norm of a complex number viewed as an element of the extension $\mathbb{R} \subseteq \mathbb{C}$ (and marvel at the excellent choice of terminology). Do the same for elements of an extension $\mathbb{Q}(\sqrt{d})$ of $\mathbb{Q}$, where d is an integer that is not a square, and compare the result with Exercise III.4.10.

Solution. To do. □

Exercise .1.13. Define the *trace* $\mathrm{tr}_{k\subseteq F}(\alpha)$ of an element α of a finite extension F of a field k by following the lead of Exercise 1.12. Prove that the trace is *additive*:

$$\mathrm{tr}_{k\subseteq F}(\alpha + \beta) = \mathrm{tr}_{k\subseteq F}(\alpha) + \mathrm{tr}_{k\subseteq F}(\beta)$$

for $\alpha, beta \in F$. Compute the trace of an element of an extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d})$, for d an integer that is not a square.

Solution. To do. □

Exercise .1.14. Let $k \subseteq k(\alpha)$ be a simple algebraic extension, and let $x^d + a_{d-1}x^{d-1} + \cdots + a_0$ be the minimal polynomial of α over k. Prove that

$$\mathrm{tr}_{k\subseteq k}(\alpha)(\alpha) = -a_{d-1} \quad \text{and} \quad N_{k\subseteq k(\alpha)}(\alpha) = (-1)^d a_0.$$

(Cf. Exercises 1.12 and 1.13.)

Solution. To do. □

Exercise .1.15. Let $k \subseteq F$ be a finite extension, and let $\alpha \in F$. Assume $[F : k(\alpha)] = r$. Prove that

$$\mathrm{tr}_{k\subseteq F}(\alpha) = r\,\mathrm{tr}_{k\subseteq k(\alpha)}(\alpha) \quad \text{and} \quad N_{k\subseteq F}(\alpha) = N_{k\subseteq k(\alpha)}(\alpha)^r.$$

(Cf. Exercises 1.12 and 1.13.)

Solution. To do. □

Exercise .1.16. Let $k \subseteq L \subseteq F$ be fields, and let $\alpha \in F$. If $k \subseteq k(\alpha)$ is a finite extension, then $L \subseteq L(\alpha)$ is finite and $[L(\alpha) : L] \leq [k(\alpha) : k]$.

Solution. If $k \subseteq k(\alpha)$ is finite, then it is algebraic. That is, there is some polynomial $p(x) \in k[x]$ such that $p(\alpha) = 0$. Since $k \subseteq L$, $p(x) \in L[x]$. Then, since $L \subseteq L(\alpha)$ is finitely generated and algebraic, the extension is finite. Furthermore, the degree of this extension is bounded by the degree of p (there is no guarantee that p is irreducible over L), so $[L(\alpha) : L] \leq [k(\alpha) : k]$. □

Exercise .1.17. Let $k \subseteq F = k(\alpha_1, \ldots, \alpha_n)$ be a finitely generated extension. Prove that the evaluation map

$$k[t_1, \ldots, t_n] \to F, \quad t_i \mapsto \alpha_i$$

is an epimorphism of rings (although it need not be onto).

Solution. To do. □

Exercise .1.18. Let R be a ring sandwiched between a field k and an algebraic extension F of k. Prove that R is a field.

Is it necessary to assume that the extension is algebraic?

Solution. Let $k \subseteq R \subseteq F$. First note that R is an integral domain since it is a subring of a field. Now let $r \in R$, which implies that $r \in F$. Since F is algebraic over k, there exists a polynomial $p(x) \in k[x]$ such that $p(r) = 0$, say $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ where each $a_i \in k$. Then we find

$$\begin{aligned} & r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0 \\ \implies & r(r^{n-1} + a_{n-1}r^{n-2} + \cdots + a_1) = -a_0 \\ \implies & -a_0^{-1}(r^{n-1} + a_{n-1}r^{n-2} + \cdots + a_1) = r^{-1} \in R \end{aligned}$$

so R is a field.

It is necessary for the extension to be algebraic. Consider the counterexample

$$k \subseteq k[x] \subseteq k(x)$$

where $k[x]$ is clearly not a field. □

Exercise .1.19. Let $k \subseteq F$ be a field extension of degree p, a prime integer. Prove that there are no subrings of F properly containing k and properly contained in F. (Use Exercise 1.18).

