

Extension Fields I

Throughout these notes, the letters F , E , K denote fields.

1 Introduction to extension fields

Let F , E be fields and suppose that $F \leq E$, i.e. that F is a subfield of E . We will often view F as the primary object of interest, and in this case refer to E as an *extension field* or simply *extension* of F . For example, \mathbb{R} is an extension field of \mathbb{Q} and \mathbb{C} is an extension field of \mathbb{R} .

Now suppose that E is an extension field of F and that $\alpha \in E$. We have the evaluation homomorphism $\text{ev}_\alpha: F[x] \rightarrow E$, whose value on a polynomial $f \in F[x]$ is $f(\alpha)$. By definition, the image $\text{Im ev}_\alpha = F[\alpha]$ is a subring of E . It is the smallest subring of E containing both F and α , and it is an integral domain as it is a subring of a field. Note that, by definition,

$$F[\alpha] = \text{Im ev}_\alpha = \{f(\alpha) : f \in F[x]\}.$$

There are now two cases:

Case I: $\text{Ker ev}_\alpha = \{0\}$. In other words, if $f \in F[x]$ is a nonzero polynomial, then $f(\alpha) \neq 0$, i.e. α is not the root of any nonzero polynomial in f . In this case, we say that α is *transcendental over F* . If α is transcendental over F , then $\text{ev}_\alpha: F[x] \rightarrow E$ is injective, and hence ev_α is an isomorphism from $F[x]$ to $F[\alpha] \subseteq E$. Note that $\text{ev}_\alpha(x) = \alpha$. In particular, $F[\alpha]$ is not a field, since $F[x]$ is not a field. By results on the field of quotients of an integral domain, ev_α extends to an injective homomorphism $\tilde{\text{ev}}_\alpha: F(x) \rightarrow E$. Clearly, the image of $\tilde{\text{ev}}_\alpha$ is the set of all quotients in E of the form $f(\alpha)/g(\alpha)$, where $f, g \in F[x]$ and $g \neq 0$. By general properties of fields of quotients, $f_1(\alpha)/g_1(\alpha) = f_2(\alpha)/g_2(\alpha) \iff f_1(\alpha)g_2(\alpha) = f_2(\alpha)g_1(\alpha) \iff f_1g_2 = f_2g_1$. Defining

$$F(\alpha) = \text{Im } \tilde{\text{ev}}_\alpha = \{f(\alpha)/g(\alpha) : f, g \in F[x], g \neq 0\},$$

we see that $F(\alpha)$ is a field and it is the smallest subfield of E containing F and α .

For example, if $F = \mathbb{Q}$ and $E = \mathbb{R}$, “most” elements of \mathbb{R} are transcendental over \mathbb{Q} . In fact, it is not hard to show that the set of elements of \mathbb{R} which are not transcendental over \mathbb{Q} is countable, and since \mathbb{R} is uncountable there are an uncountable number of elements of \mathbb{R} which are transcendental over \mathbb{Q} . It is much harder to show that a given element of \mathbb{R} is transcendental over \mathbb{Q} . For example e and π are both transcendental over \mathbb{Q} . (The transcendence of π shows that it is impossible to “square the circle,” in other words to construct a square with straightedge and compass whose area is π .) Hence, the subring $\mathbb{Q}[\pi]$ of \mathbb{R} is isomorphic to the polynomial ring $\mathbb{Q}[x]$: every element of $\mathbb{Q}[\pi]$ can be uniquely written as a polynomial $\sum_{i=0}^n a_i \pi^i$ in π , where the $a_i \in \mathbb{Q}$. The field $\mathbb{Q}(\pi)$ is then the set of all quotients, $f(\pi)/g(\pi)$, where $f, g \in \mathbb{Q}[x]$ and $g \neq 0$. Finally, note that the property of transcendence is very much a relative property. Thus, $\pi \in \mathbb{R}$ is transcendental over \mathbb{Q} , but π is **not** transcendental over \mathbb{R} ; in fact, π is a root of the nonzero polynomial $x - \pi \in \mathbb{R}[x]$.

