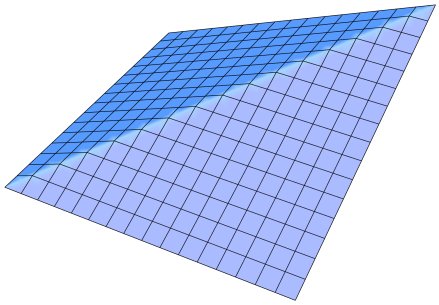


# PMATH 348: Fields and Galois Theory

Prof. Frank Zorzitto • Winter 2015 • University of Waterloo
TWF 9:30–10:20 in B2 350

---

Transcribed, LaTeXed, and edited by Rob Zimmerman

**Note:** These are personal lecture notes, not official course materials. They may contain errors (which by default you should attribute to me, Rob Zimmerman, rather than the course instructor). The permanent home of these — and all of my other lecture notes — is https://rob-zimmerman.github.io/coursenotes.

## Contents

# 1. Irreducible Polynomials and Algebraic Extensions

## Fields and Galois Theory

**Definition 0.1** A **field** $F$ is a commutative ring in which every nonzero element has an inverse, and $0 \neq 1$.

**Example 0.2** Examples of fields include $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. The rings $\mathbb{Z}$ and $\mathbb{N} = \{1, 2, 3, \dots\}$ are not fields.

**Example 0.3** Another example is $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$, where $p$ is prime and $\langle p \rangle$ is the ideal generated by $p$. Here

$$\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\},$$

with addition and multiplication performed modulo $p$.

If $F$ is a field, then $F[X]$ is the ring of polynomials in the indeterminate $X$, and $F(X)$ is the field of rational functions $(f(X))/(g(X))$, where $f(X), g(X) \in F[X]$ and $g(X) \neq 0$.

Henceforth, $F$ will denote an arbitrary field and $F[X]$ will denote the polynomial ring over $F$ in the indeterminate $X$.

## Ideals in $F[X]$

If $f, g \in F[X]$ and $g \neq 0$, then Euclidean division says that there exist unique $q, r \in F[X]$ such that

$$f = gq + r, \quad \text{where } 0 \leq \deg r < \deg g \text{ or } r = 0.$$

This can be used to show that every ideal $J$ in $F[X]$ is principal, that is,

$$J = \langle h \rangle = \{hk : k \in F[X]\}.$$

**Definition 0.4** The polynomial $h$ that satisfies $J = \langle h \rangle$ is called a **generator** of the ideal $J$.

Any two generators of $J$ are constant multiples of each other. If we insist that $h$ be monic, then the generator of $J$ is unique. In particular, if $f, g \in F[X]$, then the ideal

$$\langle f, g \rangle = \{fk + gl : k, l \in F[X]\}$$

has a unique monic generator $h$, so $\langle f, g \rangle = \langle h \rangle$. This $h$ is the greatest common divisor of $f$ and $g$. So $h = \gcd(f, g)$ if and only if $h$ is monic and

$$f = hs, \qquad g = ht, \qquad \text{and} \qquad h = fk + gl$$

for some $s, t, k, l \in F[X]$.

## Roots

If $a \in F$, we have the substitution homomorphism

$$\begin{aligned} \varphi_a : F[X] &\longrightarrow F \\ g(X) &\longmapsto g(a). \end{aligned}$$

The polynomial $X - a$ lies in the ideal $\ker \varphi_a$. Since $\ker \varphi_a = \langle h \rangle$ for some unique monic $h \in F[X]$, we have $h \mid (X - a)$ in $F[X]$. Since $h$ is monic and nonconstant while $X - a$ is linear, we get $h = X - a$. So $\ker \varphi_a = \langle X - a \rangle$.

**Definition 0.5** An element $a \in F$ is a **root** of $f \in F[X]$ if $f(a) = 0$, that is, if $f \in \ker \varphi_a$.

This gives us our first result.

**Proposition 0.6 (Factor theorem)** An element $a \in F$ is a root of $f \in F[X]$ if and only if $(X - a) \mid f$ in $F[X]$.

Here is another important fact.

**Proposition 0.7** If $f \in F[X]$, $f \neq 0$, and $n = \deg f$, then $f$ has at most $n$ roots.

**Proof.** We argue by induction on $n$. If $\deg f = 0$, then $f$ is constant and has 0 roots. Suppose every polynomial of degree $n-1$ has at most $n-1$ roots, and consider $f$ of degree $n$. If $f$ has no roots, then clearly $0 \leq n$. Otherwise, pick a root $a$ of $f$. Then $f = (X - a)g$ for some $g \in F[X]$ of degree $n - 1$. If $b$ is another root of $f$ (that is, $f(b) = 0$ and $b \neq a$), then

$$f(b) = (b - a)g(b).$$

Since $b - a \neq 0$, this forces $g(b) = 0$. By the inductive assumption, $g$ has at most $n - 1$ roots. Thus $f$ has the root $a$, plus at most $n - 1$ additional roots. Therefore $f$ has at most $n$ roots. □

## Finite Groups of Units in a Field

Recall that the set $F^* = \{a \in F : a \neq 0\}$ is an abelian group under multiplication, sometimes called the **group of units** of $F$. Such an $F^*$ might contain finite subgroups. For example, $\mathbb{Z}_p^*$ is

finite with $p-1$ elements. Also, in $\mathbb{C}$, for every positive integer $n$, the set

$$T_n = \{z \in \mathbb{C} : z^n = 1\}$$

is a subgroup of $\mathbb{C}^*$ of order $n$.

In fact, if $\zeta = e^{2\pi i/n}$, then

$$T_n = \{1, \zeta, \zeta^2, \zeta^3, \ldots, \zeta^{n-1}\}.$$

Figure 1 displays these roots on the unit circle.

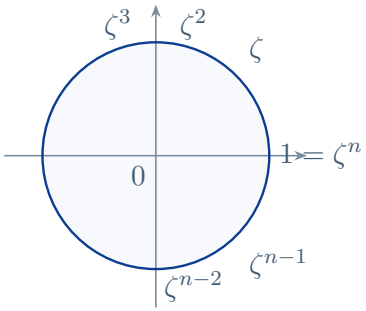



FIGURE 1

This is the group of ***n*th roots of unity**. Notice that $T_n$ is cyclic.

**Theorem 0.8** If $G$ is a finite subgroup of $F^*$, then $G$ is cyclic.

**Proof.** We need a refresher on finite abelian groups. If $G$ is such a group and $p$ is a prime that divides the order of $G$, Cauchy's theorem says that $G$ has an element of order $p$. Then the set

$$G_p = \{x \in G : x^{p^k} = 1 \text{ for some exponent } p^k\}$$

is a subgroup of $G$. Some call this a primary subgroup of $G$. Every finite abelian group is isomorphic to the direct product of its primary subgroups:

$$G \cong G_{p_1} \times G_{p_2} \times \cdots \times G_{p_k},$$

where the $p_j$ are the primes dividing the order of $G$. This is called the primary decomposition of $G$. If each $G_{p_j}$ is cyclic, the Chinese remainder theorem says that $G$ is cyclic. We recall this

as $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ when $m$ and $n$ are coprime (using addition here). So, to show that our finite subgroup $G$ of $F^*$ is cyclic, it suffices to treat the case where $G$ is a $p$-group for one prime $p$. Let $x$ be an element of $G$ whose order $p^k$ is as large as possible. The order of every $y$ in $G$ is $p^j$ for some $j \leq k$. So for every $y$ in $G$, we have

$$y^{p^k} = \left(y^{p^j}\right)^{p^{k-j}} = 1^{p^{k-j}} = 1.$$

Hence every $y$ in $G$ is a root of $X^{p^k} - 1$. By the degree bound on the number of roots, the order of $G$ is at most $p^k$. Since $p^k$ is the order of $x$, it divides the order of $G$. Thus $p^k = |G|$. This means that $x$ generates $G$. □

**Corollary 0.9** If $F$ is a finite field (for example, $F = \mathbb{Z}_p$ for any prime $p$), then $F^*$ is a cyclic group.

This fact, applied to very large finite fields, is the basis for the famous encryption protocol known as the **Diffie–Hellman scheme**.

Also recall that if $G$ is a finite cyclic group of order $n$ with $x$ as a generator, then the other generators of $G$ are the powers $x^k$ where $k$ is coprime with $n$. Hence the number of generators of $G$ is $\phi(n)$, the number of integers $k$ from 0 to $n-1$ that are coprime with $n$. This function $\phi$ is Euler's $\phi$-function.

Another thing worth remembering about cyclic groups $G$ is that every subgroup of $G$ is also cyclic. If $G$ has order $n$ with generator $x$, then the groups generated by $x^d$, where $d \mid n$, give all subgroups of $G$.

## Irreducibility

**Definition 0.10** If $f \in F[X]$ is a nonconstant polynomial (that is, $\deg f \geq 1$), we say that $f$ is **reducible** (or **reducible over $F$**) in $F[X]$ when $f = gh$ for some $g, h \in F[X]$ with both $\deg g \geq 1$ and $\deg h \geq 1$.

If, on the other hand, the only way to factor $f = gh$ in $F[X]$ is for one of $g$ or $h$ to be constant (that is, $\deg g = 0$ or $\deg h = 0$), then $f$ is **irreducible** in $F[X]$. Equivalently, $f$ is **irreducible over $F$**.

**Example 0.11** $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$ is reducible in $\mathbb{Q}[X]$.

**Example 0.12** $X^2 + 1$ is irreducible over $\mathbb{Q}$, but

$$X^2 + 1 = (X + i)(X - i)$$

is reducible over $\mathbb{C}$.

Every polynomial in $F[X]$ of degree at least 1 can be written as a product of irreducible polynomials, and the irreducible factors are unique up to nonzero scalar multiples. For example,

$$X^2 + 1 = (2X + 2i)\left(\frac{1}{2}X - \frac{1}{2}i\right) = (X + i)(X - i)$$

does not count as different factorizations of $X^2 + 1$.

Constant polynomials (that is, degree 0) are not part of reducibility questions.

Here are some basic facts:

- Linear polynomials $aX + b$ with $a \neq 0$ are irreducible.
- Quadratics $aX^2 + bX + c$ and cubics $aX^3 + bX^2 + cX + d$ are irreducible over $F$ if and only if they have no root in $F$. Use the factor theorem and the fact that $\deg f = 2$ or 3.
- If $\deg f \geq 4$, then $f$ may be reducible over $F$ and still have no root in $F$.

**Example 0.13** $X^4 - X^2 - 2 = (X^2 + 1)(X^2 - 2)$ is reducible over $\mathbb{Q}$ but has no root in $\mathbb{Q}$.

- In $\mathbb{C}[X]$, the only irreducible polynomials are linear, by the fundamental theorem of algebra.
- In $\mathbb{R}[X]$, a polynomial is irreducible if and only if it is linear, or it has the form $aX^2 + bX + c$ with $b^2 - 4ac < 0$.
- In $\mathbb{Z}_p[X]$, it is not obvious that irreducibles of arbitrary degree exist. But they do!

In $\mathbb{Q}[X]$, it can be hard to decide when a polynomial is irreducible, so we need a few tools.

For one, if $f \in \mathbb{Q}[X]$, there is an integer $c$ such that $cf \in \mathbb{Z}[X]$. This self-evident process is called

**clearing denominators**.

**Example 0.14** If $f = 2/3X^2 + 1/4X - 5 \in \mathbb{Q}[X]$, then $12f \in \mathbb{Z}[X]$.

Since rescaling has no effect on reducibility over $\mathbb{Q}$ (or over any field), we only need to worry about polynomials in $\mathbb{Z}[X]$. This brings **Gauss' lemma** into play: if $f \in \mathbb{Z}[X]$ and $f = gh$ where $g, h \in \mathbb{Q}[X]$, then there is a scalar $c \in \mathbb{Q}$ such that $cg \in \mathbb{Z}[X]$ and $1/ch \in \mathbb{Z}[X]$. Then, of course,

$$f = (cg)\left(\frac{1}{c}h\right)$$

is a factorization of $f$ in $\mathbb{Z}[X]$. It follows from Gauss' lemma that if $f \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Z}$, then $f$ remains irreducible over $\mathbb{Q}$.

## The Rational Root Test

If $f \in \mathbb{Z}[X]$, our first job might be to check whether $f$ has any roots in $\mathbb{Q}$, and thereby identify linear factors.

**Proposition 0.15 (Rational root test)** If $f = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ and $r = c/d$ is a rational root of $f$, where $c$ and $d$ are coprime integers, then $c \mid a_0$ and $d \mid a_n$.

**Proof.** We have

$$a_n\left(\frac{c}{d}\right)^n + \cdots + a_1\left(\frac{c}{d}\right) + a_0 = 0.$$

Thus

$$a_nc^n + a_{n-1}c^{n-1}d + \cdots + a_1cd^{n-1} + a_0d^n = 0.$$

Clearly $c \mid a_0d^n$, and since $c$ and $d$ are coprime, we get $c \mid a_0$. Likewise, $d \mid a_nc^n$, and since $c$ and $d$ are coprime, we get $d \mid a_n$. □

This reduces the search for rational roots from the infinite set $\mathbb{Q}$ to a finite process.

**Example 0.16** We can check whether $f = 2X^3 + X^2 - 1$ has any rational roots. Any such root $c/d$ in lowest terms must satisfy $c \mid 1$ and $d \mid 2$.

The only possibilities are $\pm 1/2, \pm 1$. By substitution, none of these is a root. So $f$ has no rational root. Since $f$ is cubic, it must be irreducible over $\mathbb{Q}$.

## Testing Irreducibility by Collapsing Modulo $p$

For each prime $p$, the familiar residue map

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow \mathbb{Z}_p \\ n &\longmapsto \bar{n} \end{aligned}$$

sends $n$ to its residue modulo $p$. This lifts to a ring homomorphism

$$\begin{aligned} \varphi : \mathbb{Z}[X] &\longrightarrow \mathbb{Z}_p[X] \\ a_n X^n + \cdots + a_1 X + a_0 &\longmapsto \bar{a}_n X^n + \cdots + \bar{a}_1 X + \bar{a}_0. \end{aligned}$$

This process is known as **collapsing** coefficients modulo $p$.

**Example 0.17** The polynomial $7X^4 + 3X^3 + 14X^2 - 8X - 10$ collapses modulo 5 to $\bar{7}X^4 + \bar{3}X^3 + \bar{14}X^2 + \overline{-8}X + \overline{-10}$, which simplifies to $\bar{2}X^4 + \bar{3}X^3 + \bar{4}X^2 + \bar{2}X + \bar{0}$, and we usually write this as $2X^4 + 3X^3 + 4X^2 + 2X$.

**Proposition 0.18** If $f = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ and $p$ is a prime such that $p \nmid a_n$ and the collapsed polynomial $\varphi(f)$ in $\mathbb{Z}_p[X]$ is irreducible, then $f$ is irreducible in $\mathbb{Q}[X]$.

**Proof.** Suppose $f = gh$ with $g, h \in \mathbb{Q}[X]$, $\deg g \geq 1$, and $\deg h \geq 1$, and seek a contradiction. By Gauss' lemma, we may assume $g, h \in \mathbb{Z}[X]$. Then

$$\varphi(f) = \varphi(gh) = \varphi(g)\varphi(h)$$

gives a factorization of $\varphi(f)$ in $\mathbb{Z}_p[X]$. The condition $p \nmid a_n$ shows that $\deg \varphi(f) = \deg f$. So

$$\deg g + \deg h = \deg f = \deg \varphi(f) = \deg \varphi(g) + \deg \varphi(h).$$

But clearly $\deg \varphi(g) \leq \deg g$ and $\deg \varphi(h) \leq \deg h$. Thus $\deg \varphi(g) = \deg g \geq 1$ and $\deg \varphi(h) = \deg h \geq 1$, which contradicts the irreducibility of $\varphi(f)$ in $\mathbb{Z}_p[X]$. □

**Example 0.19** Take $f = 3X^4 - 6X^3 + 10X^2 - 5X + 9$ in $\mathbb{Z}[X]$. Using $p = 2$, $f$ collapses to $\varphi(f) = X^4 + X + 1$ in $\mathbb{Z}_2[X]$.

We now check that $\varphi(f)$ is irreducible in $\mathbb{Z}_2[X]$. Certainly 0 and 1 are not roots of $\varphi(f)$ in $\mathbb{Z}_2$. So $\varphi(f)$ has no linear factors.

Could $\varphi(f)$ have quadratic factors? Suppose

$$X^4 + X + 1 = (X^2 + aX + b)(X^2 + cX + d)$$

with $a, b, c, d \in \mathbb{Z}_2$.

Comparing coefficients gives

$$X^0 \implies bd = 1 \tag{1}$$
$$X^1 \implies ad + bc = 1 \tag{2}$$
$$X^2 \implies ac + b + d = 0 \tag{3}$$
$$X^3 \implies a + c = 0 \tag{4}$$

Now (1) gives $b = d = 1$. Then (2) gives $a + c = 1$, which contradicts (4).

Thus $\varphi(f)$ is irreducible in $\mathbb{Z}_2[X]$, and therefore $f$ is irreducible in $\mathbb{Q}[X]$.

Here is a famous irreducibility test.

**Proposition 0.20 (Eisenstein's criterion)** If $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ and $p$ is a prime such that the following hold:

1. $p \nmid a_n$.
2. $p \mid a_j$ for all other $a_j$.
3. $p^2 \nmid a_0$.

then $f$ is irreducible over $\mathbb{Q}$.

**Proof.** Suppose, on the contrary, that $f = gh$ where $g, h \in \mathbb{Q}[X]$ with $\deg g \geq 1$ and $\deg h \geq 1$.

By Gauss' lemma, we can take $g, h \in \mathbb{Z}[X]$. Collapse this factorization modulo $p$ to get

$$\varphi(f) = \varphi(g)\varphi(h), \quad \text{in } \mathbb{Z}_p[X].$$

Since $p \mid a_j$ for every $a_j$ except $a_n$, we get

$$\varphi(f) = \overline{a}_n X^n,$$

where $\overline{a}_n$ is the residue of $a_n$ in $\mathbb{Z}_p$. We also have

$$n = \deg f = \deg \varphi(f) = \deg \varphi(g) + \deg \varphi(h),$$

and since $\deg \varphi(g) \leq \deg g$ and $\deg \varphi(h) \leq \deg h$, we conclude $\deg \varphi(g) = \deg g \geq 1$ and $\deg \varphi(h) = \deg h \geq 1$. Write $g = b_k X^k + \cdots + b_0$ where $k = \deg g$, and $h = c_\ell X^\ell + \cdots + c_0$ where $\ell = \deg h$. The unique factorization of $\varphi(f) = \overline{a}_n X^n$ in $\mathbb{Z}_p[X]$ forces $\varphi(g) = \overline{b}_k X^k$ and $\varphi(h) = \overline{c}_\ell X^\ell$. In particular, $\overline{b}_0 = \overline{c}_0 = 0$ in $\mathbb{Z}_p$. This says $p \mid b_0$ and $p \mid c_0$, which implies $p^2 \mid b_0 c_0 = a_0$, contrary to the assumption that $p^2 \nmid a_0$. □

**Example 0.21** $f = 10X^7 - 6X^3 + 27X + 12$ is irreducible in $\mathbb{Q}[X]$ by Eisenstein's criterion using the prime $p = 3$.

Here is an important example:

**Example 0.22** For any prime $p$, the $p$th cyclotomic polynomial is the unique monic polynomial $\Phi_p(X)$ in $\mathbb{Z}[X]$ such that

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

Is that second factor irreducible in $\mathbb{Q}[X]$? It does not immediately fit Eisenstein's criterion, but a substitution trick helps. Let

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Take $f(X) = \Phi_p(X + 1)$. Then

$$\begin{aligned} f(X) &= \frac{(X+1)^p - 1}{(X+1) - 1} \\ &= \frac{(X+1)^p - 1}{X} \end{aligned}$$

$$= \frac{X^p + \binom{p}{1}X^{p-1} + \binom{p}{2}X^{p-2} + \binom{p}{3}X^{p-3} + \cdots + \binom{p}{p-1}X}{X}$$
$$= X^{p-1} + \binom{p}{1}X^{p-2} + \binom{p}{2}X^{p-3} + \binom{p}{3}X^{p-4} + \cdots + \binom{p}{p-1}.$$

The binomial coefficients $\binom{p}{k}$ are all divisible by $p$. But the constant term $\binom{p}{p-1} = p$ is not divisible by $p^2$. So by Eisenstein's criterion, $f(X)$ is irreducible in $\mathbb{Q}[X]$.