Solution. Since $k \subseteq F$ is a finite extension, it is algebraic. By Exercise 1.18, every intermediate ring R between k and F is a field. Then we find that $[F : k] = [F : R] \cdot [R : k]$, but since $[F : k] = p$ is prime, either $[F : R] = 1$, in which case R is not properly contained in F, or $[R : k] = 1$, in which case R does not properly contain k. □

Exercise .1.20. Let p be a prime integer, and let $\alpha = \sqrt[p]{2} \in \mathbb{R}$. Let $g(x) \in \mathbb{Q}[x]$ be any non-constant polynomial of degree $< p$. Prove that α may be expressed as a polynomial in $g(\alpha)$ with rational coefficients.

Prove that an analogous statement for $\sqrt[4]{2}$ is false.

Solution. First note that $x^p - 2$ is the minimal polynomial of α in $\mathbb{Q}$ (easily verified by rational roots test). Furthermore, $\mathbb{Q}(g(\alpha)) \subseteq \mathbb{Q}(\alpha)$ is an extension. Then we find

$$p = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(g(\alpha))] \cdot [\mathbb{Q}(g(\alpha)) : \mathbb{Q}].$$

The second factor cannot be 1 since this would imply that $g(\alpha) \in \mathbb{Q}$, which is impossible since $\deg(g) < p$ and α is algebraic of degree p. Thus, we must have $[\mathbb{Q}(\alpha) : \mathbb{Q}(g(\alpha))] = 1$ so the two fields are equal. In particular, $\alpha \in \mathbb{Q}(g(\alpha))$.

For a counterexample with $\alpha = \sqrt[4]{2}$, let $g(x) = x^2$. Then $g(\alpha) = \sqrt{2} \notin \mathbb{Q}$, and we find that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. This implies that $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$ so the fields are not equal. In particular, $\sqrt{2} \notin \mathbb{Q}(\sqrt[4]{2})$. □

Exercise .1.21. Let $k \subseteq F$ be a field extension, and let E be the intermediate field consisting of the elements of F which are algebraic over k. For $\alpha \in F$, prove that α is algebraic over E if and only if $\alpha \in E$. Deduce that $\overline{\mathbb{Q}}$ is algebraically closed.

Solution. If $\alpha \in E$, then α is algebraic over k. That is, there is a polynomial $p(x) \in k[x]$ such that $p(\alpha) = 0$. But then $p(x) \in E[x]$ so α is algebraic over E. Now suppose α is algebraic over E so there is a polynomial $p(x) \in E[x]$, say $p(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$, such that $p(\alpha) = 0$. Since each $b_i \in E$ is algebraic over k, the extension $k \subseteq k(b_0, b_1, \ldots, b_{n-1}) = L$ is finite. Then $p(x) \in L[x]$ so α is algebraic over L and, by Corollary 18, α is algebraic over k. Finally, the same reasoning as above shows that α is algebraic over E.

Recall that $\overline{\mathbb{Q}}$ is the set of elements of $\mathbb{C}$ which are algebraic over $\mathbb{Q}$. Then every polynomial with coefficients in this field determines an element which is algebraic over this field, and as we have shown above, elements which are algebraic over this field are in this field. Thus, every polynomial in $\overline{\mathbb{Q}}[x]$ has a root in $\overline{\mathbb{Q}}$ so the field is algebraically closed. □

Exercise .1.22. Let $k \subseteq F$ be a field extension, and let $\alpha \in F, \beta \in F$ be algebraic, of degree d, e, resp. Assume d, e are relatively prime, and let $p(x)$ be the minimal polynomial of β over k. Prove $p(x)$ is irreducible over $k(\alpha)$.

Solution. This is equivalent to showing that $p(x)$ is the minimal polynomial of β over $k(\alpha)$, or that $[k(\alpha, \beta) : k(\alpha)] = e$. Note that we have the extensions

$$k \subseteq k(\alpha) \subseteq k(\alpha, \beta)$$

where the first extension has degree d. Then d divides $[k(\alpha,\beta):k]$. Similarly, e divides $[k(\alpha,\beta):k]$ by considering the extensions $k \subseteq k(\beta) \subseteq k(\alpha,\beta)$ and since the two are relatively prime, we find de divides $[k(\alpha,\beta):k]$. Then

$$[k(\alpha,\beta):k] = [k(\alpha,\beta):k(\alpha)] \cdot [k(\alpha):k]$$

implies $de = [k(\alpha,\beta) : k(\alpha)] \cdot d$, or $[k(\alpha,\beta) : k(\alpha)] = e$, and the minimal polynomial of β over $k(\alpha)$ has degree e and must be monic, hence making it equal to $p(x)$. □

Exercise .1.23. Express $\sqrt{2}$ explicitly as a polynomial function in $\sqrt{2}+\sqrt{3}$ with rational coefficients.

