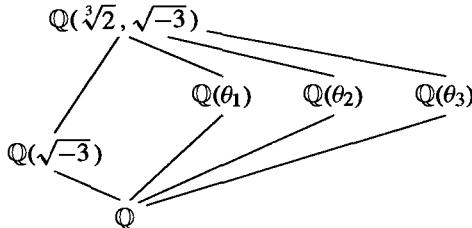


Since this extension degree is also divisible by 3 (because $\mathbb{Q}(\sqrt[3]{2}) \subset K$), the degree is divisible by 6, hence must be 6.

This gives us the diagram of known subfields:



where

$$\theta_1 = \sqrt[3]{2}, \quad \theta_2 = \sqrt[3]{2} \left(\frac{-1 + i\sqrt{3}}{2} \right), \quad \theta_3 = \sqrt[3]{2} \left(\frac{-1 - i\sqrt{3}}{2} \right).$$

- (4) One must be careful in computing splitting fields. The splitting field for the polynomial $x^4 + 4$ over \mathbb{Q} is smaller than one might at first suspect. In fact this polynomial factors over \mathbb{Q} :

$$\begin{aligned} x^4 + 4 &= x^4 + 4x^2 + 4 - 4x^2 = (x^2 + 2)^2 - 4x^2 \\ &= (x^2 + 2x + 2)(x^2 - 2x + 2) \end{aligned}$$

where these two factors are irreducible (Eisenstein again). Solving for the roots of the two factors by the quadratic formula, we find the four roots

$$\pm 1 \pm i$$

so that the splitting field of this polynomial is just the field $\mathbb{Q}(i)$, an extension of degree 2 of \mathbb{Q} .

In general, if $f(x) \in F[x]$ is a polynomial of degree n , then adjoining one root of $f(x)$ to F generates an extension F_1 of degree at most n (and equal to n if and only if $f(x)$ is irreducible). Over F_1 the polynomial $f(x)$ now has at least one linear factor, so that any other root of $f(x)$ satisfies an equation of degree at most $n - 1$ over F_1 . Adjoining such a root to F_1 we therefore obtain an extension of degree at most $n - 1$ of F_1 , etc. Using the multiplicativity of extension degrees, this proves

Proposition 26. A splitting field of a polynomial of degree n over F is of degree at most $n!$ over F .

As the examples above show, the degree of a splitting field may be smaller than $n!$. It will be proved later using Galois Theory that a “general” polynomial of degree n (in a well defined sense) over \mathbb{Q} has a splitting field of degree $n!$, so this may be viewed as the “generic” situation (although most of the interesting examples we shall consider have splitting fields of smaller degree).

Example: (Splitting Field of $x^n - 1$: Cyclotomic Fields)

Consider the splitting field of the polynomial $x^n - 1$ over \mathbb{Q} . The roots of this polynomial are called the n^{th} roots of unity.

Recall that every nonzero complex number $a + bi \in \mathbb{C}$ can be written uniquely in the form

$$re^{i\theta} = r(\cos \theta + i \sin \theta) \quad r > 0, \quad 0 \leq \theta < 2\pi$$

which is simply representing the point $a + bi$ in the complex plane in terms of polar coordinates: r is the distance of (a, b) from the origin and θ is the angle made with the real positive axis.

Over \mathbb{C} there are n distinct solutions of the equation $x^n = 1$, namely the elements

$$e^{2\pi ki/n} = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right)$$

for $k = 0, 1, \dots, n - 1$. These points are given geometrically by n equally spaced points starting with the point $(1, 0)$ (corresponding to $k = 0$) on a circle of radius 1 in the complex plane (see Figure 6). The fact that these are all n^{th} roots of unity is immediate, since

$$(e^{2\pi ki/n})^n = e^{(2\pi ki/n)n} = e^{2\pi ki} = 1.$$

It follows that \mathbb{C} contains a splitting field for $x^n - 1$ and we shall frequently view the splitting field for $x^n - 1$ over \mathbb{Q} as the field generated over \mathbb{Q} in \mathbb{C} by the numbers above.

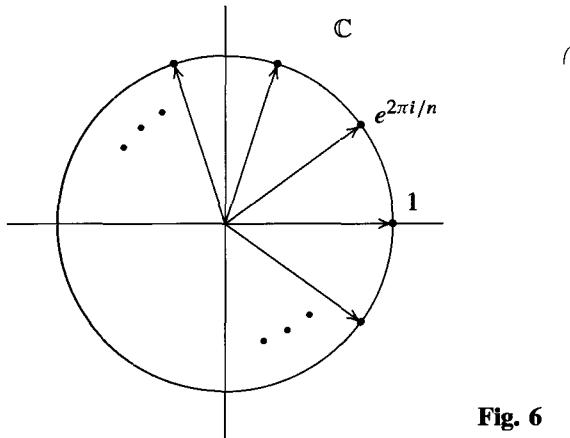


Fig. 6

In any abstract splitting field K/\mathbb{Q} for $x^n - 1$ the collection of n^{th} roots of unity form a group under multiplication since if $\alpha^n = 1$ and $\beta^n = 1$ then $(\alpha\beta)^n = 1$, so this subset of K^\times is closed under multiplication. It follows that this is a cyclic group (Proposition 18 of Chapter 9); we shall see that there are n distinct roots in K so it has order n .