If we had $\Phi_p(X) = g(X)h(X)$ for some $g, h \in \mathbb{Q}[X]$ of positive degree, then we would also get

$$f(X) = \Phi_p(X+1) = g(X+1)h(X+1),$$

where $g(X+1)$ and $h(X+1)$ have the same degrees as $g(X)$ and $h(X)$. Since this is impossible, it follows that $\Phi_p(X)$ is irreducible in $\mathbb{Q}[X]$.

**Warning** The above does not hold when $p$ is not prime! For example, $X^4 - 1$ factors as $(X-1)(X+1)(X^2+1)$, and $X^6 - 1$ factors as $(X-1)(X+1)(X^2+X+1)(X^2-X+1)$.

## Irreducible Polynomials Make Fields

What are irreducible polynomials good for, anyway? Recall that $f \in F[X]$ is irreducible if and only if the ideal $\langle f \rangle$ is maximal (that is, there are no ideals properly between $\langle f \rangle$ and $F[X]$), which is equivalent to the quotient ring $F[X]/\langle f \rangle$ being a field. Without returning to that theory, here is a *practical* way to get the inverse of every nonzero element in $F[X]/\langle f \rangle$ when $f$ is irreducible.

Let $g + \langle f \rangle$ be a nonzero element in $F[X]/\langle f \rangle$. Then $f \nmid g$ in $F[X]$, and since $f$ is irreducible, we get $\gcd(f, g) = 1$. By the Euclidean algorithm in $F[X]$, there exist $k, h \in F[X]$ such that

$$1 = gk + fh.$$

Then

$$1 + \langle f \rangle = (g + \langle f \rangle)(k + \langle f \rangle) + \underbrace{(f + \langle f \rangle)}_{=0}(h + \langle f \rangle)$$
$$= (g + \langle f \rangle)(k + \langle f \rangle),$$

so $k + \langle f \rangle$ is $(g + \langle f \rangle)^{-1}$.

**Example 0.23** By Eisenstein's criterion, using $p = 2$, we see that $f = X^3 - 2$ is irreducible in $\mathbb{Q}[X]$. Thus $\mathbb{Q}[X]/\langle f \rangle$ is a field. We can find $(X^2 + X + \langle f \rangle)^{-1}$ in this field.

We need $k, h \in \mathbb{Q}[X]$ such that

$$(X^2 + X)k + (X^3 - 2)h = 1 = \gcd(X^2 + X, X^3 - 2).$$

The Euclidean algorithm gives

$$\begin{array}{r|l} & X - 1 \\ \hline X^2 + X & X^3 \quad\quad - 2 \\ & -X^3 - X^2 \\ \hline & \quad -X^2 \\ & \quad X^2 + X \\ \hline & \quad\quad X - 2 \end{array}$$

so

$$X^3 - 2 = (X^2 + X)(X - 1) + (X - 2). \tag{1}$$

Next,

$$\begin{array}{r|l} & X + 3 \\ \hline X - 2 & X^2 \ + X \\ & -X^2 + 2X \\ \hline & \quad 3X \\ & \quad -3X + 6 \\ \hline & \quad\quad 6 \end{array}$$

so

$$X^2 + X = (X - 2)(X + 3) + 6. \tag{2}$$

Equation (2) gives

$$6 = (X^2 + X) - (X - 2)(X + 3). \tag{3}$$

and (1) gives

$$X - 2 = (X^3 - 2) - (X^2 + X)(X - 1). \tag{4}$$

Plug (4) into (3):

$$\begin{aligned} 6 &= (X^2+X) - \left[(X^3-2) - (X^2+X)(X-1)\right](X+3) \\ &= (X^2+X)\left(1+(X-1)(X+3)\right) - (X^3-2)(X+3) \\ &= (X^2+X)(\underbrace{X^2+2X-2}_{k}) + (X^3-2)(\underbrace{-(X+3)}_{h}). \end{aligned}$$

This tells us that

$$(X^2+X+\langle f\rangle)(X^2+2X-2+\langle f\rangle) = 6+\langle f\rangle.$$

Therefore,

$$(X^2+X+\langle f\rangle)^{-1} = \frac{1}{6}X^2+\frac{1}{3}X-\frac{1}{3}+\langle f\rangle.$$

## 2. Algebraic Extensions

Henceforth, the letters $E, F, K, L$ will stand *exclusively* for fields. If $F$ is a subfield of $K$, we also say that $K$ is a **field extension** of $F$.

**Example 0.24** $\mathbb{C}$ extends $\mathbb{R}$ which extends $\mathbb{Q}$. $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ extends $\mathbb{Q}$.

### The Characteristic of a Field

If $K$ is a field, there is the ring homomorphism

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow K \\ j &\longmapsto j \cdot 1 \quad (\text{This } 1 \in K) \end{aligned}$$

The kernel $\ker\varphi$ is an ideal of $\mathbb{Z}$. So there is an integer $n$ such that $\ker\varphi = \langle n\rangle = \{nk : k \in \mathbb{Z}\}$. The generator $n$ can vary only up to its sign.

**Definition 0.25** The unique nonnegative generator $n$ of $\ker\varphi$ is called the **characteristic** of $K$.

If $n = 0$, then $\varphi$ is one-to-one, and thereby $\varphi(\mathbb{Z}) \cong \mathbb{Z}$. It makes good sense to identify $\mathbb{Z}$ with its isomorphic copy $\varphi(\mathbb{Z})$. In this way, all fields $K$ of characteristic 0 contain $\mathbb{Z}$ as a subring. Since

$K$ is a field, it also contains $\mathbb{Q}$. Thus fields of characteristic 0 are extensions of $\mathbb{Q}$.

If $n > 0$, the first isomorphism theorem gives $\mathbb{Z}/\langle n\rangle \cong \varphi(\mathbb{Z})$, which is an integral domain inside $K$. So the ideal $\langle n\rangle$ is a prime ideal, which means that $n$ is a prime. Habit forces us to rename $n$ as $p$. But then $\mathbb{Z}/\langle p\rangle$ is the usual field $\mathbb{Z}_p$ of residues mod $p$. By making the obvious identification of $\mathbb{Z}_p$ with $\varphi(\mathbb{Z})$, we see that fields of prime characteristic are those that extend $\mathbb{Z}_p$.

**Remark 0.26** Many authors denote $\mathbb{Z}_p$ by $\mathbb{F}_p$ and also by $GF(p)$, but we will stick with $\mathbb{Z}_p$.

## The Degree of An Extension

If $K$ is a field extension of $F$, then $K$ is also a **vector space** over the field $F$. We know how to add inside $K$, and if $\alpha$ in $K$ is a "vector" and $\lambda$ in $F$ is a "scalar", then $\lambda\alpha$ in $K$ is our rescaled vector.

**Definition 0.27** If the dimension of $K$ over $F$ is finite, we say that $K$ is a **finite extension** of $F$, and $\dim_F(K)$ is usually denoted by $[K : F]$. It is common to call $[K : F]$ the **degree** of the extension $K$ over $F$.

**Example 0.28** $[\mathbb{C} : \mathbb{R}] = 2$ since a basis for $\mathbb{C}$ as a vector space over $\mathbb{R}$ is $\{1, i\}$. Also, $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$ with $\{1, \sqrt{2}\}$ being a basis for $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$.

Here is a quick and easy application of this notion of degree:

**Proposition 0.29** If $F$ is a finite field, then the number of elements in $F$ is $p^n$ where the prime $p$ is the characteristic of $F$ and $n$ is a positive integer.

**Proof.** Since $F$ is finite, it must extend $\mathbb{Z}_p$ for some prime $p$. The degree $[F : \mathbb{Z}_p]$ has to be finite as well. If $\alpha_1, \ldots, \alpha_n$ is a basis for $F$ over $\mathbb{Z}_p$, then every element $\alpha$ of $F$ takes the form

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$$

where the $a_j$ in $\mathbb{Z}_p$ are uniquely determined by $\alpha$. Each $a_j$ has $p$ possibilities. Thus $\alpha$ has $p^n$ possibilities. □

## Algebraic Elements in an Extension

**Definition 0.30** If $K$ extends $F$ and $\alpha \in K$, we say that $\alpha$ is **algebraic** over $F$ when there is a nonzero polynomial $f \in F[X]$ such that $f(\alpha) = 0$.

**Example 0.31** $i$ is algebraic over $\mathbb{Q}$ because $f = X^2 + 1$ gives $f(i) = i^2 + 1 = 0$, and $\zeta = e^{2\pi i/5}$ in $\mathbb{C}$ is algebraic over $\mathbb{Q}$ because $f = X^5 - 1$ gives $f(\zeta) = 0$.

Every $\alpha \in F$ is algebraic over $F$ using $f = X - \alpha$ in $F[X]$.

**Definition 0.32** If there is no nonzero polynomial in $F[X]$ for which $\alpha$ is a root, we say that $\alpha$ is **transcendental** over $F$.

For example, $e, \pi$ and $\sum_{n=1}^{\infty} 1/(10^{n!})$ are transcendental over $\mathbb{Q}$. But alas, we must leave the proofs for another day.

**Proposition 0.33** If $K$ is a finite extension of $F$, then every $\alpha \in K$ is algebraic over $F$.

**Proof.** If $\alpha \in K$, the powers $1, \alpha, \alpha^2, \ldots, \alpha^n$ become linearly dependent over $F$ once $n \geq [K : F]$. Then a nontrivial combination

$$a_0 \cdot 1 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

where the $a_j \in F$ are not all zero. Thus $\alpha$ is a root of the nonzero polynomial $a_0 + a_1X + \cdots + a_nX^n \in F[X]$. □

**Example 0.34** Every $\alpha \in \mathbb{Q}[\sqrt{2}]$ is algebraic over $\mathbb{Q}$ because $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2 < \infty$.

If $K$ extends $F$, each $\alpha \in K$ gives rise to the substitution map:

$$\begin{aligned} \varphi_\alpha : F[X] &\longrightarrow K \\ f(X) &\longmapsto f(\alpha). \end{aligned}$$

This is a ring homomorphism.

**Example 0.35** $\alpha = \sqrt{2}$ in $\mathbb{R}$ gives $\varphi_{\sqrt{2}} : \mathbb{Q}[X] \to \mathbb{R}$, where, for instance:

$$\begin{aligned}\varphi_{\sqrt{2}} : 3X^4 - \frac{1}{7}X^3 + 2X^2 - \frac{5}{9} &\mapsto 3(\sqrt{2})^4 - \frac{1}{7}(\sqrt{2})^3 + 2(\sqrt{2})^2 - \frac{5}{9} \\ &= 12 - \frac{2}{7}\sqrt{2} + 4 - \frac{5}{9} \\ &= \frac{139}{9} - \frac{2}{7}\sqrt{2}.\end{aligned}$$

**Example 0.36** With $\alpha = \pi$ in $\mathbb{R}$ and $\varphi_\pi : \mathbb{Q}[X] \to \mathbb{R}$, we get

$$\varphi_\pi(1/2X^3 - 9X^2 + 10) = 1/2\pi^3 - 9\pi^2 + 10.$$

The image $\operatorname{im} \varphi_\alpha = \varphi_\alpha(F[X])$ is the subring of $K$ consisting of all expressions of the type $\sum_j a_j \alpha^j$ where $a_j \in F$. These are "polynomials in $\alpha$." This image is the smallest subring of $K$ that contains $F$ and $\alpha$. The usual notation for $\operatorname{im} \varphi_\alpha$ is $F[\alpha]$ and is called the ring formed by **adjoining** $\alpha$ to $F$.

**Example 0.37** With $\alpha = \sqrt{2}$ in $\mathbb{R}$ as an extension of $\mathbb{Q}$ we get

$$\mathbb{Q}[\sqrt{2}] = \{a_0 + a_1\sqrt{2} + \cdots + a_n(\sqrt{2})^n : n \geq 0 \text{ and } a_j \in \mathbb{Q}\}$$

which simplifies to

$$\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}, \text{ as expected.}$$

The kernel $\ker \varphi_\alpha$ is an ideal of $F[X]$. If $\alpha$ is transcendental over $F$, this means $\ker \varphi_\alpha$ is the zero ideal in $F[X]$. Then $\varphi_\alpha$ is one-to-one, and

$$F[X] \cong \operatorname{im} \varphi_\alpha = F[\alpha].$$

Here $F[\alpha]$ is just a copy of $F[X]$. For example, $\mathbb{Q}[\pi] \cong \mathbb{Q}[X]$.

But if $\alpha$ is algebraic over $F$, then $\ker \varphi_\alpha = \langle g \rangle$ for a unique, monic, nonconstant $g$ in $F[X]$.

The first isomorphism theorem tells us that

$$F[X]/\ker \varphi_\alpha \cong \operatorname{im} \varphi_\alpha$$

where $f(X) + \ker \varphi_\alpha \mapsto f(\alpha)$. In other words, $F[X]/\langle g \rangle \cong F[\alpha]$. Since $F[\alpha]$ is an integral domain, so is $F[X]/\langle g \rangle$, and thereby $\langle g \rangle$ is a nonzero prime ideal of $F[X]$. This forces $g$ to be irreducible

in $F[X]$. Then $\langle g \rangle$ is a maximal ideal in $F[X]$, which causes $F[X]/\langle g \rangle$, and thereby $F[\alpha]$, to be a field.

We can summarize what we just learned as follows.

**Proposition 0.38** An element $\alpha$ in an extension $K$ of $F$ is algebraic if and only if $F[\alpha]$ is a field.

We also have the following useful fact.

**Proposition 0.39** If $\alpha$ in an extension $K$ of $F$ is algebraic over $F$, then there is a polynomial $g$ in $F[X]$ which is unique with the following properties:

1. $g$ is monic.
2. $g(\alpha) = 0$.
3. $g$ is irreducible.

**Proof.** The monic generator $g$ of $\ker \varphi_\alpha$ has these properties. If $f$ is another polynomial with these properties, then $f \in \ker \varphi_\alpha = \langle g \rangle$. Thus $f = gh$ for some $h \in F[X]$. Since $f$ is irreducible and $g$ is not constant, $h$ must be constant. Since both $f$ and $g$ are monic we get $h = 1$, and then $f = g$. □

**Definition 0.40** The unique $g$ in $F[X]$ with Properties (1)–(3) is called the **minimal polynomial** of $\alpha$.

Also, if $g$ is the minimal polynomial of $\alpha$ and $f \in F[X]$ is any polynomial that has $\alpha$ as a root, that is, $f(\alpha) = 0$, then $g \mid f$ in $F[X]$.

**Example 0.41** Let $\zeta = e^{2\pi i/5}$ in $\mathbb{C}$. Since $\zeta$ is a root of $X^5 - 1$, we see that $\zeta$ is algebraic over $\mathbb{Q}$. We have $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1)$. Since $\zeta \neq 1$, our $\zeta$ is a root of $X^4 + X^3 + X^2 + X + 1$. This polynomial is monic, and we saw it was irreducible. So the minimal polynomial of $\zeta$ is $X^4 + X^3 + X^2 + X + 1$.

**Example 0.42** If $\alpha = \sqrt{2}+i$, is $\alpha$ algebraic over $\mathbb{Q}$, and if so what is its minimal polynomial?

Well,

$$\begin{aligned} \alpha^2 &= (\sqrt{2}+i)^2 = 2 + 2\sqrt{2}i - 1 = 1 + 2\sqrt{2}i \\ \alpha^2 - 1 &= 2\sqrt{2}i \\ (\alpha^2-1)^2 &= -8 \\ \alpha^4 - 2\alpha^2 + 1 &= -8 \\ \alpha^4 - 2\alpha^2 + 9 &= 0. \end{aligned}$$

So $\alpha$ is algebraic over $\mathbb{Q}$ because it is a root of $g = X^4 - 2X^2 + 9$ in $\mathbb{Q}[X]$.

But is $g$ irreducible? The only possible rational roots are $\pm 1, \pm 3, \pm 9$, and none of these are roots. So $g$ has no linear factor. Could we have $g = fh$, where $f, h$ are quadratics in $\mathbb{Q}[X]$? In that case, Gauss' lemma lets us replace $f, h$ by quadratics in $\mathbb{Z}[X]$, and since $g$ is monic, this would force $f, h$ to be monic.

Thus we would get

$$X^4 - 2X^2 + 9 = (X^2 + aX + b)(X^2 + cX + d)$$

where $a, b, c, d \in \mathbb{Z}$.

Then, by comparing coefficients:

$$a + c = 0 \tag{1}$$
$$b + d + ac = -2 \tag{2}$$
$$bc + ad = 0 \tag{3}$$
$$bd = 9 \tag{4}$$

Now (1) implies $a = -c$, and then (3) implies $a(b-d) = 0$, so either $a = c = 0$ or $b = d$.

If $a = c = 0$, (2) becomes $b + d = -2$, and using (4) we get the possibilities:

$$b = 1, -1, 3, -3, 9, -9$$
$$d = 9, -9, 3, -3, 1, -1$$

which never give $b+d=-2$.

So we get $a=-c\neq 0$ and $b=d$. Then (4) gives $b=d=\pm 3$. Then (2) gives

$$\pm 6-a^2=-2,$$

so $a^2=8$ or $a^2=-4$, neither of which is possible for an integer $a$.

An alternative way to see that $X^4-2X^2+9$ is irreducible over $\mathbb{Q}$ is to factor it in $\mathbb{R}[X]$ as

$$X^4-2X^2+9=(X^2-2\sqrt{2}X+3)(X^2+2\sqrt{2}X+3).$$

These quadratics are irreducible in $\mathbb{R}[X]$ (because $b^2-4ac<0$). By unique factorization in $\mathbb{R}[X]$ and the fact $2\sqrt{2}\notin\mathbb{Q}$, we cannot factor $X^4-2X^2+9$ into quadratics in $\mathbb{Q}[X]$.

## Adjoining Algebraic Elements

If $K$ extends $F$ and $\alpha\in K$ is algebraic over $F$, then $\alpha$ has a minimal polynomial $g$ in $F[X]$ and $F[\alpha]$ is a field extension of $F$, which is isomorphic to $F[X]/\langle g\rangle$.

**Proposition 0.43** If $K$ extends $F$ and $\alpha\in K$ is algebraic over $F$ with minimal polynomial $g$, then

$$[F[\alpha]:F]=\deg g.$$

Thus every $\beta$ in $F[\alpha]$ is algebraic over $F$, as well.

**Proof.** Let $n=\deg g$. We verify that $1,\alpha,\alpha^2,\ldots,\alpha^{n-1}$ is a basis for $F[\alpha]$ as a vector space over $F$. Every element in $F[\alpha]$ takes the form $f(\alpha)$ for some $f(X)\in F[X]$. By Euclidean division in $F[X]$, we have polynomials $q,r\in F[X]$ such that

$$f=gq+r \qquad \text{and} \qquad \deg r<\deg g \text{ or } r=0.$$

Then substitute $X=\alpha$ to get

$$f(\alpha)=g(\alpha)q(\alpha)+r(\alpha)=r(\alpha).$$

Thus every element in $F[\alpha]$ takes the form $r(\alpha)$ where $r\in F[X]$ and $\deg r<n$ or $r=0$ (zero polynomial). This tells us that $1,\alpha,\ldots,\alpha^{n-1}$ span $F[\alpha]$. If these were linearly dependent over $F$, this would yield a nonzero polynomial $h\in F[X]$ such that $h(\alpha)=0$ and $\deg h\leq n-1$. But then

$g \mid h$ in $F[X]$, which is impossible since $\deg h < \deg g$. □

**Example 0.44** For $\zeta = e^{2\pi i/5}$ with minimal polynomial $g = X^4 + X^3 + X^2 + X + 1$ in $\mathbb{Q}[X]$, a basis for $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$ consists of $1, \zeta, \zeta^2, \zeta^3$. For instance, $\zeta^4 = -1 - \zeta - \zeta^2 - \zeta^3$.