For another example, let F be an arbitrary field and consider $F(x)$, the field of rational functions with coefficients in F . Thus $F(x)$ is the field of quotients of the polynomial ring $F[x]$, and the elements of $F(x)$ are quotients f/g , where $f, g \in F[x]$ and $g \neq 0$. However, when we think of $F(x)$ as a field in its own right, it is traditional to rename the variable x by some other letter such as t , which we still refer too as an “indeterminate,” to avoid confusion with x which we reserve for the “variable” of a polynomial. With this convention, the field $F(t)$ (with t an indeterminate) is an extension field of F . Moreover, $t \in F(t)$ is transcendental over F , since, if $f \in F[x]$ is a nonzero polynomial, then $\text{ev}_t f = f(t)$, which is a nonzero element of $F[t]$ and hence of $F(t)$.

Case II: $\text{Ker ev}_\alpha \neq \{0\}$. In other words, there exists a nonzero polynomial $f \in F[x]$ $f(\alpha) = 0$. In this case, we say that α is *algebraic over F* . This will be the important case for us, so we state the main result as a proposition:

Proposition 1.1. *Suppose that E is an extension field of F and that $\alpha \in E$ is algebraic over F . Then $\text{Ker ev}_\alpha = (p)$, where $p \in F[x]$ is an irreducible polynomial. Moreover, if $f \in F[x]$ is any polynomial such that $f(\alpha) = 0$, then $p \mid f$. The homomorphism ev_α induces an isomorphism, denoted $\hat{\text{ev}}_\alpha$, from $F[x]/(p)$ to $F[\alpha]$, with the property that $\hat{\text{ev}}_\alpha(x + (p)) = \alpha$. Finally, $F[\alpha] = \text{Im ev}_\alpha$ is a field.*

Proof. By hypothesis, Ker ev_α is a nonzero ideal in $F[x]$. Moreover, by the proof of the first isomorphism theorem, the homomorphism ev_α induces an

isomorphism, denoted $\widehat{\text{ev}}_\alpha$, from $F[x]/\text{Ker ev}_\alpha$ to $F[\alpha]$, and in particular $F[\alpha] \cong F[x]/\text{Ker ev}_\alpha$. By the definition of $\widehat{\text{ev}}_\alpha$, if $I = \text{Ker ev}_\alpha$, then we have $\widehat{\text{ev}}_\alpha(g + I) = \text{ev}_\alpha(g) = g(\alpha)$. In particular $\widehat{\text{ev}}_\alpha(x + \text{Ker ev}_\alpha) = \alpha$. Since $F[\alpha]$ is a subring of a field, it is an integral domain. Thus $F[x]/\text{Ker ev}_\alpha$ is also an integral domain, and hence Ker ev_α is a prime ideal. But we have seen that every nonzero prime ideal is maximal, hence $F[\alpha]$ is a subfield of E , and that the nonzero prime ideals are exactly those of the form (p) , where $p \in F[x]$ is an irreducible polynomial. Thus $\text{Ker ev}_\alpha = (p)$ for some irreducible polynomial $p \in F[x]$. By definition, $f(\alpha) = 0 \iff f \in \text{Ker ev}_\alpha \iff p|f$. \square

Definition 1.2. Let E be an extension field of F and suppose that $\alpha \in E$ is algebraic over F . We set $F(\alpha) = F[\alpha]$. As in Case I, $F(\alpha)$ is a subfield of E and is the smallest subfield of E containing both F and α .

With E and α as above, suppose that $p_1, p_2 \in F[x]$ are two polynomials such that $\text{Ker ev}_\alpha = (p_1) = (p_2)$. Then $p_1|p_2$ and $p_2|p_1$. Then there exists a $c \in F^*$ such that $p_2 = cp_1$. In particular, there is a unique monic polynomial $p \in F[x]$ such that $\text{Ker ev}_\alpha = (p)$.