Solution. Note that $(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2}+9\sqrt{3}$. Then we can easily verify that

$$\frac{1}{2}(\sqrt{2}+\sqrt{3})^3 - \frac{9}{2}(\sqrt{2}+\sqrt{3}) = \sqrt{2}$$

which is a polynomial in $\sqrt{2}+\sqrt{3}$ with coefficients in $\mathbb{Q}$. □

Exercise .1.24. Generalize the situation examined in Example 1.19: let k be a field of characteristic $\neq 2$, and let $a, b \in k$ be elements that are not squares in k; prove that $k(\sqrt{a},\sqrt{b}) = k(\sqrt{a}+\sqrt{b})$.

Prove that $k(\sqrt{a},\sqrt{b})$ has degree 2, resp., 4, over k according to whether ab is, resp., is not, a square in k.

Solution. Clearly, we have $k(\sqrt{a}+\sqrt{b}) \subseteq k(\sqrt{a},\sqrt{b})$. For the other direction, note that $k \subseteq k(\sqrt{a},\sqrt{b})$ is an algebraic extension of degree at most 4. Consider the tower of extensions

$$k \subseteq k(\sqrt{a}+\sqrt{b}) \subseteq k(\sqrt{a},\sqrt{b})$$

where the overall degree is ≤ 4. The overall degree cannot be 1 as this implies that the fields are isomorphic and that $\sqrt{a} \in k$. We know $k \subset k(\sqrt{a}+\sqrt{b})$ is a proper containment so this extension has degree greater than 1. Thus, if the overall degree is 2 or 3, the latter two fields are isomorphic by the multiplicativity of the degree of extensions. Finally, if the overall extension has degree 4, then the elements

$$1, \quad (\sqrt{a}+\sqrt{b}), (\sqrt{a}+\sqrt{b})^2, \quad (\sqrt{a}+\sqrt{b})^3, \quad (\sqrt{a}+\sqrt{b})^4$$

are linearly dependent and the minimal polynomial of this element $p(x) \in k[x]$ has degree 4, implying that $[k(\sqrt{a}+\sqrt{b}):k] = 4$ so again the latter two fields are isomorphic.

If $k(\sqrt{a},\sqrt{b})$ has degree 2 over k, then the minimal polynomial of $\sqrt{a}+\sqrt{b}$ has degree 2. Note that

$$(\sqrt{a}+\sqrt{b})^2 = a+b+2\sqrt{ab}$$

so this is an element of k only if ab is a square in k. If ab is not a square, then the minimal polynomial cannot have degree 2 since it will contain the above term, so it must have degree 4 as shown earlier. □

Exercise .1.25. Let $\xi := \sqrt{2+\sqrt{2}}$.

- Find the minimal polynomial of ξ over $\mathbb{Q}$, and show that $\mathbb{Q}(\xi)$ has degree 4 over $\mathbb{Q}$.
- Prove that $\sqrt{2-\sqrt{2}}$ is another root of the minimal polynomial of ξ.
- Prove that $\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\xi)$. (Hint: $(a+b)(a-b) = a^2 - b^2$.)
- By Proposition 1.5, sending ξ to $\sqrt{2-\sqrt{2}}$ defines an automorphism of $\mathbb{Q}(\xi)$ over $\mathbb{Q}$. Find the matrix of this automorphism w.r.t. the basis $1, \xi, \xi^2, \xi^3$.
- Prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi))$ is cyclic of order 4.

Solution. The minimal polynomial of ξ is $t^4 - 4t^2 + 2 \in \mathbb{Q}[t]$. By the rational roots test, this is an irreducible polynomial and hence the minimal polynomial of ξ, verifying that $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$.