Definition. A generator of the cyclic group of all n^{th} roots of unity is called a primitive n^{th} root of unity.

Let ζ_n denote a primitive n^{th} root of unity. The other primitive n^{th} roots of unity are then the elements ζ_n^a where $1 \leq a < n$ is an integer relatively prime to n , since these are the other generators for a cyclic group of order n . In particular there are precisely $\varphi(n)$ primitive n^{th} roots of unity, where $\varphi(n)$ denotes the Euler φ -function.

Over \mathbb{C} we can see all of this directly by letting

$$\zeta_n = e^{2\pi i/n}$$

(the first n^{th} root of unity counterclockwise from 1). Then all the other roots of unity are powers of ζ_n :

$$e^{2\pi k i/n} = \zeta_n^k$$

so that ζ_n is one possible generator for the multiplicative group of n^{th} roots of unity. When we view the roots of unity in \mathbb{C} we shall usually use ζ_n to denote this choice of a primitive n^{th} root of unity. The primitive roots of unity in \mathbb{C} for some small values of n are

$$\zeta_1 = 1$$

$$\zeta_2 = -1$$

$$\zeta_3 = \frac{-1 + i\sqrt{3}}{2}$$

$$\zeta_4 = i$$

$$\zeta_5 = \frac{\sqrt{5} - 1}{4} + i\left(\frac{\sqrt{10 + 2\sqrt{5}}}{4}\right)$$

$$\zeta_6 = \frac{1 + i\sqrt{3}}{2}$$

$$\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

(these formulas follow from the elementary geometry of n -gons and in any case can be verified directly by raising them to the appropriate power).

The splitting field of $x^n - 1$ over \mathbb{Q} is the field $\mathbb{Q}(\zeta_n)$ and this field is given a name:

Definition. The field $\mathbb{Q}(\zeta_n)$ is called the *cyclotomic field of n^{th} roots of unity*.

Determining the degree of this extension requires some analysis of the minimal polynomial of ζ_n over \mathbb{Q} and will be postponed until later (Section 6). One important special case which we have in fact already considered is when $n = p$ is a *prime*. In this case, we have the factorization

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$$

and since $\zeta_p \neq 1$ it follows that ζ_p is a root of the polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

which we showed was irreducible in Section 9.4. It follows that $\Phi_p(x)$ is the minimal polynomial of ζ_p over \mathbb{Q} , so that

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1.$$

We shall see later that in general $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where $\varphi(n)$ is the Euler phi-function of n (so that $\varphi(p) = p - 1$).

Example: (Splitting Field of $x^p - 2$, p a prime)

Let p be a prime and consider the splitting field of $x^p - 2$. If α is a root of this equation, i.e., $\alpha^p = 2$, then $(\zeta \alpha)^p = 2$ where ζ is any p^{th} root of unity. Hence the solutions of this equation are

$$\zeta \sqrt[p]{2}, \quad \zeta \text{ a } p^{\text{th}} \text{ root of unity}$$

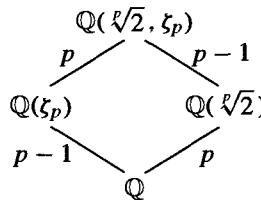
where as usual the symbol $\sqrt[p]{2}$ denotes the positive real p^{th} root of 2 if we wish to view these elements as complex numbers, and denotes any one solution of $x^p = 2$ if we view these roots abstractly. Since the ratio of the two solutions $\zeta_p \sqrt[p]{2}$ and $\sqrt[p]{2}$ for ζ_p a primitive p^{th} root of unity is just ζ_p , the splitting field of $x^p - 2$ over \mathbb{Q} contains $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$. On the other hand, all the roots above lie in this field, so that the splitting field is precisely

$$\mathbb{Q}(\sqrt[p]{2}, \zeta_p).$$

This field contains the cyclotomic field of p^{th} roots of unity and is generated over it by $\sqrt[p]{2}$, hence is an extension of degree at most p . It follows that the degree of this extension over \mathbb{Q} is $\leq p(p-1)$. Since both $\mathbb{Q}(\sqrt[p]{2})$ and $\mathbb{Q}(\zeta_p)$ are subfields, the degree of the extension over \mathbb{Q} is divisible by p and by $p-1$. Since these two numbers are relatively prime it follows that the extension degree is divisible by $p(p-1)$ so that we must have

$$[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] = p(p-1)$$

(this is Corollary 22). Note in particular that we have proved $x^p - 2$ remains irreducible over $\mathbb{Q}(\zeta_p)$, which is not at all obvious. We have the following diagram of known subfields:



The special case $p = 3$ was Example 3 above, where we simply indicated the 3rd roots of unity explicitly.