Definition 1.3. Let E be an extension field of F and suppose that $\alpha \in E$ is algebraic over F . The unique monic irreducible polynomial which is a generator of Ker ev_α will be denoted $\text{irr}(\alpha, F)$.

Thus, if E is an extension field of F and $\alpha \in E$ is algebraic over F , then $\text{irr}(\alpha, F)$ is the unique monic irreducible polynomial in $F[x]$ for which α is a root. One way to find $\text{irr}(\alpha, F)$ is as follows:

Lemma 1.4. *Suppose that E is an extension field of F and that $\alpha \in E$. Let $p \in F[x]$ be an irreducible monic polynomial such that $p(\alpha) = 0$. Then $p = \text{irr}(\alpha, F)$.*

Proof. By Proposition 1.1, $\text{irr}(\alpha, F)$ divides p , but since p is irreducible, there exists a $c \in F^*$ such that $p = c \text{irr}(\alpha, F)$. Finally, since both p and $\text{irr}(\alpha, F)$ are monic, $c = 1$, i.e. $p = \text{irr}(\alpha, F)$. \square

For example, $x^2 - 2 = \text{irr}(\sqrt{2}, \mathbb{Q})$, since $p = x^2 - 2$ is monic and (as we have seen) irreducible and $p(\sqrt{2}) = 0$. As in Case I, the definition of $\text{irr}(\alpha, F)$ is relative to the field F . For example, $\text{irr}(\sqrt{2}, \mathbb{Q}(\sqrt{2})) = x - \sqrt{2}$. Note that $x - \sqrt{2}$ is a factor of $x^2 - 2$ in $\mathbb{Q}(\sqrt{2})[x]$, but that $x - \sqrt{2}$ is not an element of $\mathbb{Q}[x]$.

One problem with finding $\text{irr}(\alpha, F)$ is that we don't have many ways of showing that a polynomial is irreducible. So far, we just know that a

polynomial of degree 2 or 3 is irreducible \iff it does not have a root. Here are a few more examples that we can handle by this method:

Example 1.5. (1) $\text{irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ since $\sqrt[3]{2}$ is irrational.

(2) There is no element $\alpha \in \mathbb{Q}(\sqrt{2})$ such that $\alpha^2 = 3$ (by a homework problem). In other words, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Thus $\text{irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 - 3$.

(3) If $\alpha = \sqrt{2} + \sqrt{3}$, then it is easy to check (homework) that α is a root of the polynomial $x^4 - 10x^2 + 1$. Thus $\text{irr}(\alpha, \mathbb{Q})$ divides $x^4 - 10x^2 + 1$, but we cannot conclude that they are equal unless we can show that $x^4 - 10x^2 + 1$ is irreducible, or by some other method. We will describe one such method in the next section.

Definition 1.6. Let E be an extension field of F . Then we say that E is a *simple extension of F* if there exists an $\alpha \in E$ such that $E = F(\alpha)$. Note that this definition makes sense both in case α is algebraic over F and in case it is transcendental over F . However, we shall mainly be interested in the case where α is algebraic over F .

In many cases, we want to consider extension fields which are not necessarily simple extensions.

Definition 1.7. Let E be an extension field of F and let $\alpha_1, \dots, \alpha_n \in E$. We define $F(\alpha_1, \dots, \alpha_n)$ to be the smallest subfield of E containing F and $\alpha_1, \dots, \alpha_n$. If $E = F(\alpha_1, \dots, \alpha_n)$, we say that E is *generated over F by $\alpha_1, \dots, \alpha_n$* . It is easy to see that $F(\alpha_1, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$. In fact, by definition, both sides of this equality are the smallest subfield of E containing F , $\alpha_1, \dots, \alpha_{n-1}$, and α_n . More generally, for every k , $1 \leq k \leq n$, $F(\alpha_1, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_k)(\alpha_{k+1}, \dots, \alpha_n)$.