**Example 0.45** For $\alpha = \sqrt{2}$ with minimal polynomial $g = X^2 - 2$ in $\mathbb{Q}[X]$, a basis for the field $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$ is $1, \sqrt{2}$.

## The Tower Theorem

**Proposition 0.46 (Tower theorem)** If $K$ is a finite extension of $F$ and $L$ is a finite extension of $K$, then $L$ is a finite extension of $F$. In fact,

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

**Proof.** Let $x_1, \ldots, x_n$ be a basis of $K$ over $F$ and $y_1, \ldots, y_m$ be a basis of $L$ over $K$. We show that the set of all products $x_i y_j$ forms a basis of $L$ over $F$.

The extension tower is shown in Figure 2.


FIGURE 2

If $z \in L$, we have $z = \sum_j a_j y_j$ for some $a_j \in K$. But each $a_j = \sum_i b_{ij} x_i$ for some $b_{ij} \in F$. So

$$z = \sum_j \left( \sum_i b_{ij} x_i \right) y_j = \sum_{i,j} b_{ij} x_i y_j,$$

where $b_{ij} \in F$. Thus the $x_i y_j$ span $L$ as a vector space over $F$. To check linear independence,

suppose $\sum_{i,j} b_{ij}x_iy_j = 0$ for some $b_{ij} \in F$. Then

$$\sum_j \left( \sum_i b_{ij}x_i \right) y_j = 0.$$

Since the $y_j$ form a basis for $L$ over $K$ and $\sum_i b_{ij}x_i \in K$, we conclude that $\sum_i b_{ij}x_i = 0$ for all $j$. Since the $x_i$ form a basis for $K$ over $F$ and $b_{ij} \in F$, we conclude $b_{ij} = 0$ for all $i$ and all $j$. □

If $L$ is a finite extension of $F$ and $K$ is an intermediate field between $L$ and $F$, that is, $F \subseteq K \subseteq L$, then the tower theorem forces both degrees $[K : F]$ and $[L : K]$ to divide $[L : F]$. This is a severe restriction on the possible intermediate fields.

The tower theorem is extremely useful.

**Example 0.47** Let $L = \mathbb{Q}[\zeta][\alpha]$ where $\alpha = \sqrt[5]{2}$ and $\zeta = e^{2\pi i/5}$.

The minimal polynomial of $\alpha$ over $\mathbb{Q}$ is $X^5 - 2$, which is irreducible by Eisenstein with $p = 2$. The minimal polynomial of $\zeta$ over $\mathbb{Q}$ is $X^4 + X^3 + X^2 + X + 1$, which we checked was irreducible (since 5 is prime).

We have the tower

$$\mathbb{Q} \subseteq \mathbb{Q}[\zeta] \subseteq \mathbb{Q}[\zeta][\alpha] = L,$$

all inside $\mathbb{C}$. We know that the degree $[\mathbb{Q}[\zeta] : \mathbb{Q}] = \deg(X^4 + X^3 + X^2 + X + 1) = 4$.

To get the degree $[L : \mathbb{Q}]$ by the tower theorem, we need $[L : \mathbb{Q}[\zeta]]$. So we need the minimal polynomial $g$ of $\alpha$ in $\mathbb{Q}[\zeta][X]$. Since $\alpha$ is a root of $X^5 - 2$, the minimal polynomial $g$ divides $X^5 - 2$ in $\mathbb{Q}[\zeta][X]$. But at this point we cannot be sure that $g = X^5 - 2$.

Does $X^5 - 2$ reduce in $\mathbb{Q}[\zeta][X]$? Maybe! For one thing, the tower theorem tells us that

$$[L : \mathbb{Q}] = \underbrace{[L : \mathbb{Q}[\zeta]]}_{\leq 5} \underbrace{[\mathbb{Q}[\zeta] : \mathbb{Q}]}_{=4} \leq 20.$$

But $\mathbb{Q}[\alpha]$ is a subfield of $L$ too! So $[\mathbb{Q}[\alpha] : \mathbb{Q}]$, which is 5, divides $[L : \mathbb{Q}]$, by the tower theorem. Likewise $[\mathbb{Q}[\zeta] : \mathbb{Q}]$, which is 4, divides $[L : \mathbb{Q}]$. So $[L : \mathbb{Q}]$ is a number $\leq 20$ and divisible by both 5 and 4. The only such number is 20.

We now see that $[L : \mathbb{Q}[\zeta]]$ must be 5. So the minimal polynomial of $\alpha$ over $\mathbb{Q}[\zeta]$ remains

$X^5 - 2$.

Figure 3 summarizes the extensions and their degrees.

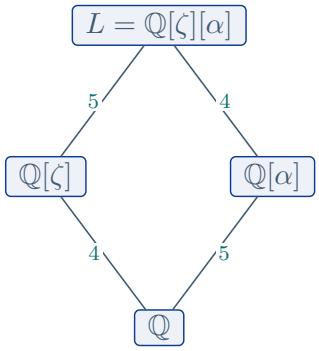



FIGURE 3

The integers denote the degrees of the extensions.

Incidentally, the roots of $X^5 - 2$ are

$$\alpha, \alpha\zeta, \alpha\zeta^2, \alpha\zeta^3, \alpha\zeta^4,$$

where $\alpha = \sqrt[5]{2}$ and $\zeta = e^{2\pi i/5}$. All these roots are in $L = \mathbb{Q}[\zeta][\alpha]$. Any subfield of $\mathbb{C}$ that contains the above roots also contains $\zeta = ((\alpha\zeta))/\alpha$, and thereby contains $L$. So $L$ is the smallest subfield of $\mathbb{C}$ that contains all roots of $X^5 - 2$. As we shall come to learn, $L$ is what is known as the **splitting field** of $X^5 - 2$.

## Algebraic Extensions of Algebraic Extensions

**Definition 0.48** An extension $K$ of $F$ is called **algebraic** over $F$ when every $\alpha$ in $K$ is algebraic over $F$.

We saw in Proposition 0.33 that if $K$ has finite degree over $F$, then $K$ is an algebraic extension of $F$. In Proposition 0.43 we saw that if $\alpha$ is in an extension $K$ of $F$ and $\alpha$ is algebraic over $F$, then the extension $F[\alpha]$ has finite degree over $F$. Hence the whole extension $F[\alpha]$ is algebraic over $F$, that is, every $\beta$ in $F[\alpha]$ is algebraic over $F$.

We will also need the following fact.

**Proposition 0.49** If $F \subseteq L \subseteq K$ is a tower of fields with $L$ algebraic over $F$ and $K$ algebraic over $L$, then $K$ is algebraic over $F$.

**Proof.** Let $\alpha \in K$. Since $\alpha$ is algebraic over $L$, there exists

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in L[X]$$

such that $f(\alpha) = 0$. Now inspect the following tall tower of field extensions:

$$F \subseteq F[a_0] \subseteq F[a_0][a_1] \subseteq F[a_0][a_1][a_2] \subseteq \cdots \subseteq F[a_0][a_1]\ldots[a_{n-1}] = E.$$

Note that $E \subseteq L$. Each extension in this tower has finite degree over its preceding extension because each $a_i$, being in $L$, is algebraic over $F$, and thereby algebraic over its preceding extension. By the tower theorem, the final field $E$ in the tower has finite degree over $F$. Clearly $\alpha$ is algebraic over $E$ (not just over the bigger field $L$). So the degree $[E[\alpha] : E]$ is finite too. By the tower theorem applied to the tower

$$F \subseteq E \subseteq E[\alpha]$$

we see that the degree $[E[\alpha] : F]$ is finite. Thus $E[\alpha]$ is an algebraic extension of $F$. In particular, $\alpha$ is algebraic over $F$. □

## The Field of Algebraic Elements

We should also keep the following in mind.

**Proposition 0.50** If $K$ is a field extension of $F$, then the set

$$L = \{\alpha \in K : \alpha \text{ is algebraic over } F\}$$

is a subfield of $K$ and $L$ extends $F$.

**Proof.** Let $\alpha, \beta \in K$ and assume both are algebraic over $F$. Certainly $\beta$ remains algebraic over $F[\alpha]$. Then we get a tower of fields:

$$F \subseteq F[\alpha] \subseteq F[\alpha][\beta]$$

where the degree of each extension is finite. By the tower theorem the degree $[F[\alpha][\beta] : F]$ is finite. Thus every element in $F[\alpha][\beta]$ is algebraic over $F$. But in $F[\alpha][\beta]$ we find $\alpha \pm \beta$, $\alpha\beta$, and, whenever $\alpha$ and $\beta$ are nonzero, also $\alpha^{-1}$ and $\beta^{-1}$. This proves that algebraic elements are closed under the field operations, and thereby form a subfield of $K$, as claimed. Clearly, the subfield $L$, consisting of all algebraic elements over $F$, is an extension of $F$ because everything in $F$ is algebraic over $F$. □

## The Algebraic Closure of $\mathbb{Q}$

As noted several times, if $K$ is an extension of finite degree over $F$, then $K$ is an algebraic extension of $F$ (that is, every $\alpha$ in $K$ is algebraic over $F$). But the converse does not hold, as we now shall see.

Of course $\mathbb{C}$ extends $\mathbb{Q}$. Let $A$ be the field of all complex numbers that are algebraic over $\mathbb{Q}$. In $A$ we find $\sqrt{2}, i, e^{2\pi i/n}, \sqrt{2}+\sqrt{3}$, but not $\pi$ nor $e$ nor countlessly many more less famous transcendental numbers. Inside $A$ we have the subfields $\mathbb{Q}[\sqrt[n]{2}]$, one for each $n$. The minimal polynomial of $\sqrt[n]{2}$ is $X^n - 2$, which is irreducible by Eisenstein's criterion. So the degree $[\mathbb{Q}[\sqrt[n]{2}] : \mathbb{Q}] = n$. Thus $A$ contains subfields of arbitrarily high degree over $\mathbb{Q}$. By the usual dimension arguments, the degree of $A$ over $\mathbb{Q}$ is infinite.

But, besides being algebraic over $\mathbb{Q}$, $A$ has another noteworthy property. Namely, there is no algebraic extension $K$ of $A$, except for $A$ itself! To see this, suppose $K$ were such an extension of $A$ and that $K \supset A$ properly. Let $\alpha \in K \setminus A$, and let $g \in A[X]$ be the minimal polynomial of $\alpha$. Thus $g$ is irreducible but not linear (since $\alpha \notin A$). The coefficients of $g$ are in $A$ and therefore in $\mathbb{C}$. By the fundamental theorem of algebra (which we take for granted), $g$ has a root, say $\beta$, in $\mathbb{C}$.

This $\beta$ is algebraic over $A$, since the coefficients of $g$ are in $A$. By Proposition 0.49, $\beta$ is algebraic over $\mathbb{Q}$, because we have the tower of algebraic extensions

$$\mathbb{Q} \subseteq A \subseteq A[\beta].$$

But then $\beta \in A$ which consists of all algebraic numbers over $\mathbb{Q}$. Thus the irreducible $g$ in $A[X]$ of degree $> 1$, has a root $\beta$ in $A$. By the factor theorem, $g$ has a linear factor in $A[X]$, contradicting the irreducibility of $g$.

**Definition 0.51** An algebraic extension $A$ of a field $F$, such that $A$ admits no proper algebraic extensions of $A$, is called an **algebraic closure** of $F$.

We have just used the fundamental theorem of algebra about $\mathbb{C}$, to see that $\mathbb{Q}$ has an algebraic

closure, namely $A$, the field of all algebraic numbers.

For those with a view towards research, here is a problem. An automorphism $\varphi : A \to A$ is a homomorphism that is one-to-one and onto. The set $\mathrm{Aut}(A)$ of all automorphisms of $A$ is a group under composition. What can we say about this group? For instance, complex conjugation $z \mapsto \bar{z}$ is in $\mathrm{Aut}(A)$. It is known that $\mathrm{Aut}(A)$ is an uncountable group. In the world of algebra research, $\mathrm{Aut}(A)$ is a *hot item*.

Using the axiom of choice, it can be shown that every field $F$ has an algebraic closure. But we will skip that item.

## Another Way to Look at Extensions of Finite Degree

If $K$ is a finite degree extension of $F$, take a basis $\alpha_1, \ldots, \alpha_n$ of $K$ as a vector space over $F$. These $\alpha_i$ are all algebraic over $F$. Thus we get a tower of algebraic field extensions

$$F \subseteq F[\alpha_1] \subseteq F[\alpha_1][\alpha_2] \subseteq F[\alpha_1][\alpha_2][\alpha_3] \subseteq \cdots \subseteq F[\alpha_1][\alpha_2] \ldots [\alpha_n] = K. \qquad (*)$$

Conversely, suppose $K$ extends $F$, that we have $\alpha_1, \ldots, \alpha_n$ in $K$ algebraic over $F$, and that $K$ sits at the top of the tower (*). Then the tower theorem tells us that $K$ is a finite degree extension of $F$.

To keep the notation simple, we consider an algebraic tower with just two steps:

$$F \subseteq F[\alpha] \subseteq F[\alpha][\beta] = K$$

where $\alpha, \beta$ are algebraic over $F$. Now $\gamma \in K$ if and only if $\gamma = \sum_j a_j \beta^j$ for some polynomial $f = \sum_i a_i X^i$ in $F[\alpha][X]$. Then each $a_j = \sum_i b_{ij} \alpha^i$ for some polynomial $g_j = \sum_i b_{ij} Y^i$ in $F[Y]$. So

$$\gamma = \sum_j \left( \sum_i b_{ij} \alpha^i \right) \beta^j = \sum_{j,i} b_{ij} \alpha^i \beta^j.$$

This tells us $K$ consists of all polynomial expressions $h(\alpha, \beta)$ where $h(X, Y)$ is a polynomial in $F[X, Y]$. In other words, $K$ is the image of the substitution homomorphism

$$\begin{aligned} \varphi : F[X, Y] &\longrightarrow K \\ f(X, Y) &\mapsto f(\alpha, \beta). \end{aligned}$$

Thus $K$ is the smallest ring containing $F$ and the algebraic elements $\alpha, \beta$. We also write $K = F[\alpha, \beta]$. More generally, every finite degree extension $K$ of $F$ takes the form $K = F[\alpha_1, \ldots, \alpha_n]$

with $\alpha_i$ algebraic over $F$.

Here is a problem we will encounter often. An algebraic extension $K = F[\alpha_1, \ldots, \alpha_n]$ sits before us, with some algebraic elements $\alpha_1, \ldots, \alpha_n$ generating the extension, in the sense that every $\alpha$ in $K$ is a polynomial in the $\alpha_1, \ldots, \alpha_n$ with coefficients in $F$. What is the degree of $K$ over $F$?

Of course, we have the tower

$$F \subseteq F[\alpha_1] \subseteq F[\alpha_1][\alpha_2] = F[\alpha_1, \alpha_2] \subseteq \cdots \subseteq F[\alpha_1][\alpha_2] \ldots [\alpha_n] = F[\alpha_1, \ldots, \alpha_n] = K.$$

So all we need is the degree of each extension in the tower over the preceding extension. After that we can use the tower theorem. We may well know the minimal polynomials $g_1, \ldots, g_n$ in $F[X]$ for $\alpha_1, \ldots, \alpha_n$, respectively. Then of course

$$[F[\alpha_1] : F] = \deg g_1.$$

But in trying to find $[F[\alpha_1][\alpha_2] : F[\alpha_1]]$ we get stuck. Since $\alpha_2$ is a root of $g_2$ and $g_2 \in F[X]$, we see that $g_2 \in F[\alpha_1][X]$ as well. So the minimal polynomial of $\alpha_2$ in $F[\alpha_1][X]$ is merely a divisor of $g_2$ in $F[\alpha_1][X]$. If we are lucky, the minimal polynomial of $\alpha_2$ in $F[\alpha_1][X]$ could equal $g_2$, but we will not always be lucky.

**Example 0.52** The smallest field containing all roots of $(X^2-2)(X^2-3)$ is $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. What is $[K : \mathbb{Q}]$?

We suspect the answer is 4, but we should check. There is the tower

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt{2}][\sqrt{3}] = K.$$

The minimal polynomials in $\mathbb{Q}[X]$ of $\sqrt{2}$ and $\sqrt{3}$ are $X^2 - 2$ and $X^2 - 3$, respectively. So, we can be sure that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

The minimal polynomial $g$ of $\sqrt{3}$ in $\mathbb{Q}(\sqrt{2})[X]$ divides $X^2 - 3$, so either $g = X^2 - 3$ or $g$ is linear. Suppose it is linear. Then $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, so

$$\sqrt{3} = a + b\sqrt{2}$$

for some $a, b \in \mathbb{Q}$. We cannot have $b = 0$, since $\sqrt{3} \notin \mathbb{Q}$. Squaring gives

$$3 = a^2 + 2b^2 + 2ab\sqrt{2}.$$

If $a \neq 0$, this would put $\sqrt{2} \in \mathbb{Q}$; if $a = 0$, it would give $b^2 = 3/2$, which is impossible for rational $b$. Thus $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, and $g = X^2 - 3$.

So $g = X^2 - 3$, as a polynomial in $\mathbb{Q}(\sqrt{2})[X]$, and then $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. By the tower theorem $[K : \mathbb{Q}] = 4$.

A basis for $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$ is $1, \sqrt{2}$, and a basis for $K$ over $\mathbb{Q}[\sqrt{2}]$ is $1, \sqrt{3}$. Then a basis for $K$ over $\mathbb{Q}$ is obtained by taking all products of first basis with the second basis to get $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. So

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}.$$

**Example 0.53** The roots of $X^3 - 2$ in $\mathbb{C}$ are $\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}, \sqrt[3]{2}e^{4\pi i/3}$. To save writing let $\alpha = \sqrt[3]{2}$, $\omega = e^{2\pi i/3}$. So the roots are $\alpha, \alpha\omega, \alpha\omega^2$. They are plotted in Figure 4.

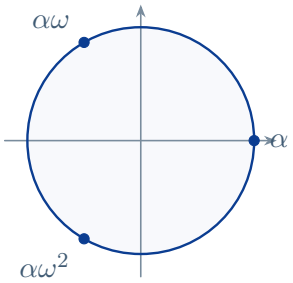



FIGURE 4

The smallest subfield of $\mathbb{C}$ that contains these roots is $K = \mathbb{Q}[\alpha, \alpha\omega, \alpha\omega^2]$. What is $[K : \mathbb{Q}]$?

Notice that $\omega = ((\alpha\omega))/\alpha \in K$, so $K = \mathbb{Q}[\alpha, \omega]$ as well. The smallest field containing the original roots equals the smallest field containing $\alpha$ and $\omega$. This gives us a better chance to find $[K : \mathbb{Q}]$. We have the tower $\mathbb{Q} \subseteq \mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\alpha, \omega] = K$. The minimal polynomial of $\alpha$ in $\mathbb{Q}[X]$ is $X^3 - 2$, by Eisenstein's criterion, so $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$.

The minimal polynomial of $\omega$ in $\mathbb{Q}[X]$ is $X^2 + X + 1$, since $\omega$ is a root of $X^3 - 1 = (X - 1)(X^2 + X + 1)$ and $\omega \neq 1$, and we saw that $X^2 + X + 1$ is irreducible in $\mathbb{Q}[X]$. Before we can conclude by the tower theorem that $[K : \mathbb{Q}] = 6$, we need to check that $X^2 + X + 1$ stays the minimal polynomial of $\omega$ in $\mathbb{Q}[\sqrt[3]{2}][X]$.

If this were not so, the minimal polynomial of $\omega$ in $\mathbb{Q}[\sqrt[3]{2}][X]$ would be $X - \omega$. This would put $\omega \in \mathbb{Q}[\sqrt[3]{2}]$. However, $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$, while $\omega \notin \mathbb{R}$. So $X^2 + X + 1$ remains the minimal polynomial of $\omega$ in $\mathbb{Q}[\sqrt[3]{2}][X]$.

**Example 0.54** If $\alpha = e^{\pi i/4} = 1/\sqrt{2} + i1/\sqrt{2}$ and $K = \mathbb{Q}[i, \alpha]$, what is $[K : \mathbb{Q}]$?