We find that

$$\begin{aligned}\left(\sqrt{2-\sqrt{2}}\right)^4 - 4\left(\sqrt{2-\sqrt{2}}\right)^2 + 2 &= (4 - 4\sqrt{2} + 2) - 4(2-\sqrt{2}) + 2 \\ &= 0\end{aligned}$$

so $\sqrt{2-\sqrt{2}}$ is another root of the minimal polynomial of ξ.

Note that $(\sqrt{2+\sqrt{2}})(\sqrt{2-\sqrt{2}}) = \sqrt{2}$ which is an element of $\mathbb{Q}(\xi)$ since $\sqrt{2} = \xi^2 - 2$. Thus,

$$\sqrt{2-\sqrt{2}} = \frac{\xi^2 - 2}{\xi} \in \mathbb{Q}(\xi).$$

A lot of tedious work in transforming ξ^{-1} to a polynomial in ξ shows that $\sqrt{2-\sqrt{2}} = \xi^3 - 3\xi$, allowing us to express the automorphism as a matrix with the natural basis.

Then the matrix associated with the automorphism mapping ξ to $\sqrt{2-\sqrt{2}}$ is

$$M = \begin{pmatrix} 1 & 0 & 4 & 0 \\ 0 & -3 & 0 & -10 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 3 \end{pmatrix}$$

Then it becomes a matter of verifying that M, M^2, M^3, M^4 are all distinct and $M^4 = I_4$. That is, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi))$ is generated by M and has order 4, so it is cyclic of order 4. □

Exercise .1.26. Let $k \subseteq F$ be a field extension, let I be an indexing set, and let $\{\alpha_i\}_{i\in I}$ be a choice of elements of F. This choice determines a homomorphism φ of k-algebras from the polynomial ring $k[I]$ on the set I to F (the polynomial ring is a free commutative k-algebra; cf. Proposition III.6.4). We say that $\{\alpha_i\}_{i\in I}$ is *algebraically independent* over k if φ is injective. For example, distinct elements $\alpha_1, \ldots, \alpha_n$ of F are algebraically independent over k if there is no nonzero polynomial $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ such that $f(\alpha_1, \ldots, \alpha_n) = 0$.

Prove that $\alpha_1, \ldots, \alpha_n$ are algebrically independent if and only if the assignment $t_1 \mapsto \alpha_1, \ldots, t_n \mapsto \alpha_n$ defines a homomorphism of k-algebras (and hence an isomorphism) from the field of rational functions $k(t_1, \ldots, t_n)$ to $k(\alpha_1, \ldots, \alpha_n)$.

Solution. This follows rather trivially from the idea that the indeterminates in the field of rational functions are defined to be independent of one another. If the assignment is an isomorphism, then the $\alpha_1, \ldots, \alpha_n$ are algebraically independent. If the α_i are algebraically independent, then there is no function such that $f(\alpha_1, \ldots, \alpha_n) = 0$. In particular, they are all independent of one another and hence function identically to the indeterminates in the field of rational functions. □

Exercise .1.27. With notation and terminology as in Exercise 1.26, the indexed set $\{\alpha_i\}_{i\in I}$ is a *transcendence basis* for F over k if it is a maximal algebraically independent set in F.

- Prove that $\{\alpha_i\}_{i\in I}$ is a transcendence basis for F over k if and only if it is algebraically independent and F is algebraic over $k(\{\alpha_i\}_{i\in I})$.
- Prove that transcendence bases exist. (Zorn)
- Prove that any two transcendence bases for F over k have the same cardinality. (Mimic the proof of Proposition VI.1.9. Don't feel too bad if you prefer to deal only with the case of finite transcendence bases.)

The cardinality of a transcendence basis is called the *transcendence degree* of F over k, denoted $\mathrm{tr.deg}_{k\subseteq F}$.

Solution. Certainly if $\{\alpha_i\}_{i\in I}$ is a transcendence basis for F, then it is algebraically independent. If F is not algebraic over $k(\{\alpha_i\}_{i\in I})$, then there exists some element $\beta \in F$ which is transcendental over the latter field, and thus algebraically independent of the elements α_i. But this contradicts that $\{\alpha_i\}$ is maximal. Therefore, F is algebraic over $k(\{\alpha_i\}_{i\in I})$. The other direction is effectively the same.