Example 1.8. Consider the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and hence $\mathbb{Q}(\alpha) \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. However, it is another homework problem to show that $\sqrt{2} \in \mathbb{Q}(\alpha)$ and that $\sqrt{3} \in \mathbb{Q}(\alpha)$. Thus $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \leq \mathbb{Q}(\alpha)$ and hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$. In conclusion, a field such as $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ which is not obviously a simple extension may turn out to be a simple extension. We shall analyze this in much greater detail later.

2 Finite and algebraic extensions

Let E be an extension field of F . Then E is an F -vector space.

Definition 2.1. Let E be an extension field of F . Then E is a *finite extension of F* if E is a finite dimensional F -vector space. If E is a finite

extension of F , then the positive integer $\dim_F E$ is called the *degree of E over F* , and is denoted $[E : F]$. Note that $[E : F] = 1 \iff E = F$.

Proposition 2.2. *Suppose that $E = F(\alpha)$ is a simple extension of F . Then E is a finite extension of $F \iff \alpha$ is algebraic over F . In this case*

$$[E : F] = \deg_F \alpha,$$

where by definition $\deg_F \alpha$ is the degree of $\text{irr}(\alpha, F)$. Finally, if α is algebraic over F and $\deg_F \alpha = \text{irr}(\alpha, F) = d$, then $1, \alpha, \dots, \alpha^{d-1}$ is a basis for $F(\alpha)$ as an F -vector space.

Proof. First suppose that α is transcendental over F . Then we have seen that $F \leq F[\alpha] \leq F(\alpha)$, and that $\text{ev}_\alpha: F[x] \rightarrow F[\alpha]$ is an isomorphism, which is clearly F -linear. Since $F[x]$ is not a finite dimensional F -vector space, $F[\alpha]$ is also not a finite dimensional F -vector space. But then $F(\alpha)$ is also not a finite dimensional F -vector space, since every vector subspace of a finite dimensional F -vector space is also finite dimensional. Hence $F(\alpha)$ is not a finite extension of F .

Now suppose that α is algebraic over F . Then ev_α induces an isomorphism $\widehat{\text{ev}}_\alpha: F[x]/(\text{irr}(\alpha, F)) \rightarrow F[\alpha] = F(\alpha)$. Concretely, given $g \in F[x]$, $\widehat{\text{ev}}_\alpha(g + (\text{irr}(\alpha, F))) = g(\alpha)$. Moreover, every coset in the quotient ring $F[x]/(\text{irr}(\alpha, F))$ can be uniquely written as $\sum_{i=0}^{d-1} c_i x^i + (\text{irr}(\alpha, F))$, where $d = \deg \text{irr}(\alpha, F)$. It follows that every element of $F[\alpha] = F(\alpha)$ can be uniquely written as $\sum_{i=0}^{d-1} c_i \alpha^i$. Thus, $1, \alpha, \dots, \alpha^{d-1}$ is a basis for $F(\alpha)$ as an F -vector space. It then follows that $\dim_F F(\alpha) = d$. \square

To be able to calculate the degree $[E : F]$ and use it to extract more information about field extensions, we shall need to consider a sequence of extension fields:

Proposition 2.3. *Suppose that F , E , and K are fields such that $F \leq E \leq K$, i.e. that E is an extension field of F and that K is an extension field of E . Then K is a finite extension field of $F \iff K$ is a finite extension field of E and E is a finite extension field of F . Moreover, in this case*

$$[K : F] = [K : E][E : F].$$

Proof. First suppose that K is a finite extension field of F . Then E is an F -vector subspace of the finite dimensional F -vector space K , hence E is finite dimensional and thus is a finite extension of F . Also, there exists an F -basis $\alpha_1, \dots, \alpha_n$ of K . Thus every element of K is a linear combination of the

α_i with coefficients in F and hence with coefficients in E . Thus $\alpha_1, \dots, \alpha_n$ span K as an E -vector space, so that K is a finite dimensional E -vector space. Thus K is a finite extension field of E .