We have the tower

$$\mathbb{Q} \subseteq \mathbb{Q}[i] \subseteq \mathbb{Q}[i][\alpha] = K.$$

Clearly $[\mathbb{Q}[i] : \mathbb{Q}] = 2$ because $X^2 + 1$ is the minimal polynomial of $i$ in $\mathbb{Q}[X]$. What is $[\mathbb{Q}[i][\alpha] : \mathbb{Q}[i]]$?

Well, $\alpha^4 = (e^{\pi i/4})^4 = e^{\pi i} = -1$, so $\alpha$ is a root of $X^4 + 1$ in $\mathbb{Q}[X]$. Since $X^4 + 1$ is irreducible in $\mathbb{Q}[X]$, this is the minimal polynomial of $\alpha$ in $\mathbb{Q}[X]$. However, in $\mathbb{Q}[i][X]$ we get

$$X^4 + 1 = (X^2 + i)(X^2 - i),$$

a reduction. In fact, $\alpha^2 = e^{\pi i/2} = i$. So $\alpha$ is a root of $X^2 - i$ in $\mathbb{Q}[i][X]$. Now is $X^2 - i$ irreducible in $\mathbb{Q}[i][X]$? If not, this would mean that $\alpha \in \mathbb{Q}[i]$ (as argued in earlier examples). But if we had $\alpha \in \mathbb{Q}[i]$, this would mean

$$\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}} = a + bi$$

for some $a, b \in \mathbb{Q}$. Equating real parts gives $1/\sqrt{2} \in \mathbb{Q}$, which is impossible. Thus the degree $[\mathbb{Q}(i)(\alpha) : \mathbb{Q}(i)] = 2$, and by the tower theorem $[K : \mathbb{Q}] = 4$, not 8.

For an even quicker solution, look at the tower

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha)(i) = K.$$

Then notice $\alpha^2 = i \in \mathbb{Q}(\alpha)$. Thus $K = \mathbb{Q}(\alpha)(i) = \mathbb{Q}(\alpha)$. Since the minimal polynomial of $\alpha$ is $X^4 + 1$, we see that $[K : \mathbb{Q}] = 4$.

## Making Roots Out of Thin Air

So far we have considered $\alpha$ in a field $K$ that are algebraic over a subfield $F$. Such $\alpha$ gave us a monic irreducible polynomial $g$ in $F[X]$ for which $\alpha$ is a root and we called $g$ the minimal polynomial of $\alpha$ over $F$.

Now, what if we start with an irreducible polynomial $g$ in $F[X]$? Is there a field extension $K$ of $F$ that contains a root $\alpha$ of $g$? The result that answers affirmatively is known as Kronecker's theorem. Except for a bit of creative imagination, we already know it.

**Proposition 0.55 (Kronecker's theorem)** If $f$ is a nonconstant polynomial in $F[X]$, then there exists a field extension $K$ of $F$ such that $K$ contains a root of $f$.

**Proof.** First pick an irreducible factor $g$ in $F[X]$ of $f$. We will create an extension $K$ that contains a root of $g$, which of course will also be a root of $f$. Take $K = F[X]/\langle g\rangle$. Since $g$ is irreducible in $F[X]$, the ideal $\langle g\rangle = \{gh : h \in F[X]\}$ is maximal in $F[X]$, and then $K = F[X]/\langle g\rangle$ is a field. But how is $K$ an extension of $F$, and where is the root $\alpha$ of $g$? Take the canonical map

$$\begin{aligned} \varphi : F[X] &\longrightarrow F[X]/\langle g\rangle = K \\ h &\longmapsto h + \langle g\rangle. \end{aligned}$$

The image of $\varphi$ is $K$. The field $F$ is a subring of $F[X]$, namely, $F$ equals the set of constant polynomials. Since $F$ is a field, the restriction of $\varphi$ to $F$ is one-to-one. Thus $F \cong \varphi(F)$, which is a subfield of $K$. Next, put $\alpha = \varphi(X)$, that is, the value of $\varphi$ at the polynomial $X$. Clearly $\alpha \in K$. Now $g \in \ker\varphi$, and writing $g = a_0 + a_1X + \cdots + a_nX^n$, we get

$$\begin{aligned} 0 = \varphi(g) &= \varphi(a_0) + \varphi(a_1)\varphi(X) + \cdots + \varphi(a_n)\varphi(X)^n \\ &= \varphi(a_0) + \varphi(a_1)\alpha + \cdots + \varphi(a_n)\alpha^n, \end{aligned}$$

so $\alpha$ is a root in $K$ of the polynomial

$$\varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n,$$

which lies in $\varphi(F)[X]$. At this point a leap of imagination is needed. Since $F \cong \varphi(F)$, we identify $F$ with $\varphi(F)$. So we declare $a = \varphi(a)$ for every $a$ in $F$. (This last step could bother some. It can be avoided at a cost of much more irritating verbiage. Better to just take the step.) With this step, $F$ becomes a subfield of $K$ and the polynomial $\varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n$, for which $\alpha$ is a root, becomes $a_0 + a_1X + \cdots + a_nX^n$, which is our $g$. □

## An Application to Algebraic Geometry

**Definition 0.56** For this discussion, an **irreducible plane curve** is a subset $V$ of $\mathbb{C}^2$ cut out by a single irreducible polynomial $f(x,y) \in \mathbb{C}[x,y]$:

$$V = \{(x,y) \in \mathbb{C}^2 : f(x,y) = 0\}.$$

To say that $f(x,y)$ is irreducible in $\mathbb{C}[x,y]$ means that the only way to factor $f = gh$ in $\mathbb{C}[x,y]$ is by having $g$ or $h$ be constant polynomials.

**Example 0.57** The plane curve given by $x^2 + y^2 - 1$ contains every point of the form $(x,y) = (\cos z, \sin z)$ with $z \in \mathbb{C}$.

It might not be so easy to confirm that a polynomial in two variables is irreducible. Our theory gives us a few useful tools.

Just for psychological reasons we shall call the variables $t$ and $x$. The ring $\mathbb{C}[t,x]$ can be viewed as the ring $\mathbb{C}[t][x]$ of polynomials in $x$ whose coefficients are polynomials in $t$. Of course $\mathbb{C}[t]$ is a subring of the fraction field $\mathbb{C}(t)$ of rational functions in the indeterminate $t$.

A variant of Gauss' lemma, applied to $\mathbb{C}[t]$ and $\mathbb{C}(t)$ instead of $\mathbb{Z}$ and $\mathbb{Q}$, says that if $f(t,x) \in \mathbb{C}[t][x]$ and $f$ is irreducible in $\mathbb{C}[t][x]$, then $f$ is irreducible in $\mathbb{C}(t)[x]$. A variant of Eisenstein's criterion says that if $f(t,x) = a_n x^n + \cdots + a_1 x + a_0$ where the $a_j = a_j(t) \in \mathbb{C}[t]$ and if $p(t)$ is an irreducible polynomial in $\mathbb{C}[t]$ such that

1. $p(t) \mid a_j(t)$ for all $j = 0, \ldots, n-1$ in $\mathbb{C}[t]$,
2. $p(t) \nmid a_n(t)$, and
3. $p^2(t) \nmid a_0(t)$

then $f(t,x)$ is irreducible in $\mathbb{C}(t)[x]$.

For a proof just replace $\mathbb{Z}$ by $\mathbb{C}[t]$ and $\mathbb{Z}[x]$ by $\mathbb{C}[t][x]$ in the original proof of Eisenstein's criterion. The same proof works because $\mathbb{C}[t]$ is a unique factorization domain, just like $\mathbb{Z}$.

**Example 0.58** The plane curve given by $x^n - t$ is irreducible for each positive integer $n$. To see this, apply Eisenstein's criterion using the irreducible polynomial $p(t) = t$ in $\mathbb{C}[t]$. We have $t \mid 0$ for the coefficients of $x^{n-1}, \ldots, x$, while $t \nmid 1$ for the coefficient of $x^n$ and $t^2 \nmid -t$ for the constant term.

**Proposition 0.59** If $n, m$ are coprime positive integers, then the plane curve given by $x^n - t^m$ is irreducible.

**Proof.** Let $K$ be a field extension of $\mathbb{C}(t)$ that contains a root $\alpha$ of $f(t, x)$ as a polynomial in $x$ with coefficients in $\mathbb{C}(t)$, that is, $\alpha^n - t^m = f(t, \alpha) = 0$.

The minimal polynomial $g$ in $\mathbb{C}(t)[x]$ of $\alpha$ is a divisor of $f$ in $\mathbb{C}(t)[x]$. Also $g$ is irreducible in $\mathbb{C}(t)[x]$. In order to prove that $f$ is irreducible in $\mathbb{C}(t)[x]$ it is enough to show that $\deg g = \deg f$ as polynomials in $x$.

As we know,

$$[\mathbb{C}(t)[\alpha] : \mathbb{C}(t)] = \deg g.$$

Now inside the field $\mathbb{C}(t)$ there is the subfield $\mathbb{C}(u)$ where $u = t^m$. This is just another field of rational functions in the variable $u$. For example,

$$\frac{3 - 7t^m + 5(t^m)^2}{12 + \frac{1}{3}(t^m)^3} \in \mathbb{C}(t^m) = \mathbb{C}(u).$$

So $\mathbb{C}(t)$ is an extension of $\mathbb{C}(u) = \mathbb{C}(t^m)$.

Notice that $X^m - u$ is irreducible in $\mathbb{C}(u)[X]$, by Eisenstein's criterion, and $t$ is a root of $X^m - u$, that is, $t^m - t^m = 0$. So $\mathbb{C}(u)[t]$ is an extension of $\mathbb{C}(u)$ of degree $m$. But $\mathbb{C}(u)[t]$ is a field containing $t$. So $\mathbb{C}(u)[t]$ contains $\mathbb{C}(t)$, and since $\mathbb{C}(u)[t] \subseteq \mathbb{C}(t)$ for obvious reasons we see that $\mathbb{C}(t) = \mathbb{C}(u)[t]$ is a field extension of $\mathbb{C}(u)$ of degree $m$.

Likewise $X^n - u$ is irreducible in $\mathbb{C}(u)[X]$, by Eisenstein's criterion. The element $\alpha$ is a root of $X^n - u$ because $\alpha^n - u = \alpha^n - t^m = 0$. So the field extension $\mathbb{C}(u)[\alpha]$ has degree $n$ over $\mathbb{C}(u)$.

The field towers and their extension degrees are shown in Figure 5.

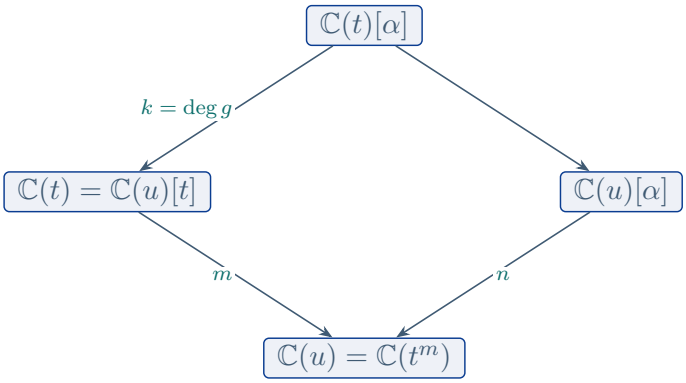



FIGURE 5

The tower theorem going up the left side says that

$$[\mathbb{C}(t)[\alpha] : \mathbb{C}(u)] = mk \leq mn \quad (\text{since } g \mid f \text{ in } \mathbb{C}(t)[x]).$$

Going up the right side shows that $n$ divides $[\mathbb{C}(t)[\alpha] : \mathbb{C}(u)]$.

Since $m, n$ are coprime, $mn$ also divides $[\mathbb{C}(t)[\alpha] : \mathbb{C}(u)]$. Thus $mn \mid mk$ and $mk \leq mn$, which forces $n = k$. That is $\deg f = \deg g$, as desired. □

This was all baby algebra. To do advanced algebra, we have to ramp up our thinking.

## 3. Splitting Fields

### What is a Splitting Field, Really?

If $f \in F[X]$, we saw how to create a field $K$ that contains a root of $f$. However, $f$ can have several roots, so we need a field $K$ that contains all of them.

**Definition 0.60** If $K$ extends $F$ and $f$ is a nonconstant polynomial in $F[X]$, we say that $f$ **splits** in $K[X]$, or that $f$ splits over $K$, when it can be written as a product of linear factors:

$$f = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

where $a \in F$ and $\alpha_1, \ldots, \alpha_n \in K$. Some roots may repeat.

**Example 0.61** $X^3 + 1$ splits in $\mathbb{C}[X]$ as

$$X^3 + 1 = (X + 1)(X - e^{\pi i/3})(X - e^{-\pi i/3}).$$

The three roots are plotted in Figure 6.

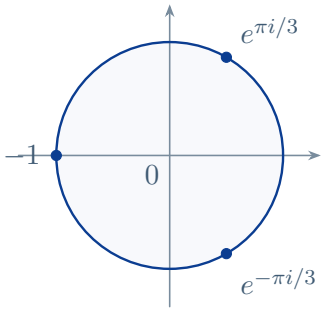



FIGURE 6

Of course, the $\alpha_j$ in $K$ are roots of $f$, and there can be no additional roots of $f$ in $K$.

If $F$ is a subfield of $\mathbb{C}$ and $f \in F[X]$, the fundamental theorem of algebra (which we still take for granted!) guarantees that $f$ splits over $\mathbb{C}$. But this guarantee is not readily available for an arbitrary field $F$. We need a proof.

**Proposition 0.62** If $f$ is a nonconstant polynomial in $F[X]$, then there is an extension $E$ of $F$ such that $f$ splits in $E[X]$.

**Proof.** We use induction on $\deg f$. If $\deg f = 1$, then $f$ is already split in $F[X]$, so we can take $E = F$. Suppose that for every field $L$ and every polynomial $g$ in $L[X]$ of degree $< n$, there is an extension of $L$ over which $g$ splits. Now take $f \in F[X]$ with $\deg f = n$. By Kronecker's theorem (Proposition 0.55), there is an extension $L$ of $F$ containing a root $\alpha$ of $f$. Thus $X - \alpha$ divides $f$ in $L[X]$, so

$$f = (X - \alpha)g$$

for some $g \in L[X]$ with $\deg g = n - 1 < n$. By the inductive hypothesis applied to $g$, the field $L$

has an extension $E$ such that $g$ splits in $E[X]$:

$$g = a(X - \alpha_2)(X - \alpha_3) \cdots (X - \alpha_n)$$

for some $a \in L$ and $\alpha_2, \alpha_3, \ldots, \alpha_n \in E$. Hence

$$f = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

where $\alpha_1 = \alpha$ and all $\alpha_j \in E$. Also, $a \in F$ because $a$ is the leading coefficient of $f$. So $f$ splits in $E[X]$, where $E$ is an extension of $F$. □

Now comes a very important definition.

**Definition 0.63** If $f$ is a nonconstant polynomial in $F[X]$, an extension $K$ of $F$ is called a **splitting field** of $f$ provided there exist $\alpha_1, \ldots, \alpha_n$ in $K$ and $a \in F$ such that the following hold:

1. $f = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$ in $K[X]$.
2. $K = F[\alpha_1, \alpha_2, \ldots, \alpha_n]$.

By Proposition 0.62, every nonconstant $f \in F[X]$ has an extension $E$ of $F$ such that

$$f = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

with $\alpha_j \in E$ and $a \in F$. To obtain a splitting field for $f$, just set

$$K = F[\alpha_1, \alpha_2, \ldots, \alpha_n].$$

Thus $K$ is as small as possible while still allowing $f$ to split in $K[X]$.

**Example 0.64** A splitting field for $X^3 - 2$ over $\mathbb{Q}$ is $K = \mathbb{Q}[\alpha, \alpha\omega, \alpha\omega^2]$, where $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$. We already saw in Example 0.53 that $[K : \mathbb{Q}] = 6$.

**Example 0.65** When $p$ is prime, a splitting field for $X^p - 1$ over $\mathbb{Q}$ is

$$\mathbb{Q}[\zeta, \zeta^2, \ldots, \zeta^{p-1}], \quad \zeta = e^{2\pi i/p}.$$

Since all roots are powers of $\zeta$, this is simply $\mathbb{Q}[\zeta]$. Also,

$$[\mathbb{Q}[\zeta] : \mathbb{Q}] = p - 1$$

because the minimal polynomial of $\zeta$ is $X^{p-1} + \cdots + X + 1$.

Needless to say, finding a splitting field for a given polynomial in $F[X]$ can be a serious task.

## Uniqueness of Splitting Fields

We now come to a subtle question: are two splitting fields for the same $f \in F[X]$ isomorphic? They should be. To prove this, we need a way to extend isomorphisms between fields. The following material can feel intimidating, but it will make us better people.

We need one preliminary tool. Suppose $\varphi : F \to E$ is an isomorphism of fields. Then $\varphi$ lifts to an isomorphism $\varphi : F[X] \to E[X]$ by **transferring coefficients**:

$$\begin{gathered}\varphi : F[X] \longrightarrow E[X] \\ a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \longmapsto \varphi(a_n)X^n + \varphi(a_{n-1})X^{n-1} + \cdots + \varphi(a_1)X + \varphi(a_0).\end{gathered}$$

We use the same letter $\varphi$ for this extended map.

The following facts are straightforward:

- $\varphi : F[X] \to E[X]$ is a ring isomorphism, and $\deg \varphi(f) = \deg f$ for all $f \in F[X]$.
- $f \mid g$ in $F[X]$ if and only if $\varphi(f) \mid \varphi(g)$ in $E[X]$.
- $f$ is irreducible in $F[X]$ if and only if $\varphi(f)$ is irreducible in $E[X]$.
- $f$ splits in $F[X]$ if and only if $\varphi(f)$ splits in $E[X]$.

The polynomial $\varphi(f)$ is called the **$\varphi$-transfer** of $f$.

Here is a technical result.

**Proposition 0.66** Suppose the following hold:

1. $\varphi : F \to E$ is an isomorphism of fields.
2. $K$ extends $F$, and $L$ extends $E$.
3. $\alpha \in K$ has minimal polynomial $g$ in $F[X]$.
4. $\beta \in L$ has minimal polynomial $\varphi(g)$ in $E[X]$.

Then there exists an isomorphism $\psi : F[\alpha] \to E[\beta]$ such that $\psi|_F = \varphi$ and $\psi(\alpha) = \beta$.

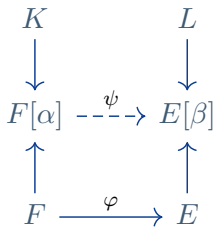
Before proving this, here is an important special case. Let $K$ extend $F$, and let $\alpha, \beta \in K$ be roots of the same monic irreducible polynomial $g$ in $F[X]$. Then there is an isomorphism

$$\psi : F[\alpha] \to F[\beta]$$

with $\psi(a) = a$ for all $a \in F$ and $\psi(\alpha) = \beta$. Indeed, in Proposition 0.66 take $\varphi : F \to F$ to be the identity map, take $K = L$, and note that $\varphi(g) = g$.

Elements such as $\alpha, \beta \in K$ that have the same minimal polynomial in $F[X]$ are called **conjugates** over $F$. For example, $\pm\sqrt{2}$ in $\mathbb{R}$ are conjugate over $\mathbb{Q}$, with minimal polynomial $X^2 - 2$; $\sqrt[5]{7}$ and $\sqrt[5]{7}e^{2\pi i/5}$ are conjugate over $\mathbb{Q}$, with minimal polynomial $X^5 - 7$; and $\pm i$ are conjugate over $\mathbb{R}$, with minimal polynomial $X^2 + 1$.