Consider all algebraically independent subsets of F over k ordered by inclusion. Given a chain in this set, the union of all elements in this chain is an upper bound since it contains all elements of the chain and is algebraically independent by definition. Then, by Zorn's lemma, this poset has maximal elements, and these are by definition transcendence bases.

For the third part, let B be a transcendence basis for F over k and let S be any algebraically independent subset of F over k. We construct an injective map $j : S \to B$ which we define inductively. Let $\leq$ be a well-ordering on S, let $\beta \in S$, and suppose we have defined $j(\alpha)$ for all $\alpha < \beta$. Let B' be the set obtained from B by replacing all $j(\alpha)$ by α for $\alpha < \beta$. By the inductive hypothesis, B' is still a transcendence basis. We can choose $j(\beta)$ such that it is unique and the set obtained from B' by replacing β by $j(\beta)$ is still a transcendence basis. Indeed, the set $B' \cup \{\beta\}$ is algebraically dependent so there is a polynomial $f \in k[t_1, t_2, \ldots, t_n, t_{n+1}]$ such that $f(\{\alpha_i\}, \beta) = 0$. Necessarily, the coefficients of β are not all zero, and not all the elements of $\{\alpha_i\}$ are in S since S is algebraically independent. Thus, we may assume that $\alpha_1 \in B' \setminus S$ and has nonzero coefficient. Then $\alpha_1 \neq j(\alpha)$ for any $\alpha < \beta$ so we set $j(\beta) = \alpha_1$. It suffices to verify that the set B'' obtained from B' by replacing α_1 by β is a transcendence basis. But we have an algebraic relation among $B' \cup \{\beta\}$ given by f so replacing an element of B' by β again yields a maximal algebraically independent set. □

Exercise .1.28. Let $k \subseteq E \subseteq F$ be field extensions. Prove that $\mathrm{tr.deg}_{k \subseteq F}$ is finite if and only if both $\mathrm{tr.deg}_{k \subseteq E}$ and $\mathrm{tr.deg}_{E \subseteq F}$ (see Exercise 1.27) are finite and in this case

$$\mathrm{tr.deg}_{k \subseteq F} = \mathrm{tr.deg}_{k \subseteq E} + \mathrm{tr.deg}_{E \subseteq F}.$$

Solution. If F admits a finite transcendence basis over k, then separating this basis into elements contained in E and those not contained in E gives transcendental bases for F over E and E over k respectively, showing that they are both finite. Conversely, suppose that we have finite transcendence bases for F over E and for E over k. Then taking the union of these bases yields a transcendence basis for F over k, and certainly the two bases are disjoint so $\mathrm{tr.deg}_{k \subseteq F}$ is the sum of the other two transcendence degrees. □

Exercise .1.29. An extension $k \subseteq F$ is *purely transcendental* if it admits a transcendence basis $\{\alpha_i\}_{i \in I}$ (see Exercise 1.27) such that $F = k(\{\alpha_i\}_{i \in I})$.

Prove that any field extension $f \subseteq F$ may be decomposed as a purely transcendental extension follows by an algebraic extension. (Not all field extensions may be decomposed as an algebraic extension followed by a purely transcendental extension.)

Solution. Let B be a transcendence basis for F over f (which exists by Exercise 27). Then $f \subseteq f(B) = k$ is a purely transcendental extension where F is algebraic over k, so $k \subseteq F$ is an algebraic extensions. Thus, $f \subseteq F$ is a purely transcendental extension followed by an algebraic extension. □

Exercise .1.30. Let $k \subseteq k(\alpha)$ be a simple extension, with α transcendental over k. Let E be a subfield of $k(\alpha)$ properly containing k. Prove that $\mathrm{tr.deg}_{k \subseteq E} = 1$.

Lüroth's theorem asserts that in this situation $k \subseteq E$ is itself a simple transcendental extension of k; that is, it is purely transcenental (Exercise 1.29).

Solution. If E properly contains k, then it must contain some minimal power of α, say α^n. We claim that $\{\alpha^n\}$ is a transcendental basis for E over k. Certainly it is algebraically independent since α and hence α^n is transcendental over k. To show that it is maximal, let β be another transcendental element of E. Then it is some polynomial in α^n, hence it is algebraic in α^n. Therefore, this set is maximal and $\mathrm{tr.deg}_{k \subseteq E} = 1$. $\square$