Conversely, suppose that K is a finite extension field of E and E is a finite extension field of F . The proof then follows from the following more general lemma (taking $V = K$): \square

Lemma 2.4. *Let E be a finite extension field of F and let V be an E -vector space. Then, viewing V as an F -vector space, V is a finite-dimensional F -vector space $\iff V$ is a finite-dimensional E -vector space, and in this case*

$$\dim_F V = [E : F] \dim_E V.$$

Proof. \implies : As in the proof above, an F -basis of V clearly spans V over E , hence if V is a finite-dimensional F -vector space, then it is a finite-dimensional E -vector space.

\impliedby : Let v_1, \dots, v_n be an E -basis for V and let $\alpha_1, \dots, \alpha_m$ be an F -basis for E . We claim that $\alpha_i v_j$ is an F -basis for V . First, the $\alpha_i v_j$ span V : if $v \in V$, since the v_j are an E -basis for V , there exist $a_j \in E$ such that $\sum_{j=1}^n a_j v_j = v$. Since the α_i are an F -basis of E , there exist $b_{ij} \in F$ such that $a_j = \sum_{i=1}^m b_{ij} \alpha_i$. Hence

$$v = \sum_{j=1}^n a_j v_j = \sum_{i,j} b_{ij} \alpha_i v_j.$$

Thus the $\alpha_i v_j$ span V .

Finally, to see that the $\alpha_i v_j$ are linearly independent, suppose that there exist $b_{ij} \in F$ such that $\sum_{i,j} b_{ij} \alpha_i v_j = 0$. We must show that all of the b_{ij} are 0. Regrouping this sum as

$$0 = \sum_{i,j} b_{ij} \alpha_i v_j = \sum_{j=1}^n \left(\sum_{i=1}^m b_{ij} \alpha_i \right) v_j,$$

and using the fact that the v_j are linearly independent over E , it follows that, for every j , the sum $\sum_{i=1}^m b_{ij} \alpha_i$ is 0. But since the α_i are linearly independent over F , we must have $b_{ij} = 0$ for all i and j . Hence the $\alpha_i v_j$ are linearly independent, and therefore a basis. \square

Corollary 2.5. *If $F \leq E \leq K$ and K is a finite extension of F , then $[K : E]$ and $[E : F]$ both divide $[K : F]$.*

Proof. This is immediate from the formula above. \square

The proof also shows the following:

Corollary 2.6. *If K is a finite extension field of E with basis β_1, \dots, β_n and E is a finite extension field of F with basis $\alpha_1, \dots, \alpha_m$, then $\alpha_i \beta_j$, $1 \leq i \leq m$ and $1 \leq j \leq n$, is an F -basis of K . \square*

Example 2.7. By a homework problem, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Thus

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

A \mathbb{Q} -basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. Furthermore, with $\alpha = \sqrt{2} + \sqrt{3}$, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and so $\deg_{\mathbb{Q}} \alpha = 4$. In particular, $\text{irr}(\alpha, \mathbb{Q})$ has degree 4 and divides $x^4 - 10x^2 + 1$, so that $\text{irr}(\alpha, \mathbb{Q}) = x^4 - 10x^2 + 1$. Another basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as \mathbb{Q} -vector space is then $1, \alpha, \alpha^2, \alpha^3$; here $\alpha = \sqrt{2} + \sqrt{3}$, $\alpha^2 = 5 + \sqrt{6}$, and $\alpha^3 = 11\sqrt{2} + 9\sqrt{3}$. Of course there are many other possible bases.

Example 2.8. The real number $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$, because if it were, then $\mathbb{Q}(\sqrt{2})$ would be a subfield of $\mathbb{Q}(\sqrt[3]{2})$, hence $2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ would divide $3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$.

Example 2.9. The above corollary is the main point in showing that various geometric constructions with straightedge and compass such as trisecting every angle or doubling the cube are impossible.

Returning to a general extension of fields, we have the following basic definition:

Definition 2.10. Let E be an extension field of F . Then E is an *algebraic extension* of F if, for every $\alpha \in E$, α is algebraic over F .