**Proof of Proposition 0.66.** Keep the following diagram in mind:




where $g$ is the minimal polynomial of $\alpha$ in $F[X]$ and $\varphi(g)$ is the minimal polynomial of $\beta$ in $E[X]$. Define two surjective homomorphisms:

$$\begin{aligned} \sigma : F[X] &\longrightarrow F[\alpha] \\ f &\longmapsto f(\alpha), \end{aligned}$$

so $\ker \sigma = \langle g \rangle$, and

$$\begin{aligned} \tau : F[X] &\longrightarrow E[\beta] \\ f &\longmapsto \varphi(f)(\beta). \end{aligned}$$

The second map is the composition

$$F[X] \xrightarrow{\varphi\text{-transfer}} E[X] \xrightarrow{\text{substitute } \beta} E[\beta].$$

Now compute $\ker \tau$. For $f \in F[X]$,

$$\begin{aligned} f \in \ker \tau &\iff \varphi(f)(\beta) = 0 \\ &\iff \varphi(f) \in \langle \varphi(g) \rangle \\ &\iff \varphi(g) \mid \varphi(f) \text{ in } E[X] \\ &\iff g \mid f \text{ in } F[X] \\ &\iff f \in \langle g \rangle. \end{aligned}$$

So $\sigma$ and $\tau$ have the same kernel. By the first isomorphism theorem,

$$\begin{aligned} \bar{\sigma} : F[X]/\langle g \rangle &\cong F[\alpha], & f + \langle g \rangle &\longmapsto f(\alpha), \\ \bar{\tau} : F[X]/\langle g \rangle &\cong E[\beta], & f + \langle g \rangle &\longmapsto \varphi(f)(\beta). \end{aligned}$$

Hence

$$\bar{\tau} \circ \bar{\sigma}^{-1} : F[\alpha] \xrightarrow{\cong} E[\beta]$$

is the desired isomorphism $\psi$. Moreover,

$$\alpha \xmapsto{\bar{\sigma}^{-1}} X + \langle g \rangle \xmapsto{\bar{\tau}} \varphi(X)(\beta) = \beta,$$

and if $a \in F$,

$$a \xmapsto{\bar{\sigma}^{-1}} a + \langle g \rangle \xmapsto{\bar{\tau}} \varphi(a).$$

So $\psi$ extends $\varphi$ and sends $\alpha$ to $\beta$. □

The next theorem will be used repeatedly.

**Proposition 0.67 (Isomorphism extension theorem)** Suppose the following hold:

1. $\varphi : F \to E$ is an isomorphism of fields.
2. $f$ is a nonconstant polynomial in $F[X]$.
3. $\varphi(f)$ is its $\varphi$-transfer in $E[X]$.
4. $K$ is a splitting field for $f$, so $F \subseteq K$.
5. $L$ is a splitting field for $\varphi(f)$, so $E \subseteq L$.
6. $\alpha \in K$ has minimal polynomial $g$ in $F[X]$.
7. $\beta \in L$ has minimal polynomial $\varphi(g)$ in $E[X]$.

Then there is an isomorphism $\psi : K \to L$ such that $\psi|_F = \varphi$ and $\psi(\alpha) = \beta$.

Before the proof, here is an important special case. Take $\varphi = \mathrm{id}_F$, so $F = E$, let $K$ and $L$ be splitting fields of the same polynomial $f \in F[X]$, and take $\alpha = \beta = 0 \in F$, with minimal polynomial $X$. Then there is an isomorphism $\psi : K \to L$ that restricts to the identity on $F$:

$$\begin{array}{ccc} K & \xrightarrow{\psi} & L \\ \uparrow & & \uparrow \\ F & \xrightarrow{\mathrm{id}} & F \end{array}$$

So any two splitting fields of the same polynomial in $F[X]$ are isomorphic by a map that fixes $F$ pointwise.

**Proof of Proposition 0.67.** We start with a picture to keep track of things.

$$\begin{array}{ccc} K & \overset{\psi}{\dashrightarrow} & L \\ \uparrow & & \uparrow \\ R & \xrightarrow{\sigma} & \sigma(R) \\ \uparrow & & \uparrow \\ F[\alpha] & \longrightarrow & E[\beta] \\ \uparrow & & \uparrow \\ F & \xrightarrow{\varphi} & E \end{array}$$

Consider all field embeddings $\sigma : R \to L$ such that $R$ is an intermediate field between $F[\alpha]$ and $K$, $\sigma$ extends $\varphi$, and $\sigma(\alpha) = \beta$. By Proposition 0.66, this family is nonempty: we already have one map $F[\alpha] \to E[\beta] \subseteq L$. Suppose $\sigma : R \to L$ is such a map and $R \subsetneq K$. Since $K$ is a splitting field for $f$, there exists a root $\gamma$ of $f$ with $\gamma \in K \setminus R$. Let $h$ be the minimal polynomial of $\gamma$ in $R[X]$. Then $\deg h \geq 2$ because $\gamma \notin R$. Because $\sigma : R \to \sigma(R)$ is an isomorphism, it induces a transfer map

$$\sigma : R[X] \to \sigma(R)[X].$$

Since $h \mid f$ in $R[X]$, we have $\sigma(h) \mid \sigma(f)$ in $\sigma(R)[X]$. Now $\sigma(f) = \varphi(f)$, and $\varphi(f)$ splits in $L[X]$. Hence $\sigma(h)$ has a root $\varepsilon \in L$. Also, $h$ is irreducible in $R[X]$, so $\sigma(h)$ is irreducible in $\sigma(R)[X]$. Apply Proposition 0.66 to the isomorphism $\sigma : R \to \sigma(R)$, the element $\gamma$, and the element $\varepsilon$. We obtain an isomorphism

$$\tilde{\sigma} : R[\gamma] \to \sigma(R)[\varepsilon]$$

with $\tilde{\sigma}|_R = \sigma$. In particular, $\tilde{\sigma}(\alpha) = \sigma(\alpha) = \beta$. So we can strictly enlarge $R$. Iterating, we get a strictly increasing tower

$$F[\alpha] = R_1 \subsetneq R_2 \subsetneq \cdots \subsetneq R_m \subseteq K$$

with embeddings $\sigma_j : R_j \to L$ extending $\varphi$ and sending $\alpha$ to $\beta$. Since $[K : F]$ is finite, this process terminates with $R_m = K$. Thus we obtain an embedding

$$\psi : K \to L$$

that extends $\varphi$ and satisfies $\psi(\alpha) = \beta$. It remains to prove surjectivity. The image $\psi(K)$ is a subfield of $L$. Since $f$ splits in $K[X]$, its $\psi$-transfer $\psi(f)$ splits in $\psi(K)[X]$. But $\psi|_F = \varphi$, so $\psi(f) = \varphi(f)$. Therefore $\varphi(f)$ splits over $\psi(K)$. Also, $\psi(F) = E$, so $\psi(K)$ is an extension of $E$. Because $L$ is the splitting field of $\varphi(f)$ over $E$, we must have

$$L \subseteq \psi(K).$$

Since $\psi(K) \subseteq L$ by definition, we conclude $\psi(K) = L$. Hence $\psi$ is an isomorphism. □

An important corollary of Proposition 0.67 is that it makes sense to speak of *the* splitting field of a polynomial over $F$, up to $F$-isomorphism.

**Proposition 0.68** Let $K$ be the splitting field of a polynomial $f$ in $F[X]$. Suppose $\alpha, \beta \in K$ have the same minimal polynomial $g$ in $F[X]$. Then there exists an automorphism $\psi : K \to K$ such that $\psi(a) = a$ for all $a \in F$, and $\psi(\alpha) = \beta$.

**Proof.** Apply Proposition 0.67 with $E = F$, $\varphi = \mathrm{id}_F$, and $L = K$. Then $\varphi(f) = f$, $\varphi(g) = g$,

and $g$ is the minimal polynomial of both $\alpha$ and $\beta$. The conclusion of Proposition 0.67 yields the required automorphism of $K$. □

In other words, if $\alpha$ and $\beta$ are $F$-conjugates in a splitting field $K$, then some automorphism of $K$ fixing $F$ sends $\alpha$ to $\beta$. This foreshadows the richness of what we will soon call the **Galois group** of the splitting field.

## The Normality Theorem

Here is terminology that we will use frequently.

**Definition 0.69** Suppose $E$ and $L$ extend $F$, and let $\varphi : E \to L$ be a field homomorphism.

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & L \\ \uparrow & & \uparrow \\ F & \xrightarrow{\text{id}} & F \end{array}$$

If $\varphi(a) = a$ for every $a \in F$, we say that $\varphi$ **fixes** $F$. Such a map is called an ***F*-embedding**, or simply an ***F*-map**.

If, in addition, $\varphi$ is onto $L$, we call it an ***F*-isomorphism**. If $E = L$ and $\varphi$ is onto, we call it an ***F*-automorphism**.

Any $F$-map $\varphi : E \to L$ is automatically an $F$-linear transformation between the vector spaces $E$ and $L$ over $F$.

**Proposition 0.70 (Normality theorem)** For a finite extension $K$ of a field $F$, the following are equivalent:

1. $K$ is the splitting field of some $f \in F[X]$.
2. For every extension $L$ of $K$ and every $F$-map $\psi : L \to L$, the restriction $\psi|_K$ is an $F$-automorphism of $K$.
3. For every $\alpha \in K$, its minimal polynomial in $F[X]$ splits in $K[X]$.

**Proof.** (1) *implies* (2). Suppose $K$ is the splitting field of some $f \in F[X]$, let $L$ extend $K$, and let $\psi : L \to L$ be an $F$-map.

$$\begin{array}{ccc} L & \xrightarrow{\psi} & L \\ \uparrow & & \uparrow \\ K & \xrightarrow{\psi|_K} & K \\ \uparrow & & \uparrow \\ F & \xrightarrow{\mathrm{id}} & F \end{array}$$

Take any root $\alpha \in K$ of $f$. Writing $f = \sum_j a_j X^j$ with $a_j \in F$, we get

$$\begin{aligned} f(\psi(\alpha)) &= \sum_j a_j \, \psi(\alpha)^j \\ &= \sum_j \psi(a_j) \, \psi(\alpha)^j \quad \text{(because } \psi \text{ fixes } F\text{)} \\ &= \psi\left( \sum_j a_j \alpha^j \right) \quad \text{(because } \psi \text{ is a homomorphism)} \\ &= \psi(f(\alpha)) = 0. \end{aligned}$$

So $\psi$ sends roots of $f$ to roots of $f$, hence permutes the finite root set. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f$ in $K$. Since $K$ is the splitting field of $f$, every element of $K$ can be written as a polynomial expression in the $\alpha_j$ with coefficients in $F$:

$$\eta = \sum_i a_{i_1 \ldots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}.$$

Applying $\psi$ gives

$$\psi(\eta) = \sum_i a_{i_1 \ldots i_n} \, \psi(\alpha_1)^{i_1} \cdots \psi(\alpha_n)^{i_n} \in K,$$

since $\psi$ fixes $F$ and permutes the roots. Hence $\psi(K) \subseteq K$. Because $\psi$ permutes the roots and fixes $F$, the field $\psi(K)$ contains $F$ and all roots of $f$. By minimality of the splitting field, $K \subseteq \psi(K)$. Therefore $\psi(K) = K$, so $\psi|_K$ is an $F$-automorphism of $K$.

(2) *implies* (3). Suppose that for any extension $L$ of $K$ and any $F$-map $\psi : L \to L$, the restriction $\psi|_K$ is an $F$-automorphism of $K$. We want to show that for every $\alpha \in K$, the minimal polynomial of $\alpha$ over $F$ splits in $K[X]$.

Take any $\alpha \in K$, and let $g \in F[X]$ be its minimal polynomial. We must show that $g$ splits in $K[X]$.

Since $[K : F] < \infty$, there exist $\alpha_1, \ldots, \alpha_n \in K$ such that

$$K = F[\alpha_1, \ldots, \alpha_n].$$

Let $g_j \in F[X]$ be the minimal polynomial of $\alpha_j$, and define

$$f = g\, g_1 \cdots g_n \in F[X].$$

Let $L$ be a splitting field of $f$ over $K$; then $K \subseteq L$. We claim that $L$ is also a splitting field of $f$ over $F$. Indeed, if $S$ denotes the roots of $f$ in $L$ that are not among the $\alpha_j$, then

$$\begin{aligned} L &= K[\alpha_1, \ldots, \alpha_n, S] && \text{(because } L \text{ is a splitting field of } f \text{ over } K) \\ &= F[\alpha_1, \ldots, \alpha_n][\alpha_1, \ldots, \alpha_n, S] && \text{(because } K = F[\alpha_1, \ldots, \alpha_n]) \\ &= F[\alpha_1, \ldots, \alpha_n, S] && \text{(because } F[\alpha_1, \ldots, \alpha_n] \text{ already contains } \alpha_1, \ldots, \alpha_n). \end{aligned}$$

So $L$ is generated over $F$ by roots of $f$, and thus is a splitting field of $f$ over $F$. Now let $\beta \in L$ be any root of $g$. By Proposition 0.67, applied to the splitting field $L$ of $f$ over $F$ and the $F$-conjugates $\alpha$ and $\beta$, there exists an $F$-map $\psi : L \to L$ such that $\psi(\alpha) = \beta$. By condition (2), $\psi|_K$ is an $F$-automorphism of $K$. Since $\alpha \in K$, we get

$$\beta = \psi(\alpha) \in K.$$

Thus every root of $g$ lies in $K$, so $g$ splits in $K[X]$.

(3) *implies* (1). Assume that for every $\alpha \in K$, the minimal polynomial of $\alpha$ over $F$ splits in $K[X]$. Again write

$$K = F[\alpha_1, \ldots, \alpha_n]$$

for suitable $\alpha_j \in K$, and let $g_j$ be the minimal polynomial of $\alpha_j$ over $F$. Set

$$f = g_1 g_2 \cdots g_n \in F[X].$$

By assumption, each $g_j$ splits in $K[X]$, so $f$ splits in $K[X]$. Since $K$ is generated over $F$ by roots of $f$, it follows that $K$ is the splitting field of $f$ over $F$. □

**Example 0.71** $K = \mathbb{Q}[\sqrt[3]{2}]$ is not the splitting field of $X^3 - 2$ over $\mathbb{Q}$, because the other

two roots,

$$\sqrt[3]{2}e^{2\pi i/3} \qquad \text{and} \qquad \sqrt[3]{2}e^{-2\pi i/3},$$

are nonreal while $K \subseteq \mathbb{R}$.

The normality theorem says more: since $\sqrt[3]{2} \in K$ and its minimal polynomial $X^3 - 2$ does not split in $K[X]$, there is no polynomial $f \in \mathbb{Q}[X]$ for which $K$ is the splitting field.

So some finite extensions are not splitting fields, regardless of the polynomial we choose.

**Example 0.72** The splitting field of $(X^2 - 2)(X^2 - 3)$ over $\mathbb{Q}$ is

$$K = \mathbb{Q}[\sqrt{2}, \sqrt{3}].$$

Since $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$, the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}[\sqrt{2}]$ is still $X^2 - 3$. Hence

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$$

is a tower with each step of degree 2, so $[K : \mathbb{Q}] = 4$. By the normality theorem, the minimal polynomial over $\mathbb{Q}$ of every element of $K$ must split in $K[X]$.

We can verify this with

$$\alpha = \sqrt{2} + \sqrt{3}.$$

Then

$$\alpha^2 = 5 + 2\sqrt{6} \qquad \text{and} \qquad (\alpha^2 - 5)^2 = 24,$$

so

$$\alpha^4 - 10\alpha^2 + 1 = 0.$$

Thus $\alpha$ is a root of $X^4 - 10X^2 + 1$ in $\mathbb{Q}[X]$. We can check that this polynomial is irreducible in $\mathbb{Q}[X]$. Its roots are

$$\pm\sqrt{2} \pm \sqrt{3},$$

which are all in $K$. Also,

$$\mathbb{Q}[\sqrt{2} + \sqrt{3}] \subseteq K,$$

and

$$[\mathbb{Q}[\sqrt{2} + \sqrt{3}] : \mathbb{Q}] = \deg(X^4 - 10X^2 + 1) = 4,$$

so $K = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.

If $K = F[\alpha, \beta]$ for algebraic elements $\alpha, \beta$, can we always find $\gamma \in K$ such that $K = F[\gamma]$? Good

question! Such a $\gamma$ is called a **primitive element**.

## Finite Fields Are Splitting Fields

We are now in a position to say quite a bit about finite fields. Suppose $F$ is a finite field. Then $F$ contains $\mathbb{Z}_p$ for some prime $p$. If

$$[F : \mathbb{Z}_p] = n,$$

then $F$ has exactly $p^n$ elements. The multiplicative group $F^*$ has order $p^n - 1$ and is abelian (in fact, cyclic). By **Lagrange's theorem**, every $\alpha \in F^*$ satisfies

$$\alpha^{p^n-1} = 1.$$

Hence every $\alpha \in F$ satisfies

$$\alpha^{p^n} = \alpha.$$

This says that every $\alpha \in F$ is a root of the polynomial $X^{p^n} - X \in \mathbb{Z}_p[X]$. The roots of $X^{p^n} - X$ make up the whole of $F$. Clearly, $F$ is a splitting field of $X^{p^n} - X$ over $\mathbb{Z}_p$, because $F$ contains all the roots of $X^{p^n} - X$ and no proper subfield of $F$ contains all these roots. But any two splitting fields of the same polynomial are isomorphic by the isomorphism extension theorem (Proposition 0.67), so any two fields with $p^n$ elements are isomorphic.

To address the *existence* of fields of size $p^n$, let $K$ be a splitting field of $X^{p^n} - X$ over $\mathbb{Z}_p$, and let $F$ be the set of roots of $X^{p^n} - X$ in $K$. Then $F$ is a finite set with at most $p^n$ elements, and it now turns out that $F$ is a field.

To see this, take $\alpha, \beta \in F$. Using the **Frobenius map** (more commonly known as the **freshman's dream**), we have

$$(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta,$$

so $\alpha \pm \beta \in F$. Also,

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta,$$

so $\alpha\beta \in F$. If $\alpha \neq 0$, then

$$(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1},$$

so $\alpha^{-1} \in F$, and hence $F$ is a field. Since $F$ is exactly the root set of $X^{p^n} - X$ in $K$, we have $F = K$.

At this point, one further issue remains: to conclude that $|F| = p^n$, we must know that $X^{p^n} - X$ has no repeated roots. We will verify that soon enough. For now, pretending that we *do* know that $X^{p^n} - X$ has no repeated roots, we summarize what we have learned:

**Proposition 0.73** For every prime $p$ and every integer $n \geq 1$, there is, up to isomorphism, one and only one field of size $p^n$.

The standard notation for the field of size $p^n$ is $\mathbb{F}_{p^n}$.

## Irreducibles over $\mathbb{Z}_p$

Given $n \geq 1$, does there exist an irreducible polynomial in $\mathbb{Z}_p[X]$ of degree $n$? The answer is not obvious! The existence of $\mathbb{F}_{p^n}$ answers this question.

The group $\mathbb{F}_{p^n}^*$ is cyclic, as we know. Let $\alpha \in \mathbb{F}_{p^n}^*$ be a generator. Then

$$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{p^n-2}, \alpha^{p^n-1} = 1$$

runs through all of $\mathbb{F}_{p^n}^*$, so

$$\mathbb{F}_{p^n} = \mathbb{Z}_p[\alpha].$$

But

$$[\mathbb{Z}_p[\alpha] : \mathbb{Z}_p] = [\mathbb{F}_{p^n} : \mathbb{Z}_p] = n,$$

so the minimal polynomial of $\alpha$ over $\mathbb{Z}_p$ is an irreducible of degree $n$. Moreover, this minimal polynomial divides $X^{p^n} - X$ in $\mathbb{Z}_p[X]$, because $\alpha$ is a root of $X^{p^n} - X$.

In fact, *every* irreducible polynomial in $\mathbb{Z}_p[X]$ of degree $n$ divides $X^{p^n} - X$. To see this, take an irreducible $f \in \mathbb{Z}_p[X]$ of degree $n$, and without loss of generality assume $f$ is monic. By Kronecker's theorem, some extension contains a root $\alpha$ of $f$; take $K = \mathbb{Z}_p[\alpha]$. Then of course

$$[K : \mathbb{Z}_p] = \deg f = n$$

since $f$, being irreducible and monic, is the minimal polynomial of $\alpha$ in $\mathbb{Z}_p[X]$. Hence $K$ is a field with $p^n$ elements, and therefore $K \cong \mathbb{F}_{p^n}$.

Hence every element of $K$, in particular $\alpha$, satisfies $X^{p^n} = X$. Since $f$ is the minimal polynomial of $\alpha$, it follows that

$$f \mid X^{p^n} - X, \quad \text{in } \mathbb{Z}_p[X].$$

The upshot is that to find all irreducibles of degree $n$ over $\mathbb{Z}_p$, we only need to factor $X^{p^n} - X$, although in practice this opens up a new can of worms.