We now return to the problem of proving it makes no difference how the splitting field of a polynomial $f(x)$ over a field F is constructed. As in Theorem 8 it is convenient to state the result for an arbitrary isomorphism $\varphi : F \xrightarrow{\sim} F'$ between two fields.

Theorem 27. Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ be a polynomial and let $f'(x) \in F'[x]$ be the polynomial obtained by applying φ to the coefficients of $f(x)$. Let E be a splitting field for $f(x)$ over F and let E' be a splitting field for $f'(x)$ over F' . Then the isomorphism φ extends to an isomorphism $\sigma : E \xrightarrow{\sim} E'$, i.e., σ restricted to F is the isomorphism φ :

$$\begin{array}{ccc} \sigma : & E & \xrightarrow{\sim} E' \\ & | & | \\ \varphi : & F & \xrightarrow{\sim} F' \end{array}$$

Proof: We shall proceed by induction on the degree n of $f(x)$. As in the discussion before Theorem 8, recall that an isomorphism φ from one field F to another field

F' induces a natural isomorphism between the polynomial rings $F[x]$ and $F'[x]$. In particular, if $f(x)$ and $f'(x)$ correspond to one another under this isomorphism then the irreducible factors of $f(x)$ in $F[x]$ correspond to the irreducible factors of $f'(x)$ in $F'[x]$.

If $f(x)$ has all its roots in F then $f(x)$ splits completely in $F[x]$ and $f'(x)$ splits completely in $F'[x]$ (with its linear factors being the images of the linear factors for $f(x)$). Hence $E = F$ and $E' = F'$, and in this case we may take $\sigma = \varphi$. This shows the result is true for $n = 1$ and in the case where all the irreducible factors of $f(x)$ have degree 1.

Assume now by induction that the theorem has been proved for any field F , isomorphism φ , and polynomial $f(x) \in F[x]$ of degree $< n$. Let $p(x)$ be an irreducible factor of $f(x)$ in $F[x]$ of degree at least 2 and let $p'(x)$ be the corresponding irreducible factor of $f'(x)$ in $F'[x]$. If $\alpha \in E$ is a root of $p(x)$ and $\beta \in E'$ is a root of $p'(x)$, then by Theorem 8 we can extend φ to an isomorphism $\sigma' : F(\alpha) \xrightarrow{\sim} F'(\beta)$:

$$\begin{array}{ccc} \sigma' : & F(\alpha) & \xrightarrow{\sim} F'(\beta) \\ & | & | \\ \varphi : & F & \xrightarrow{\sim} F'. \end{array}$$

Let $F_1 = F(\alpha)$, $F'_1 = F'(\beta)$, so that we have the isomorphism $\sigma' : F_1 \xrightarrow{\sim} F'_1$. We have $f(x) = (x - \alpha)f_1(x)$ over F_1 where $f_1(x)$ has degree $n - 1$ and $f'(x) = (x - \beta)f'_1(x)$. The field E is a splitting field for $f_1(x)$ over F_1 : all the roots of $f_1(x)$ are in E and if they were contained in any smaller extension L containing F_1 , then, since F_1 contains α , L would also contain all the roots of $f(x)$, which would contradict the minimality of E as the splitting field of $f(x)$ over F . Similarly E' is a splitting field for $f'_1(x)$ over F'_1 . Since the degrees of $f_1(x)$ and $f'_1(x)$ are less than n , by induction there exists a map $\sigma : E \xrightarrow{\sim} E'$ extending the isomorphism $\sigma' : F_1 \xrightarrow{\sim} F'_1$. This gives the extended diagram:

$$\begin{array}{ccc} \sigma : & E & \xrightarrow{\sim} E' \\ & | & | \\ \sigma' : & F_1 & \xrightarrow{\sim} F'_1 \\ & | & | \\ \varphi : & F & \xrightarrow{\sim} F'. \end{array}$$

Then as the diagram indicates, σ restricted to F_1 is the isomorphism σ' , so in particular σ restricted to F is σ' restricted to F , which is φ , showing that σ is an extension of φ , completing the proof.

Corollary 28. (Uniqueness of Splitting Fields) Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are isomorphic.

Proof: Take φ to be the identity mapping from F to itself and E and E' to be two splitting fields for $f(x) (= f'(x))$.

As we mentioned before, this result justifies the terminology of *the* splitting field for $f(x)$ over F , since any two are isomorphic. Splitting fields play a natural role in