The following two lemmas are then easy corollaries of Proposition 2.3:

Lemma 2.11. *Let E be a finite extension of F . Then E is an algebraic extension of F .*

Proof. If $\alpha \in E$, then we have a sequence of extensions

$$F \leq F(\alpha) \leq E.$$

Since E is a finite extension of F , $F(\alpha)$ is a finite extension of F as well, by Proposition 2.3. Thus α is algebraic over F . \square

Lemma 2.12. *Let E be an extension field of F and let $\alpha, \beta \in E$ be algebraic over F . Then $\alpha \pm \beta$, $\alpha \cdot \beta$, and (if $\beta \neq 0$) α/β are all algebraic over F .*

Proof. Consider the sequence of extensions

$$F \leq F(\alpha) \leq F(\alpha)(\beta) = F(\alpha, \beta).$$

Then $F(\alpha)$ is a finite extension of F since α is algebraic over F . Moreover, β is the root of a nonzero polynomial with coefficients in F , and hence with coefficients in $F(\alpha)$. Thus β is algebraic over $F(\alpha)$, so that $F(\alpha)(\beta)$ is a finite extension of $F(\alpha)$. By Proposition 2.3, $F(\alpha, \beta)$ is then a finite extension of F , and by the previous lemma it is an algebraic extension of F . Thus every element of $F(\alpha, \beta)$ is algebraic over F , in particular $\alpha \pm \beta$, $\alpha \cdot \beta$, and α/β if $\beta \neq 0$. \square

Definition 2.13. Let E be an extension field of F . We define the *algebraic closure of F in E* to be

$$\{ \alpha \in E : \alpha \text{ is algebraic over } F \}.$$

Thus the algebraic closure of F in E is the set of all elements of E which are algebraic over F .

Corollary 2.14. *The algebraic closure of F in E is a subfield of E containing F . Moreover, it is an algebraic extension of F .*

Proof. It clearly contains F , since every $a \in F$ is algebraic over F , and it is a subfield of E by Lemma 2.12. By definition, the algebraic closure of F in E is an algebraic extension of F . \square

Example 2.15. There are many fields which are algebraic over \mathbb{Q} but not finite over \mathbb{Q} . For example, it is not hard to see that the smallest subfield $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$ of \mathbb{R} which contains the square roots of all of the prime numbers, and hence of every positive integer, is not a finite extension of \mathbb{Q} .

For another important example, let \mathbb{Q}^{alg} , the *field of algebraic numbers*, be the algebraic closure of \mathbb{Q} in \mathbb{C} . Thus

$$\mathbb{Q}^{\text{alg}} = \{ \alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q} \}.$$

Then \mathbb{Q}^{alg} is a subfield of \mathbb{C} , and by definition it is the largest subfield of \mathbb{C} which is algebraic over \mathbb{Q} . The extension field \mathbb{Q}^{alg} is not a finite extension of \mathbb{Q} , since for example it contains $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$.

Finally, let F be an arbitrary field and consider the extension $F(t)$ of F , where t is an indeterminate. As we have seen $F(t)$ is not an algebraic extension of F . In fact, one can show that the algebraic closure of F in $F(t)$ is F , in other words that if a rational function $f(t)/g(t)$ is the root of a nonzero polynomial with coefficients in F , then $f(t)/g(t)$ is constant, i.e. lies in the subfield F of $F(t)$.

We now give another characterization of finite extensions:

Lemma 2.16. *Let E be an extension of F . Then E is a finite extension of F \iff there exist $\alpha_1, \dots, \alpha_n \in E$, all algebraic over F , such that $E = F(\alpha_1, \dots, \alpha_n)$.*