However, we can still say more about its factors. First, if $d \mid n$ in $\mathbb{Z}$, then $X^{p^d} - X$ divides $X^{p^n} - X$

in $\mathbb{Z}_p[X]$. Indeed, write $n = dk$ with $k \geq 1$. Then

$$p^n - 1 = p^{dk} - 1 = (p^d)^k - 1 = (p^d - 1)\ell$$

for some positive integer $\ell$. Hence

$$X^{p^n-1} - 1 = (X^{p^d-1})^\ell - 1 = (X^{p^d-1} - 1)h$$

for some $h \in \mathbb{Z}_p[X]$, and multiplying by $X$ gives

$$X^{p^n} - X = (X^{p^d} - X)h, \quad \text{in } \mathbb{Z}_p[X].$$

Since every irreducible of degree $d$ divides $X^{p^d} - X$, we conclude that if $d \mid n$, then every irreducible of degree $d$ appears among the factors of $X^{p^n} - X$.

As it turns out, if $f$ is irreducible in $\mathbb{Z}_p[X]$ and $f \mid X^{p^n} - X$, then $\deg f$ must divide $n$. To see this, let $d = \deg f$, and let $\mathbb{F}_{p^n}$ be the splitting field of $X^{p^n} - X$. Since $f$ divides this polynomial, $f$ splits in $\mathbb{F}_{p^n}[X]$, so $f$ has a root $\alpha \in \mathbb{F}_{p^n}$. Then

$$\mathbb{Z}_p \subseteq \mathbb{Z}_p[\alpha] \subseteq \mathbb{F}_{p^n},$$

and

$$[\mathbb{Z}_p[\alpha] : \mathbb{Z}_p] = d.$$

By the tower theorem,

$$d \mid [\mathbb{F}_{p^n} : \mathbb{Z}_p] = n.$$

We summarize what we have learned:

**Proposition 0.74** The degree $d$ of every irreducible factor of $X^{p^n} - X$ divides $n$, and for each divisor $d$ of $n$, every irreducible polynomial of degree $d$ over $\mathbb{Z}_p$ divides $X^{p^n} - X$.

## The Subfields Of $\mathbb{F}_{p^n}$

While we are at it, we may as well determine the subfields of $\mathbb{F}_{p^n}$.

If $E$ is a subfield of $\mathbb{F}_{p^n}$, then $E$ has size $p^d$ for some $d \leq n$, and $d = [E : \mathbb{Z}_p]$. From

$$\mathbb{Z}_p \subseteq E \subseteq \mathbb{F}_{p^n},$$

the tower theorem gives

$$d \mid [\mathbb{F}_{p^n} : \mathbb{Z}_p] = n.$$

So only sizes $p^d$ with $d \mid n$ are possible. If $E$ and $L$ are two subfields of $\mathbb{F}_{p^n}$ of size $p^d$, then both are exactly the root set of $X^{p^d} - X$. Hence for each divisor $d$ of $n$, there is at most one subfield of size $p^d$.

Does such a subfield always exist when $d \mid n$? Most certainly. If $d \mid n$, then $X^{p^d} - X$ divides $X^{p^n} - X$ in $\mathbb{Z}_p[X]$. Since $\mathbb{F}_{p^n}$ is the splitting field (indeed the full root set) of $X^{p^n} - X$, the polynomial $X^{p^d} - X$ splits in $\mathbb{F}_{p^n}[X]$. As we will prove later, $X^{p^d} - X$ has no repeated roots. For now we use this fact. Let

$$E = \{\alpha \in \mathbb{F}_{p^n} : \alpha^{p^d} = \alpha\}.$$

Then $|E| = p^d$. Also, $E$ is a field. If $\alpha, \beta \in E$, then by the freshman's dream,

$$(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d} = \alpha + \beta,$$

so $\alpha + \beta \in E$. Similarly,

$$(\alpha\beta)^{p^d} = \alpha\beta,$$

and for $\alpha \neq 0$,

$$(\alpha^{-1})^{p^d} = \alpha^{-1}.$$

Thus $E$ is a subfield of $\mathbb{F}_{p^n}$ with size $p^d$.

When $d \mid n$, there is another way to get the unique subfield $E$ of size $p^d$ inside $\mathbb{F}_{p^n}$, and this method gives us more information about the subfield. First note that the group $\mathbb{F}_{p^n}^*$ is cyclic of order $p^n - 1$.

**Remark 0.75** For a cyclic group $G$ of order $m$, every subgroup is cyclic of order $\ell$ with $\ell \mid m$, and for each divisor $\ell$ there is exactly one subgroup of that order. If $x$ generates $G$, then the unique subgroup of order $\ell$ is generated by $x^{m/\ell}$.

Pick a generator $\alpha$ of $\mathbb{F}_{p^n}^*$. If $d \mid n$, then $p^d - 1 \mid p^n - 1$, so

$$\beta = \alpha^{(p^n-1)/(p^d-1)}$$

generates the unique subgroup $H \subseteq \mathbb{F}_{p^n}^*$ of order $p^d - 1$. Throwing in 0, we see that $E = H \cup \{0\}$ is the unique subfield of size $p^d$. Indeed, every $\gamma \in H$ satisfies $\gamma^{p^d-1} = 1$, so every $\gamma \in E$ satisfies $\gamma^{p^d} = \gamma$. Hence $E$ is precisely the field of roots of $X^{p^d} - X$.

Furthermore, $E = \mathbb{Z}_p[\beta]$, and the minimal polynomial of $\beta$ over $\mathbb{Z}_p$ has degree $[E : \mathbb{Z}_p] = d$. So

determining that minimal polynomial gives us a solid grasp on $E$.

## Control of the Degree of a Splitting Field

**Proposition 0.76** If $K$ is the splitting field of a polynomial $f \in F[X]$, then $[K : F]$ divides $n!$, where $n = \deg f$. Furthermore, if $f$ is irreducible, then $n$ divides $[K : F]$.

**Proof.** The second assertion is easier, so we begin there, using a familiar argument. Assume $f$ is irreducible of degree $n$, and let $\alpha \in K$ be a root of $f$. Then

$$F \subseteq F[\alpha] \subseteq K.$$

By the tower theorem, $[F[\alpha] : F]$ divides $[K : F]$. Since $f$ is irreducible (up to scaling to make it monic), $f$ is the minimal polynomial of $\alpha$, so

$$[F[\alpha] : F] = n.$$

Hence $n \mid [K : F]$. Now we prove the first assertion by induction on $n = \deg f$. If $n = 1$, then $K = F$, so $[K : F] = 1$ divides $1!$. Assume the statement is true for every splitting field of every polynomial of degree $< n$ over any base field. Let $f \in F[X]$ have degree $n$, and let $K$ be its splitting field. If $f$ is irreducible, choose a root $\alpha \in K$. Then

$$f = (X - \alpha)g$$

with $g \in K[X]$ and $\deg g = n - 1 < n$.

The intermediate field used in the induction is shown in Figure 7.


FIGURE 7

Because $f$ is irreducible, $[F[\alpha] : F] = n$. Also, $K$ is the splitting field of $g$ over $F[\alpha]$; after all, $K$

contains $\alpha$ along with the other roots of $f$, which are nothing but the roots of $g$. By the induction hypothesis,

$$[K : F[\alpha]] \mid (n-1)!.$$

Therefore, by the tower theorem,

$$[K : F] = [K : F[\alpha]]\,[F[\alpha] : F] = [K : F[\alpha]]\,n$$

divides $n!$. If $f$ is reducible, write $f = gh$ with $\deg g = m$, $\deg h = k$, and $1 \leq m, k < n$. Let $\alpha_1, \ldots, \alpha_m$ be the roots of $g$ in $K$, and $\beta_1, \ldots, \beta_k$ the roots of $h$ in $K$. Then

$$K = F[\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_k] = F[\alpha_1, \ldots, \alpha_m][\beta_1, \ldots, \beta_k].$$

Set

$$E = F[\alpha_1, \ldots, \alpha_m].$$

Then $E$ is the splitting field of $g$ over $F$, and $K$ is the splitting field of $h$ over $E$.

Figure 8 records this second extension tower.


FIGURE 8

By induction,

$$[E : F] \mid m! \qquad \text{and} \qquad [K : E] \mid k!.$$

Hence

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

divides $m!k!$. Since $m + k = n$,

$$\frac{n!}{m!k!} = \binom{n}{m} \in \mathbb{Z},$$

so $m!k!$ divides $n!$. Therefore $[K : F]$ divides $n!$. □

This result is useful but coarse, since $n!$ has a lot of divisors even when $n$ is not that big. So there remains a lot of wiggle room for what $[K : F]$ can be. Perhaps the most useful information

coming out of Proposition 0.76 is when $n = 3$ with $f$ irreducible. In that case, Proposition 0.76 tells us that if $K$ is the splitting field of $f$ in $F[X]$, then

$$3 \mid [K : F] \qquad \text{and} \qquad [K : F] \mid 6,$$

so the degree of the splitting field of an irreducible cubic is either 3 or 6.

**Example 0.77** For our old friend $f = X^3 - 2$ in $\mathbb{Q}[X]$, the splitting field is

$$\mathbb{Q}[\sqrt[3]{2}, e^{2\pi i/3}],$$

which has degree 6 over $\mathbb{Q}$.

**Exercise 0.78** Find an irreducible cubic in $\mathbb{Q}[X]$ whose splitting field has degree 3.

So the natural question is: given an irreducible cubic in $F[X]$, how can we tell whether its splitting field has degree 3 or 6? We will find out soon...

What about irreducible cubics over $\mathbb{Z}_p$? In that setting, the splitting field degree of an irreducible cubic is *always* 3. We can put our knowledge of finite fields to work.

Recall that $\mathbb{F}_{p^3}$ extends $\mathbb{Z}_p$ with

$$[\mathbb{F}_{p^3} : \mathbb{Z}_p] = 3,$$

and $\mathbb{F}_{p^3}$ is the set of all roots of $X^{p^3} - X$. If $f$ is an irreducible cubic in $\mathbb{Z}_p[X]$, then $f \mid X^{p^3} - X$, so $f$ splits over $\mathbb{F}_{p^3}$. Let $\alpha \in \mathbb{F}_{p^3}$ be a root of $f$. Then we get the tower

$$\mathbb{Z}_p \subseteq \mathbb{Z}_p[\alpha] \subseteq \mathbb{F}_{p^3}.$$

Since $f$ is the minimal polynomial of $\alpha$ (up to scaling),

$$[\mathbb{Z}_p[\alpha] : \mathbb{Z}_p] = \deg f = 3.$$

Thus $\mathbb{Z}_p[\alpha] = \mathbb{F}_{p^3}$, and because $f$ splits over $\mathbb{F}_{p^3}$, this field *is* the splitting field of $f$.

## Quadratic Extensions

**Definition 0.79** If $[K : F] = 2$, we call $K$ a **quadratic extension** of $F$.

Here is a useful observation about quadratic extensions, which, curiously enough, fails in fields of characteristic 2.

**Proposition 0.80** Assume $\mathrm{char}(F) \neq 2$. An extension $K$ of $F$ is quadratic if and only if $K$ is the splitting field of an irreducible polynomial of the form $X^2 - d$ in $F[X]$.

**Proof.** *From a splitting field to a quadratic extension.* First suppose $K$ is the splitting field of $X^2 - d$ over $F$, where $X^2 - d$ is irreducible. Let $\alpha \in K$ be a root, so $\alpha^2 = d$; that is, $\alpha = \sqrt{d}$ for some choice of square root in $K$. The other root is $-\alpha$, and since $\mathrm{char}(F) \neq 2$, these roots are distinct. Thus $X^2 - d$ splits over $F[\alpha]$, so $K = F[\alpha]$. Because $X^2 - d$ is irreducible, it is the minimal polynomial of $\alpha$, and therefore

$$[K : F] = [F[\alpha] : F] = 2.$$

*From a quadratic extension to a splitting field.* Now suppose $[K : F] = 2$. Pick $\alpha \in K \setminus F$. Then the minimal polynomial of $\alpha$ over $F$ has degree 2, say

$$g(X) = X^2 + bX + c \in F[X].$$

Since $\mathrm{char}(F) \neq 2$, define

$$\beta = \alpha + \frac{b}{2} \qquad \text{and} \qquad d = \frac{b^2}{4} - c.$$

Then, completing the square (!), we get

$$\beta^2 - d = \left(\alpha + \frac{b}{2}\right)^2 - \left(\frac{b^2}{4} - c\right) = \alpha^2 + b\alpha + c = 0.$$

So $\beta$ is a root of $X^2 - d$. Also $\beta \notin F$ because $\alpha \notin F$, so $X^2 - d$ is irreducible over $F$. Hence

$$[F[\beta] : F] = 2,$$

which forces $K = F[\beta]$. Since the other root is $-\beta$, the polynomial $X^2 - d$ splits over $K$, and $K$ is its splitting field. □

If $F$ has characteristic 2, Proposition 0.80 has no hope. For instance, if $F$ is finite, then the Frobenius map $x \mapsto x^2$ is an automorphism of $F$. So every $d \in F$ is a perfect square, say $d = a^2$, for some $a \in F$. Then the freshman's dream gives

$$X^2 - d = X^2 - a^2 = (X - a)^2,$$

so *all* polynomials of the form $X^2 - d$ are reducible when $F$ is a finite field of characteristic 2.

On the other hand, if $F$ is infinite, irreducible polynomials of the form $X^2 - d$ can exist.

**Example 0.81** In $F = \mathbb{Z}_2(t)$, the polynomial $X^2 - t$ is irreducible. If $\alpha$ is a root in some extension $K$ of $F$, then

$$(X - \alpha)^2 = X^2 - \alpha^2 = X^2 - t,$$

so $X^2 - t$ splits over $F[\alpha]$ with a repeated root.

Thus, in characteristic 2, a quadratic extension need not be the splitting field of a polynomial of the form $X^2 - d$. Still, every quadratic extension is the splitting field of *some* polynomial $X^2 + bX + c$ over $F$. We leave this as an exercise.

# 4. Separability

## The Issue of Repeated Roots

We need to settle when a polynomial $f \in F[x]$ can have repeated roots in its splitting field $K$.

If $f = g_1^{e_1} \cdots g_k^{e_k}$ with distinct irreducibles $g_i \in F[x]$, then the splitting field of $f$ is the same as the splitting field of $h = g_1 \cdots g_k$. Repeating a factor adds no new roots. Also, different $g_j$ contribute different roots in $K$, because the $g_j$ are pairwise coprime. In particular, from

$$\gcd(g_i, g_j) = 1 \text{ in } F[x],$$

we still get

$$\gcd(g_i, g_j) = 1 \text{ in } K[x].$$

So the real matter of concern is this: an irreducible $g \in F[x]$ can still have repeated roots in an extension of $F$.

**Example 0.82** Take

$$F = \mathbb{Z}_2(t),$$

the field of rational functions in an indeterminate $t$ over $\mathbb{Z}_2$. Consider $x^2 - t \in F[x]$.

This polynomial is irreducible in $F[x]$, because it has no root in $F$. If

$$\left(\frac{p(t)}{q(t)}\right)^2 = t$$

with $p(t), q(t) \in \mathbb{Z}_2[t]$, then $p(t)^2 = t\,q(t)^2$. But $\deg(p(t)^2)$ is even, while $\deg(tq(t)^2)$ is odd, a contradiction.

Let $K$ be the splitting field of $x^2 - t$, and let $\alpha \in K$ be a root. Then $\alpha^2 = t$, so in $K[x]$,

$$x^2 - t = x^2 - \alpha^2 = (x - \alpha)^2.$$

Hence $\alpha$ is a repeated root of an irreducible polynomial.

We might ask "so what?" Let's talk about what. This severely limits the possibilities for the $F$-automorphisms of $K$. Since $K = F[\alpha]$, let $\varphi : K \to K$ be an $F$-automorphism. Then

$$\varphi(\alpha)^2 = \varphi(\alpha^2) = \varphi(t) = t,$$

so $\varphi(\alpha)$ is a root of $x^2 - t$. But that polynomial has only one root, namely $\alpha$. Thus $\varphi(\alpha) = \alpha$.

Now every $\beta \in K$ has the form

$$\beta = a_0 + a_1\alpha + \cdots + a_n\alpha^n, \quad a_j \in F,$$

and therefore

$$\begin{aligned}\varphi(\beta) &= \varphi(a_0) + \varphi(a_1)\varphi(\alpha) + \cdots + \varphi(a_n)\varphi(\alpha)^n \\ &= a_0 + a_1\alpha + \cdots + a_n\alpha^n \\ &= \beta,\end{aligned}$$

because $\varphi$ fixes $F$ and $\alpha$. So $\varphi = \mathrm{id}_K$. Apart from the identity map, there are no other $F$-automorphisms of $K$.

## Derivatives

The main tool for detecting repeated roots is the derivative.

**Definition 0.83** If

$$f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n,$$

then the **derivative** of $f$ is

$$f' = a_1 + 2a_2X + 3a_3X^2 + \cdots + na_nX^{n-1} \in F[X].$$

If $f$ is constant, then $f' = 0$. But in characteristic $p$, $f'$ can vanish even for nonconstant polynomials.

**Example 0.84**

$$(X^{5p} + 2X^p - 4)' = 5p\,X^{5p-1} + 2p\,X^{p-1} = 0$$

in characteristic $p$.

For $f, g \in F[x]$, the usual rules hold:

$$(f \pm g)' = f' \pm g',$$
$$(fg)' = fg' + f'g.$$

We omit the utterly dreary verifications.

**Definition 0.85** If $f \in F[x]$ has a root $\alpha$ in an extension $K$, we say that $\alpha$ is a **repeated root** when $(X - \alpha)^2$ divides $f$ in $K[X]$.

**Proposition 0.86** A nonzero polynomial $f \in F[x]$ has a repeated root in some extension of $F$ if and only if $f$ and $f'$ are not coprime in $F[x]$.

**Proof.** Whenever $K$ is an extension containing a root $\alpha$ of $f$, we can write

$$f = (x - \alpha)g, \quad \text{for some } g \in K[x]. \tag{0.1}$$

Differentiating and using the product rule for derivatives gives

$$f' = (x - \alpha)g' + g. \tag{0.2}$$

*Not coprime implies a repeated root.* Suppose first that $f$ and $f'$ are not coprime in $F[x]$. Then $\gcd(f, f')$ is nonconstant. Let $K$ be a splitting field of $\gcd(f, f')$, and choose a root $\alpha$ of $\gcd(f, f')$. Then $\alpha$ is a root of both $f$ and $f'$. By (0.2), $\alpha$ is a root of $g$, and then (0.1) shows $(x - \alpha)^2 \mid f$ in $K[x]$. So $\alpha$ is a repeated root.

*A repeated root implies not coprime.* Suppose $\alpha$ is a repeated root of $f$ in some extension $K$ of $F$. Then $(x - \alpha)^2 \mid f$ in $K[x]$. By (0.1), we get $x - \alpha \mid g$ in $K[x]$. Then (0.2) gives $x - \alpha \mid f'$ in $K[x]$. If $f$ and $f'$ were coprime in $F[x]$, Bézout's identity would give $a, b \in F[x]$ such that $af + bf' = 1$. The same identity would hold in $K[x]$, which is impossible because $x - \alpha$ divides both terms on the left. Hence $f$ and $f'$ are not coprime in $F[x]$. □

The beauty of Proposition 0.86 is that we can predict the appearance of repeated roots in some extension of $F$ by just looking within $F[x]$.

**Example 0.87** Does

$$f = x^4 + 4x^3 + 8x^2 + 8x + 4$$

have a repeated root in $\mathbb{C}$?

Its derivative is

$$f' = 4x^3 + 12x^2 + 16x + 8.$$

A Euclidean algorithm computation gives

$$\gcd(f, f') = x^2 + 2x + 2.$$

So $f$ does have repeated roots in $\mathbb{C}$. In fact those repeated roots are the roots of $\gcd(f, f')$, namely $-1 \pm i$, by the quadratic formula.

By Proposition 0.86, if $f$ and $f'$ are coprime in $F[x]$, then $f$ has no repeated roots in any extension of $F$.

As we might recall, in the proof of existence of finite fields of all possible sizes $p^n$, we took $K$ to be the splitting field of $X^{p^n} - X$ over $\mathbb{Z}_p$, and then discovered that its roots fill all of $K$.