Proof. \Leftarrow : By induction on n . In case $n = 1$, this is just the statement that, if α_1 is algebraic over F , then the simple extension $F(\alpha_1)$ is a finite extension of F . For the inductive step, suppose that we have showed that $F(\alpha_1, \dots, \alpha_i)$ is a finite extension of F . Then α_{i+1} is algebraic over F , hence over $F(\alpha_1, \dots, \alpha_i)$ as in the proof of Lemma 2.12. Thus $F(\alpha_1, \dots, \alpha_{i+1}) = F(\alpha_1, \dots, \alpha_i)(\alpha_{i+1})$ is a finite extension of $F(\alpha_1, \dots, \alpha_i)$. Now consider the sequence of extensions

$$F \leq F(\alpha_1, \dots, \alpha_i) \leq F(\alpha_1, \dots, \alpha_{i+1}).$$

Since $F(\alpha_1, \dots, \alpha_{i+1})$ is a finite extension of $F(\alpha_1, \dots, \alpha_i)$ and $F(\alpha_1, \dots, \alpha_i)$ is a finite extension of F , it follows from Proposition 2.3 that $F(\alpha_1, \dots, \alpha_{i+1})$ is a finite extension of F . This completes the inductive step, and hence the proof that $E = F(\alpha_1, \dots, \alpha_n)$ is a finite extension of F .

\implies : Let $N = [E : F]$. The proof is by complete induction on N , and the case $N = 1$ is clear since then $E = F$ and we can just take $\alpha_1 = 1$. Now suppose that we have showed that, for every finite extension $F_1 \leq E_1$ with degree $[E_1 : F_1] < N$, there exist $\beta_1, \dots, \beta_k \in E_1$ such that $E_1 = F_1(\beta_1, \dots, \beta_k)$. Let E be a finite extension of F with $[E : F] = N > 1$. Since $E \neq F$, there exists an $\alpha_1 \in E$ with $\alpha_1 \notin F$. Hence $[F(\alpha_1) : F] > 1$. Since $N = [E : F] = [E : F(\alpha_1)][F(\alpha_1) : F]$, it follows that $[E : F(\alpha_1)] < N$. By the inductive hypothesis, there exist $\alpha_2, \dots, \alpha_n \in E$ such that $E = F(\alpha_1)(\alpha_2, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_n)$. Finally, the α_i are automatically algebraic over F since E is a finite extension of F . This completes the proof of the inductive step and hence of the lemma. \square

Lemma 2.17. *Let $F \leq E \leq K$ be a sequence of field extensions, with E an algebraic extension of F , and let $\alpha \in K$. Then α is algebraic over F \iff α is algebraic over E .*

Proof. \implies : This is clear since, if α is a root of a nonzero polynomial $f \in F[x]$, then since $F[x] \subseteq E[x]$, α is also a root of the nonzero polynomial f viewed as an element of $E[x]$.

\Leftarrow : Write $\text{irr}(\alpha, E) = x^n + a_{n-1}x^{n-1} + \dots + a_0$, where the $a_i \in E$ and hence the a_i are algebraic over F . By the previous lemma, $F(a_0, \dots, a_{n-1})$ is a finite extension of F , and clearly α is algebraic over $F(a_0, \dots, a_{n-1})$ since

it is the root of a nonzero polynomial with coefficients in $F(a_0, \dots, a_{n-1})$.

Thus

$$F(a_0, \dots, a_{n-1})(\alpha) = F(a_0, \dots, a_{n-1}, \alpha)$$

is a finite extension of $F(a_0, \dots, a_{n-1})$. It follows from Proposition 2.3 that $F(a_0, \dots, a_{n-1}, \alpha)$ is a finite extension of F , hence an algebraic extension of F . Hence α is algebraic over F . \square

Corollary 2.18. *Let $F \leq E \leq K$ be a sequence of field extensions. Then K is an algebraic extension of $F \iff K$ is an algebraic extension of E and E is an algebraic extension of F .*

Proof. \implies : If K is an algebraic extension of F , then clearly E is an algebraic extension of F . Moreover, every element α of K is the root of a nonzero polynomial with coefficients in F and hence in E , hence α is algebraic over E . Thus K is an algebraic extension of E .

\impliedby : Follows immediately from the preceding lemma. \square

Definition 2.19. A field K is *algebraically closed* if every nonconstant polynomial $f \in K[x]$ has a root in K .

Lemma 2.20. *Let K be a field. Then the following are equivalent:*

- (i) K is algebraically closed.
- (ii) If $f \in K[x]$ is a nonconstant polynomial, then f is a product of linear factors. In other words, the irreducible polynomials in $K[x]$ are linear.
- (iii) The only algebraic extension of K is K .

Proof. (i) \implies (ii): Let $f \in K[x]$ be a nonconstant polynomial. Then f factors into a product of irreducible polynomials, so it suffices to show that every irreducible polynomial is linear. Let p be irreducible. Then, since K is algebraically closed, there exists a root α of p in K , and hence a linear factor $x - \alpha \in K[x]$ of p . Since p is irreducible, $p = c(x - \alpha)$ for some $c \in K^*$, and hence p is linear.

(ii) \implies (iii): Let E be an algebraic extension of K and let $\alpha \in E$. Then $p = \text{irr}(\alpha, K)$ is a monic irreducible polynomial, hence necessarily of the form $x - \alpha$. Since $p \in K[x]$, it follows that $\alpha \in K$.

(iii) \implies (i): If $f \in K[x]$ is a nonconstant polynomial, then there exists an extension field E of K and an $\alpha \in E$ which is a root of f . Clearly, α is algebraic over K and hence the extension field $F(\alpha)$ is an algebraic extension of K . By assumption, $K(\alpha) = K$, i.e. $\alpha \in K$. Hence there exists a root of f in K . \square

The most important example of an algebraically closed field comes from the following theorem, essentially due to Gauss (1799):

Theorem 2.21 (The Fundamental Theorem of Algebra). *The field \mathbb{C} of complex numbers is algebraically closed.* \square

Despite its name, the Fundamental Theorem of Algebra cannot be a theorem strictly about algebra, since the real numbers and hence the complex numbers are not defined algebraically. There are many proofs of the Fundamental Theorem of Algebra. A number of proofs use some basic complex analysis, or some topological properties of the plane. We will give a (mostly) algebraic proof at the end of the course.

Definition 2.22. Let F be a field. Then an extension field K of F is an *algebraic closure* of F if the following hold:

1. K is an algebraic extension of F , and
2. K is algebraically closed.

With this definition, \mathbb{C} is **not** an algebraic closure of \mathbb{Q} , because \mathbb{C} is not an algebraic extension of \mathbb{Q} .

So far, we have defined three confusingly similar sounding concepts: **the** algebraic closure of the field F in an extension field E , when a field K **is** algebraically closed (with no reference to any subfield), and when an extension field K is **an** algebraic closure of the field F . One way these concepts are related is as follows:

Proposition 2.23. *Let F be a field, let K be an extension field of F , and suppose that K is algebraically closed. Then the algebraic closure of F in K is an algebraic closure of F .*

Proof. Let E be the algebraic closure of F in K . Then E is an algebraic extension of F , and we must prove that E is algebraically closed. Let $f \in E[x]$ be a nonconstant polynomial. Then, since $E[x] \subseteq K[x]$, there exists a root $\alpha \in K$ of f . Clearly α is algebraic over E . By Lemma 2.17, α is algebraic over F , hence $\alpha \in E$. Thus E is algebraically closed. \square

Corollary 2.24. *The field \mathbb{Q}^{alg} of algebraic numbers is an algebraic closure of \mathbb{Q} .* \square

The following theorem, which we shall not prove, guarantees the existence of an algebraic closure for every field:

Theorem 2.25. *Let F be a field. Then there exists an algebraic closure of F . Moreover, every two algebraic closures of F are isomorphic. More precisely, if $F \leq K_1$ and $F \leq K_2$, then there exists an isomorphism $\rho: K_1 \rightarrow K_2$ such that $\rho(a) = a$ for all $a \in F$, viewing F as a subfield both of K_1 and K_2 . \square*

The isomorphism ρ in the previous theorem is far from unique. In fact, understanding the possible isomorphisms is, in a very vague sense, the central problem in Galois theory.