What was left to check was that $X^{p^n} - X$ has *exactly* $p^n$ distinct roots. We calculate

$$(X^{p^n} - X)' = p^n X^{p^n - 1} - 1 = -1, \quad \text{in } \mathbb{Z}_p[x].$$

Evidently, $X^{p^n} - X$ is coprime with $-1$. So $X^{p^n} - X$ does have $p^n$ roots, which are precisely the elements of $K$.

## Irreducibles Without Repeated Roots

**Definition 0.88** An irreducible polynomial $f \in F[x]$ is called **separable** if it has no repeated root in any extension of $F$. Equivalently, $f$ is separable if and only if $f$ and $f'$ are coprime.

If $f$ is irreducible and $f' \neq 0$, then $f$ and $f'$ are coprime. Indeed, any common divisor $h$ satisfies

$$\deg h \leq \deg f' < \deg f,$$

so $h$ must be constant. If instead $f' = 0$, then $\deg f \geq 2$ (a nonzero linear polynomial cannot have zero derivative). In that case,

$$\gcd(f, f') = \gcd(f, 0) = f,$$

so $f$ is not separable. In some field extension (e.g., in the splitting field of $f$), we will encounter a repeated root of $f$.

We can summarize what we have learned as follows.

**Proposition 0.89** An irreducible $f \in F[x]$ is separable if and only if $f' \neq 0$.

A useful consequence emerges:

**Proposition 0.90** If $F$ has characteristic 0, then every irreducible polynomial in $F[x]$ is separable.

**Proof.** If $f$ is irreducible, then $\deg f \geq 1$, so $f' \neq 0$ in characteristic 0. Apply Proposition 0.89. □

The term "separable" is apt: if an irreducible polynomial $f$ has degree $n$, then in its splitting field $K$ we can write

$$f = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

with all $\alpha_j$ distinct. So no two roots are on top of each other: they are "separated."

In light of Proposition 0.90, the issue of separability comes down to fields of prime characteristic $p$. In such fields, we can have irreducibles with zero derivative, and those are precisely the inseparable irreducibles.

## Polynomials with Zero Derivative in Characteristic $p$

**Proposition 0.91** Let $F$ have prime characteristic $p$. For $f \in F[x]$, we have $f' = 0$ if and only if

$$f(x) = g(x^p)$$

for some $g \in F[x]$.

Before the proof, notice that the condition $f(x) = g(x^p)$ means precisely that only powers $x^j$ appearing in the expansion of $f$ are those with $p \mid j$.

**Example 0.92**

$$x^{3p^2} + x^{7p} + 2x^{4p} + 5x^p + 7 = (x^p)^{3p} + (x^p)^7 + 2(x^p)^4 + 5(x^p) + 7(x^p)^0.$$

**Proof of Proposition 0.91.** *If $f(x) = g(x^p)$, then $f' = 0$.* Suppose

$$g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

then

$$f(x) = a_n x^{pn} + a_{n-1}x^{p(n-1)} + \cdots + a_1 x^p + a_0,$$

so

$$f'(x) = pn\, a_n x^{pn-1} + p(n-1)a_{n-1}x^{p(n-1)-1} + \cdots + pa_1 x^{p-1} = 0.$$

*If $f' = 0$, then $f(x) = g(x^p)$.* Write

$$f = \sum_j a_j x^j.$$

Then

$$0 = f' = \sum_j j a_j x^{j-1},$$

so $ja_j = 0$ for every $j$. If $j \not\equiv 0 \pmod{p}$, then $j \neq 0$ in $F$, and hence $a_j = 0$. Therefore only powers $x^j$ with $p \mid j$ appear, so $f(x) = g(x^p)$ for some $g \in F[x]$. □

We have seen that in characteristic 0, every irreducible $f \in F[x]$ is separable. Such $f$ splits in its splitting field with no repeated roots. In other words, the number of roots of $f$ in its splitting field *equals* $\deg f$.

**Question 0.93** In characteristic $p$, can every irreducible polynomial in $F[x]$ be separable?

Recall that the **Frobenius map** is

$$\begin{aligned} \sigma : F &\longrightarrow F \\ a &\longmapsto a^p. \end{aligned}$$

It is always a homomorphism and always injective, but not always surjective.

For example, for $\sigma : \mathbb{Z}_p(t) \to \mathbb{Z}_p(t)$ one cannot have $t = \sigma(h)$, because that would imply

$$t = \left(\frac{a(t)}{b(t)}\right)^p$$

for polynomials $a(t), b(t) \in \mathbb{Z}_p[t]$, hence

$$b(t)^p t = a(t)^p.$$

The left side is a polynomial of degree $p \deg b(t) + 1 \equiv 1 \pmod{p}$, while the right side is a polynomial of degree $p \deg a(t) \equiv 0 \pmod{p}$, which is impossible. So $\sigma$ is not onto for $\mathbb{Z}_p(t)$.

But sometimes, the Frobenius map *is* surjective, especially if $F$ is finite. In that case, the pigeonhole principle forces $\sigma$ to be a bijection, so $\sigma$ is an automorphism of $F$.

Next up is the main result of this section.

**Proposition 0.94** Let $F$ have characteristic $p$. Every irreducible polynomial in $F[x]$ is separable if and only if the Frobenius map $\sigma : F \to F$ is onto.

**Proof.** *Forward implication.* Assume first that $\sigma$ is not onto. Choose $b \in F \setminus \sigma(F)$. Then $x^p - b$ has no root in $F$. Let $K$ be the splitting field of $x^p - b$, and let $\theta \in K$ be a root. Since $\theta^p = b$,

$$x^p - b = x^p - \theta^p = (x - \theta)^p$$

in $K[x]$, so $\theta$ is a repeated root. Let $g \in F[x]$ be the minimal polynomial of $\theta$. Because $g \mid x^p - b$ in $F[x]$, in $K[x]$ we have

$$g = (x - \theta)^k$$

for some $k$ with $2 \leq k \leq p$. Expanding gives

$$g = x^k - k\theta x^{k-1} + \cdots .$$

Since coefficients lie in $F$, we have $k\theta \in F$. If $k \neq p$, then $k$ is invertible in $\mathbb{Z}_p$, so $\theta \in F$, contradiction. Hence $k = p$, and therefore $g = x^p - b$ is irreducible in $F[x]$ but not separable. So if the Frobenius map is not onto, not every irreducible is separable.

*Reverse implication.* Now assume the Frobenius map is onto. Let $f \in F[x]$ satisfy $f' = 0$. By Proposition 0.91,

$$f(x) = g(x^p) = a_n x^{pn} + a_{n-1} x^{p(n-1)} + \cdots + a_1 x^p + a_0.$$

Since the Frobenius map is onto, each $a_j = b_j^p$ for some $b_j \in F$. Then

$$f(x) = b_n^p x^{pn} + b_{n-1}^p x^{p(n-1)} + \cdots + b_1^p x^p + b_0^p = \left(b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0\right)^p$$

since the Frobenius map is a homomorphism of $F[x]$ (this is the freshman's dream). Obviously $f$ is reducible, because it is a perfect $p$-th power. In particular, if $f$ is irreducible, then $f' \neq 0$. By Proposition 0.89, $f$ is separable. Hence every irreducible in $F[x]$ is separable. □

An important corollary follows:

**Proposition 0.95** If $F$ is finite, then every irreducible polynomial in $F[x]$ is separable.

**Proof.** For finite $F$, the Frobenius map is onto. Apply Proposition 0.94. □

Fields over which every irreducible polynomial is separable are called **perfect fields** in the literature. This includes all fields of characteristic 0 and all finite fields. In our opinion, such terminology lacks imagination. After all, perfection is in the eye of the beholder. Why not call

splitting fields perfect? Some might feel that $\mathbb{Z}_2(t)$ should be called perfect. But we will go along with the crowd.

We might ask if there are perfect fields other than finite fields and fields of characteristic 0. This is a more specialized question, but the answer is yes.

For example, let $F$ be the algebraic closure of $\mathbb{Z}_p$. Without constructing $F$, we take it to be an algebraic extension of $\mathbb{Z}_p$ whose only algebraic extension is $F$ itself. Then $F$ is an infinite field of characteristic $p$ which is perfect, because the Frobenius map on $F$ is onto. Indeed, take $\beta \in F$. The splitting field $K$ of the polynomial $x^p - \beta$ in $F[x]$ is an algebraic extension of $F$. Since $F$ is algebraically closed, $K = F$. So $x^p - \beta$ splits over $F$. In particular, there is some $\alpha \in F$ such that $\alpha^p - \beta = 0$. That is, $\beta = \alpha^p = \sigma(\alpha)$.

More easily, the only irreducible polynomials in $F[x]$ are linear, and linear polynomials are always separable. So $F$ is perfect. 😕

## Separability for Arbitrary Polynomials

In defining separability for a general polynomial $f \in F[x]$, we have two options:

*Option 1.* We can say that $f \in F[x]$ is separable when $f$ has no repeated root in its splitting field. This is the same as saying that $f$ is coprime with its derivative $f'$ in $F[x]$.

*Option 2.* We can say that $f$ is separable when each of the irreducible factors $g$ of $f$ in $F[x]$ is separable. This means that if $g$ is irreducible and $g \mid f$ in $F[x]$, then $g$ has no repeated root in its splitting field (which is part of the splitting field of $f$). That is, $g' \neq 0$.

Some authors use Option (1). Some authors use Option (2). But the concepts are *not* the same. For instance,

$$(x^2 + 1)^3(x^2 - 2)^5 \in \mathbb{Q}[x]$$

is separable under Option (2), but not under Option (1).

If

$$f = g_1 g_2 \cdots g_k$$

with *distinct* irreducibles $g_j$, then the two notions agree. Often such polynomials are called **square-free**. For a square-free $f = g_1 \cdots g_k \in F[x]$ with splitting field $K$, let $n$ be the number of

roots of $f$ in $K$, and let $n_j$ be the number of roots of $g_j$ in $K$. Clearly,

$$n = n_1 + n_2 + \cdots + n_k \tag{0.3}$$

and

$$\deg f = \deg g_1 + \deg g_2 + \cdots + \deg g_k.$$

Now Option (1) is equivalent to $n = \deg f$, while Option (2) is equivalent to $n_j = \deg g_j$ for all $j$. But (0.3) reveals that Option (1) holds if and only if Option (2) holds. So for square-free polynomials, the two notions of separability coincide.

We also notice that if

$$f = g_1^{e_1} \cdots g_k^{e_k} \in F[x]$$

with irreducible factors $g_j$ repeated $e_j$ times, then the splitting field $K$ of $f$ is the same as the splitting field of the square-free

$$h = g_1 \cdots g_k,$$

where the irreducible factors of $f$ are taken only once.

Since (as far as making splitting fields is concerned) only square-free polynomials are needed, the choice of Option (1) or Option (2) is not actually that important. But we are mathematicians, and we must make a choice. We shall adopt Option (2) and declare $f$ to be separable if every one of its irreducible factors in $F[x]$ is separable.

One practical advantage of using Option (2) is immediate: if $F$ has characteristic 0 or if $F$ is finite, then *all* polynomials in $F[x]$ are separable in this sense.

Here is a little easy item that will come in handy later:

**Proposition 0.96** If $f \in F[x]$ is separable with splitting field $K$, and $E$ is an intermediate field with $F \subseteq E \subseteq K$, then $f$ remains separable as a polynomial in $E[x]$.

**Proof.** Let $h \in E[x]$ be irreducible with $h \mid f$ in $E[x]$. We must show $h$ has no repeated root in $K$. There *has to be* an irreducible $g \in F[x]$ such that $g \mid f$ in $F[x]$ and $h \mid g$ in $E[x]$; hence $h \mid g$ in $K[x]$ as well. If $(x-\theta)^2 \mid h$ in $K[x]$ for some $\theta \in K$, then $(x-\theta)^2 \mid g$ in $K[x]$, contradicting separability of $f$ over $F$. Therefore $h$ has no repeated root, and $f$ is separable over $E$. □

## 5. The Galois Group of a Field Extension

The Galois group is easy to define, and harder to understand.

**Definition 0.97** If $K$ extends $F$, the set of all $F$-automorphisms $\varphi : K \to K$ (that is, maps such that $\varphi(a) = a$ for all $a \in F$) is a group under composition. We shall call this group the **Galois group** of the extension and denote it by $\mathrm{Gal}(K/F)$. Some books write $\mathrm{Aut}(K/F)$.

**Example 0.98**

$$\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = \langle 1 \rangle,$$

the trivial group.

To see this, let $\phi : \mathbb{R} \to \mathbb{R}$ be a $\mathbb{Q}$-automorphism, so that for each $r \in \mathbb{Q}$, we have $\phi(r) = r$. First, $\phi$ preserves squares: if $x > 0$, then $x = y^2$ for some nonzero $y \in \mathbb{R}$, so

$$\phi(x) = \phi(y^2) = \phi(y)^2 > 0.$$

Thus $\phi$ also preserves positivity on $\mathbb{R}$: if $x > 0$, then $\phi(x) > 0$. Now, if $x < 0$, then $-x > 0$, so $\phi(-x) > 0$, and thus $\phi(x) < 0$. We conclude that $\phi$ preserves order on $\mathbb{R}$. Now, let $x \in \mathbb{R}$. For any rational $q < x$, order preservation means that $q = \phi(q) < \phi(x)$. Similarly, for any rational $q > x$, we have $\phi(x) < \phi(q) = q$. So $\phi(x)$ lies between all rational numbers less than $x$ and all rational numbers greater than $x$. By the density of $\mathbb{Q}$ in $\mathbb{R}$, this forces $\phi(x) = x$. Since $x$ was arbitrary, $\phi$ is the identity map on $\mathbb{R}$, and thus $\mathrm{Gal}(\mathbb{R}/\mathbb{Q})$ is the trivial group.

**Exercise 0.99** Show that $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is the two element group consisting of the identity map $z \mapsto z$ and the conjugation map $z \mapsto \overline{z}$.

**Example 0.100** If $K = \mathbb{Q}[\sqrt[3]{2}]$, what is $\mathrm{Gal}(K/\mathbb{Q})$?

If $\varphi : K \to K$ is a $\mathbb{Q}$-automorphism, then the identity $(\sqrt[3]{2})^3 = 2$ gives

$$\big(\varphi(\sqrt[3]{2})\big)^3 = \varphi\big((\sqrt[3]{2})^3\big) = \varphi(2) = 2.$$

So $\varphi(\sqrt[3]{2})$ is one of the three roots of $X^3 - 2$. One of those roots is $\sqrt[3]{2}$, but the other two roots are

$$\sqrt[3]{2}e^{2\pi i/3} \qquad \text{and} \qquad \sqrt[3]{2}e^{-2\pi i/3},$$

which are not real numbers. Since $K \subseteq \mathbb{R}$, we see that these other two roots are not in $K$. Thus

$$\varphi(\sqrt[3]{2}) = \sqrt[3]{2}.$$

Then every $\alpha$ in $K$ looks like

$$\alpha = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2, \quad a, b, c \in \mathbb{Q}.$$

So

$$\begin{aligned}\varphi(\alpha) &= \varphi(a) + \varphi(b)\varphi(\sqrt[3]{2}) + \varphi(c)\varphi(\sqrt[3]{2})^2 \\ &= a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \\ &= \alpha,\end{aligned}$$

since $\varphi$ fixes $\mathbb{Q}$ and $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$. We have just learned that $\mathrm{Gal}(K/\mathbb{Q})$ is the trivial group.

**Example 0.101** If $\omega = e^{2\pi i/5}$, its minimal polynomial is

$$g(X) = X^4 + X^3 + X^2 + X + 1.$$

The splitting field of $g$ over $\mathbb{Q}$ is $K = \mathbb{Q}[\omega]$.

We now find $\mathrm{Gal}(K/\mathbb{Q})$. If $\varphi : K \to K$ is a $\mathbb{Q}$-automorphism, the equation

$$\omega^4 + \omega^3 + \omega^2 + \omega + 1 = 0$$

leads to

$$0 = \varphi(\omega)^4 + \varphi(\omega)^3 + \varphi(\omega)^2 + \varphi(\omega) + 1.$$

Thus $\varphi(\omega)$ is one of the four roots of $g$, which are

$$\omega, \qquad \omega^2, \qquad \omega^3, \qquad \text{and} \qquad \omega^4.$$

Figure 9 shows their positions among the fifth roots of unity.

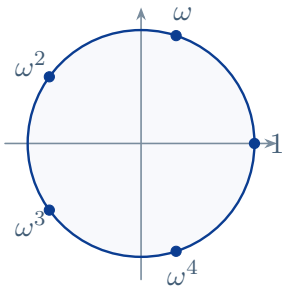



FIGURE 9

For each $j = 1, 2, 3, 4$ does there exist a $\mathbb{Q}$-automorphism $\varphi : K \to K$ such that

$$\varphi(\omega) = \omega^j?$$

Yes, by the isomorphism extension theorem, because $\omega$ and $\omega^j$ are conjugates and $K$ is a splitting field.

So far we have learned that $\mathrm{Gal}(K/\mathbb{Q})$ has order 4. Furthermore, $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic. Indeed, let $\varphi$ be given by

$$\varphi : \omega \mapsto \omega^2.$$

Then

$$\begin{aligned}
\varphi^2 &: \omega \mapsto \omega^2 \mapsto (\omega^2)^2 = \omega^4, \\
\varphi^3 &: \omega \mapsto \omega^4 \mapsto (\omega^2)^4 = \omega^8 = \omega^5\omega^3 = \omega^3, \\
\varphi^4 &: \omega \mapsto \omega^3 \mapsto (\omega^2)^3 = \omega^6 = \omega^5\omega = \omega.
\end{aligned}$$

So $\mathrm{Gal}(K/\mathbb{Q})$ is a cyclic group of order 4.

The few examples so far have all been abelian groups. But rest assured that nonabelian Galois groups are out there.

## Galois Groups Preserve Roots

If $\varphi \in \mathrm{Gal}(K/F)$ (that is, $\varphi : K \to K$ is an $F$-automorphism) and $f \in F[X]$ has a root $\alpha$ in $K$, then $\varphi(\alpha)$ must be a root of $f$ too. We have seen this before, but here it is again.

Write

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \quad a_j \in F.$$

Then

$$\begin{aligned} f(\varphi(\alpha)) &= \sum_j a_j \varphi(\alpha)^j \\ &= \sum_j \varphi(a_j)\varphi(\alpha)^j \quad \text{since } \varphi \text{ fixes } F \\ &= \varphi\left(\sum_j a_j \alpha^j\right) \quad \text{since } \varphi \text{ is an automorphism} \\ &= \varphi(f(\alpha)) \\ &= \varphi(0) = 0. \end{aligned}$$

## Galois Groups and Generators

Galois groups are determined by what they do to generators of the field extension. Suppose $K = F[\alpha_1, \alpha_2, \ldots, \alpha_n]$ and $\varphi : K \to K$ is an $F$-automorphism of $K$. Every $\alpha$ in $K$ takes the form

$$\alpha = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}, \tag{0.4}$$

with $a_{i_1,\ldots,i_n} \in F$ and $i_j \geq 0$. Then

$$\varphi(\alpha) = \sum_{i_1,\ldots,i_n} \varphi(a_{i_1,\ldots,i_n})\varphi(\alpha_1)^{i_1} \cdots \varphi(\alpha_n)^{i_n} = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} \varphi(\alpha_1)^{i_1} \cdots \varphi(\alpha_n)^{i_n},$$

since $\varphi$ fixes $F$. By looking at this, we see that $\varphi$ is fully determined on $K$ by its finitely many values $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$. In other words, if $\varphi, \psi \in \mathrm{Gal}(K/F)$ and $\varphi(\alpha_j) = \psi(\alpha_j)$ for all $j = 1, \ldots, n$, then $\varphi = \psi$ on all of $K$. As long as we know in advance that $\varphi$ is an automorphism of $K$, we can refer to $\varphi$ as *the* automorphism that sends each $\alpha_j$ to $\varphi(\alpha_j)$.

The preceding observations provide an important insight into the Galois group of a splitting field. Let $K$ be the splitting field of some polynomial $f$ in $F[X]$. Then $K = F[\alpha_1, \ldots, \alpha_n]$, where the $\alpha_j$ are the distinct roots in $K$ of $f$. For now we do not insist that $\deg f = n$; perhaps $f$ has repeated roots. Let

$$\Delta = \{\alpha_1, \ldots, \alpha_n\}$$

be the set of roots of $f$.

There is the important group $S(\Delta)$ consisting of all permutations of $\Delta$, more commonly known as the **symmetric group**. The order of $S(\Delta)$ is $n!$.

Since every $\varphi \in \mathrm{Gal}(K/F)$ sends each root $\alpha_j$ to another $\alpha_i$, and since $\varphi$ is one-to-one and $\Delta$ is finite, the restriction $\varphi|_\Delta$ becomes a permutation of $\Delta$, that is, $\varphi|_\Delta \in S(\Delta)$. The restriction to $\Delta$ makes a group homomorphism:

$$\begin{aligned} \Phi : \mathrm{Gal}(K/F) &\longrightarrow S(\Delta) \\ \varphi &\longmapsto \varphi|_\Delta. \end{aligned}$$

This $\Phi$ is an injection because each $\varphi$ is determined by what $\varphi$ does to the generators $\alpha_1, \ldots, \alpha_n$ of $K$.

To see this last important claim more formally, let $\varphi \in \ker \Phi$. Then $\varphi|_\Delta$ is the identity permutation on $\Delta$. In other words, $\varphi(\alpha_j) = \alpha_j$ for all $j$. Then, by looking back at (0.4), we see that $\varphi(\alpha) = \alpha$ for all $\alpha$ in $K$.

So the Galois group of the splitting field of each $f$ in $F[X]$ embeds, via the restriction map, into a subgroup of the group of permutations $S(\Delta)$ of the set of roots $\Delta$ of $f$. In the case of a splitting field, this tells us that the order of $\mathrm{Gal}(K/F)$ is finite and divides $n!$, where $n$ is the number of roots of $f$ inside its splitting field.

**Example 0.102** To illustrate the preceding items, let us calculate the Galois group of the splitting field of $X^3 - 2$ over $\mathbb{Q}$.

The roots of this polynomial are

$$\alpha, \qquad \alpha\omega, \qquad \text{and} \qquad \alpha\omega^2,$$

where $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$. The splitting field is

$$K = \mathbb{Q}[\alpha, \alpha\omega, \alpha\omega^2],$$

which by inspection is the same as $\mathbb{Q}[\alpha, \omega]$.

The three roots are plotted in Figure 10.

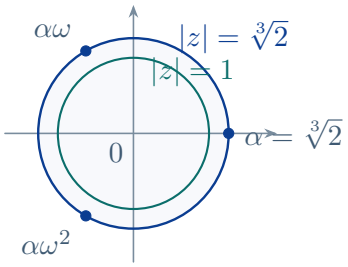



FIGURE 10

By looking at the tower

$$\mathbb{Q} \subseteq_3 \mathbb{Q}[\alpha] \subseteq_2 \mathbb{Q}[\alpha][\omega] = K,$$

with degrees as indicated based on past calculations, we see that $[K : \mathbb{Q}] = 6$. If $\varphi : K \to K$ is a $\mathbb{Q}$-automorphism, the equations $\alpha^3 = 2$ and $\omega^2 + \omega + 1 = 0$ give

$$\varphi(\alpha)^3 = \varphi(\alpha^3) = \varphi(2) = 2,$$
$$\varphi(\omega)^2 + \varphi(\omega) + \varphi(1) = \varphi(\omega^2 + \omega + 1) = \varphi(0) = 0.$$

Thus $\varphi(\alpha)$ is one of

$$\alpha, \qquad \alpha\omega, \qquad \text{and} \qquad \alpha\omega^2,$$

and $\varphi(\omega)$ is one of

$$\omega \qquad \text{and} \qquad \omega^2.$$

Thus, if $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$, then $\varphi$ can be described by one of the following six possible actions on $\alpha$ and $\omega$:

1. $\alpha \mapsto \alpha$, $\omega \mapsto \omega$;
2. $\alpha \mapsto \alpha\omega$, $\omega \mapsto \omega$;
3. $\alpha \mapsto \alpha\omega^2$, $\omega \mapsto \omega$;
4. $\alpha \mapsto \alpha$, $\omega \mapsto \omega^2$;
5. $\alpha \mapsto \alpha\omega$, $\omega \mapsto \omega^2$;
6. $\alpha \mapsto \alpha\omega^2$, $\omega \mapsto \omega^2$.

At this point we cannot conclude that these six actions on $\alpha, \omega$ give $\mathrm{Gal}(K/\mathbb{Q})$, because for

each action we need to know there exists a $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ that gives that action. In some other examples this might not even be true. But for our $X^3 - 2$ it is true.

We verify that there exists $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ such that

$$\varphi(\alpha) = \alpha\omega \qquad \text{and} \qquad \varphi(\omega) = \omega^2,$$

which is Possibility (5). Since $\alpha$ and $\alpha\omega$ are $\mathbb{Q}$-conjugates, there is a $\mathbb{Q}$-isomorphism

$$\varphi : \mathbb{Q}[\alpha] \to \mathbb{Q}[\alpha\omega]$$

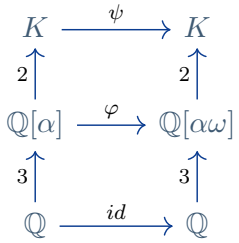
such that $\varphi(\alpha) = \alpha\omega$. This follows from the isomorphism extension theorem. Now $K$ remains the splitting field of $X^3 - 2$ over both $\mathbb{Q}[\alpha]$ and $\mathbb{Q}[\alpha\omega]$. The minimal polynomial of $\omega$ over $\mathbb{Q}[\alpha]$ is still

$$g = X^2 + X + 1.$$

The $\varphi$-transform of $g$ in $\mathbb{Q}[\alpha\omega][X]$ remains $g$, and $g$ is the minimal polynomial of $\omega^2$ over $\mathbb{Q}[\alpha\omega]$.

By the isomorphism extension theorem, there is an automorphism $\psi : K \to K$ such that

$$\psi|_{\mathbb{Q}[\alpha]} = \varphi \qquad \text{and} \qquad \psi(\omega) = \omega^2.$$




Check this closely. This $\psi$ in $\mathrm{Gal}(K/\mathbb{Q})$ is the one we want, that is,

$$\psi(\alpha) = \alpha\omega \qquad \text{and} \qquad \psi(\omega) = \omega^2.$$

In a similar way, we can confirm that for every one of the six possible ways that a $\mathbb{Q}$-automorphism of $K$ can act on $\alpha, \omega$, there does exist an automorphism to carry out that action. Of course, Possibility (1) is trivial to see.

We just learned that the order of $\mathrm{Gal}(K/\mathbb{Q})$ is 6. The fact that 6 is also the degree $[K : \mathbb{Q}]$

is no coincidence, as we shall discover.

Let $\Delta = \{\alpha, \alpha\omega, \alpha\omega^2\}$ be the set of roots of $X^3 - 2$. Remember that $S(\Delta)$, the group of permutations of three things, has order 6. Thus the restriction map

$$\Phi : \mathrm{Gal}(K/\mathbb{Q}) \to S(\Delta)$$

is onto. So in this example the Galois group is isomorphic to the nonabelian group $S_3$ of permutations on three letters.

For instance, the $\mathbb{Q}$-automorphism $\varphi : K \to K$ given by Possibility (5) implements the following permutation of $\Delta$:

$$\begin{aligned} \alpha &\mapsto \alpha\omega, \\ \alpha\omega &\mapsto (\alpha\omega)\omega^2 = \alpha\omega^3 = \alpha, \\ \alpha\omega^2 &\mapsto (\alpha\omega)(\omega^2)^2 = \alpha\omega^5 = \alpha\omega^2\omega^3 = \alpha\omega^2. \end{aligned}$$

This is the 2-cycle that interchanges $\alpha$ with $\alpha\omega$.

## The Irreducible Case

Here is an extra observation about the Galois group for the splitting field of an irreducible polynomial. Suppose $f \in F[X]$ is irreducible. Let $K$ be the splitting field of $f$, and let $\Delta$ be the finite set of roots of $f$ in $K$. We have the restriction map

$$\begin{aligned} \Phi : \mathrm{Gal}(K/F) &\longrightarrow S(\Delta) \\ \varphi &\longmapsto \varphi|_\Delta. \end{aligned}$$

This is a one-to-one group homomorphism.

Pick two roots $\alpha, \beta \in \Delta$. Since $f$ is irreducible, $\alpha$ and $\beta$ are $F$-conjugates with minimal polynomial $f$, after making $f$ monic if necessary. By the isomorphism extension theorem, there is an automorphism $\varphi : K \to K$ such that $\varphi|_F = \mathrm{id}$ on $F$ and $\varphi(\alpha) = \beta$. Therefore, for any two roots in $\Delta$, there is a $\varphi \in \mathrm{Gal}(K/F)$ that maps one to the other.

Thus $\mathrm{Gal}(K/F)$ acts transitively on the set $\Delta$ of roots of $f$. In the jargon of group theory, we say that $\mathrm{Gal}(K/F)$ embeds into a transitive subgroup of $S(\Delta)$. If $\Delta$ has $n$ roots, then $S(\Delta)$ is the familiar symmetric group $S_n$ of permutations on $n$ letters. So Galois groups of splitting fields of irreducible polynomials are transitive subgroups of $S_n$.

## An Upper Bound On the Order of the Galois Group

Now it is time to get to the core theorems of Galois theory, painful as they may be.

We first establish an upper bound on the order of $\mathrm{Gal}(K/F)$, using the absolute value notation

$$|\mathrm{Gal}(K/F)|$$

for the order of the Galois group.

**Proposition 0.103** If the degree of $K$ over $F$ is finite, then

$$|\mathrm{Gal}(K/F)| \leq [K : F].$$

**Proof.** It is easier for our proof by induction to show something a bit more general. We will prove that if $L$ is any extension of $F$, then the number of $F$-maps $\varphi : K \to L$ is at most $[K : F]$.

Since $[K : F] < \infty$, we may write

$$K = F[\alpha_1, \ldots, \alpha_n]$$

for some $\alpha_j \in K$ that are algebraic over $F$. We carry out an induction on the number $n$ of $\alpha_j$ used to generate $K$.

If $n = 0$, then $K = F$ and there is exactly one $F$-map $K \to L$. Suppose

$$E = F[\alpha_1, \ldots, \alpha_{n-1}] \qquad \text{and} \qquad K = E[\alpha_n].$$

By the induction hypothesis, the number of $F$-maps $\varphi : E \to L$ is at most $[E : F]$. Every $F$-map $\psi : K \to L$ is an extension of some $F$-map $\varphi : E \to L$. Given such a $\varphi : E \to L$, how many extensions $\psi : K \to L$ could there possibly be? We have $K = E[\alpha_n]$. If $g$ in $E[X]$ is the minimal polynomial of $\alpha_n$, let $\varphi(g)$ be its $\varphi$-transform in $L[X]$.

Now $\alpha_n$ is a root of $g$. Thus $\psi(\alpha_n)$ is a root of $\varphi(g)$. Indeed, write

$$g = a_k X^k + \cdots + a_1 X + a_0$$

in $E[X]$. Then

$$\begin{aligned} \varphi(g)(\psi(\alpha_n)) &= \varphi(a_k)\psi(\alpha_n)^k + \cdots + \varphi(a_1)\psi(\alpha_n) + \varphi(a_0) \\ &= \psi(a_k)\psi(\alpha_n)^k + \cdots + \psi(a_1)\psi(\alpha_n) + \psi(a_0) \end{aligned}$$

$$= \psi(a_k\alpha_n^k + \cdots + a_1\alpha_n + a_0)$$
$$= \psi(0) = 0.$$

Also,

$$\deg \varphi(g) = \deg g = [E[\alpha_n] : E] = [K : E].$$

So the number of options for $\psi(\alpha_n)$ is at most $[K : E]$. This means that each $F$-map $\varphi : E \to L$ has at most $[K : E]$ extensions $\psi : K \to L$. Since there are at most $[E : F]$ such maps $\varphi$, the total number of $F$-maps $K \to L$ is at most

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

as required. □

## The Fixed Field of a Galois Group

**Definition 0.104** If $H$ is a group of automorphisms of a field $K$, the set

$$\mathrm{Fix}(H) = \{\alpha \in K : \varphi(\alpha) = \alpha \text{ for all } \varphi \in H\}$$

is a subfield of $K$, known as the **fixed field** of $H$.

Every element of $F$ is fixed by every $F$-automorphism of $K$, so

$$F \subseteq \mathrm{Fix}(\mathrm{Gal}(K/F)).$$

This inclusion can at times be proper.

**Example 0.105** For $K = \mathbb{Q}[\sqrt[3]{2}]$, we saw in Example 0.100 that $\mathrm{Gal}(K/\mathbb{Q})$ is the trivial group. The trivial group fixes all of $K$, so

$$\mathrm{Fix}(\mathrm{Gal}(K/\mathbb{Q})) = K \neq \mathbb{Q}.$$

**Example 0.106** Take our old friend

$$K = \mathbb{Q}[\alpha, \omega], \qquad \alpha = \sqrt[3]{2}, \qquad \text{and} \qquad \omega = e^{2\pi i/3}.$$

This $K$ is the splitting field of $X^3 - 2$, whose roots are $\alpha, \alpha\omega, \alpha\omega^2$. We saw that $[K : \mathbb{Q}] = 6$

by looking at the tower

$$\mathbb{Q} \subseteq \mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\alpha][\omega] = K.$$

We also saw in Example 0.102 that $\mathrm{Gal}(K/\mathbb{Q})$ is a group of order 6 determined by the six actions on $\alpha$ and $\omega$ described earlier.

A basis for $K$ over $\mathbb{Q}$ is given by

$$1,\ \alpha,\ \alpha^2,\ \omega,\ \alpha\omega,\ \alpha^2\omega,$$

as can be seen from the above tower. Now suppose

$$\beta \in \mathrm{Fix}(\mathrm{Gal}(K/\mathbb{Q})).$$

Thus $\varphi(\beta) = \beta$ for all $\mathbb{Q}$-automorphisms of $K$. Write

$$\beta = a_1 + a_2\alpha + a_3\alpha^2 + a_4\omega + a_5\alpha\omega + a_6\alpha^2\omega, \quad a_j \in \mathbb{Q}.$$

Take $\varphi$ in $\mathrm{Gal}(K/\mathbb{Q})$ given by

$$\varphi(\alpha) = \alpha \qquad \text{and} \qquad \varphi(\omega) = \omega^2 = -1 - \omega,$$

recalling that $\omega^2 + \omega + 1 = 0$. Then $\varphi(\beta) = \beta$ gives

$$\begin{aligned} &a_1 + a_2\alpha + a_3\alpha^2 + a_4\omega + a_5\alpha\omega + a_6\alpha^2\omega \\ &= a_1 + a_2\alpha + a_3\alpha^2 + a_4(-1-\omega) + a_5\alpha(-1-\omega) + a_6\alpha^2(-1-\omega) \\ &= (a_1 - a_4) + (a_2 - a_5)\alpha + (a_3 - a_6)\alpha^2 - a_4\omega - a_5\alpha\omega - a_6\alpha^2\omega. \end{aligned}$$

Compare coefficients to see that $a_4 = a_5 = a_6 = 0$. Then

$$\beta = a_1 + a_2\alpha + a_3\alpha^2.$$

In $\mathrm{Gal}(K/\mathbb{Q})$ there is also a $\varphi$ such that $\varphi(\alpha) = \alpha\omega$. Then $\varphi(\beta) = \beta$ gives

$$\begin{aligned} a_1 + a_2\alpha + a_3\alpha^2 &= a_1 + a_2\alpha\omega + a_3(\alpha\omega)^2 \\ &= a_1 + a_2\alpha\omega + a_3\alpha^2(-1-\omega) \\ &= a_1 - a_3\alpha^2 + a_2\alpha\omega - a_3\alpha^2\omega. \end{aligned}$$

Compare coefficients again to see that $a_2 = a_3 = 0$. Thus $\beta = a_1 \in \mathbb{Q}$.

We have just shown that

$$\mathrm{Fix}(\mathrm{Gal}(K/\mathbb{Q})) = \mathbb{Q}.$$

## The Characterization of Galois Extensions

A fantastic but hard theorem is imminent...

**Proposition 0.107** For a finite degree extension $K$ of $F$, the following statements are equivalent:

1. $K$ is the splitting field of a separable polynomial in $F[X]$.
2. $|\mathrm{Gal}(K/F)| = [K : F]$.
3. $\mathrm{Fix}(\mathrm{Gal}(K/F)) = F$.
4. For every $\alpha$ in $K$, its minimal polynomial in $F[X]$ is separable and splits in $K[X]$.

**Proof.** (1) *implies* (2). We prove this by induction on the degree $[K : F]$. If $[K : F] = 1$, then undoubtedly $K = F$, which leads to

$$|\mathrm{Gal}(F/F)| = 1 = [F : F].$$

Now suppose $K$ is the splitting field of a separable polynomial $f$ in $F[X]$ and $[K : F] = n$. If all irreducible factors of $f$ in $F[X]$ were linear, then $f$ would already split in $F[X]$, and $K = F$. So we can take $g$ to be an irreducible factor of $f$ in $F[X]$ with $\deg g = k \geq 2$.

Pick a root $\alpha$ of $g$ in $K$ and put

$$L = F[\alpha].$$

Since $g$ is irreducible,

$$[L : F] = \deg g = k.$$

Since

$$n = [K : F] = [K : L][L : F] = [K : L]k,$$

we have $[K : L] = n/k < n$.

The field $K$ remains the splitting field of $f$ viewed as a polynomial in $L[X]$. Also $f$ remains

separable as a polynomial in $L[X]$. By the inductive hypothesis applied to the extension $K/L$,

$$|\mathrm{Gal}(K/L)| = [K : L].$$

Here $\mathrm{Gal}(K/L)$ is the group of automorphisms of $K$ that fix $L$. Clearly $\mathrm{Gal}(K/L)$ is a subgroup of $\mathrm{Gal}(K/F)$. Recall that the **index** of a subgroup $H$ of a group $G$ is the number of left cosets of $H$. Let $j$ be the index of $\mathrm{Gal}(K/L)$ in $\mathrm{Gal}(K/F)$. Lagrange's theorem tells us that

$$|\mathrm{Gal}(K/F)| = |\mathrm{Gal}(K/L)|j.$$

The tower theorem, along with the inductive hypothesis, tells us that

$$[K : F] = [K : L][L : F] = |\mathrm{Gal}(K/L)|[L : F].$$

To see that $[K : F] = |\mathrm{Gal}(K/F)|$, we need $j = [L : F]$. Remember that

$$[L : F] = [F[\alpha] : F] = \deg g = k.$$

So we need $j = k$. This is where the separability of $g$ comes in. Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be the distinct roots of $g$ inside $K$. There are $k$ of them. For each $\alpha_i$, the isomorphism extension theorem provides an automorphism $\varphi_i : K \to K$ such that

$$\varphi_i|_F = \mathrm{id} \qquad \text{and} \qquad \varphi_i(\alpha) = \alpha_i.$$

These $\varphi_i$ are in $\mathrm{Gal}(K/F)$. Since the $\alpha_i$ are distinct, we see that

$$\varphi_i(\alpha) \neq \varphi_\ell(\alpha)$$

when $i \neq \ell$. Then

$$\varphi_\ell^{-1}\varphi_i(\alpha) \neq \alpha.$$

So $\varphi_\ell^{-1}\varphi_i$ is an $F$-automorphism of $K$ that does not fix $F[\alpha] = L$. For $i \neq \ell$ we just saw that

$$\varphi_\ell^{-1}\varphi_i \notin \mathrm{Gal}(K/L).$$

This means that the cosets

$$\varphi_i\mathrm{Gal}(K/L) \qquad \text{and} \qquad \varphi_\ell\mathrm{Gal}(K/L)$$

are distinct. Consequently $j \geq k$. Now, if we had $j > k$, then we would get

$$|\mathrm{Gal}(K/F)| = |\mathrm{Gal}(K/L)|j = \frac{n}{k}j > n = [K : F].$$

But this contradicts Proposition 0.103, which told us that

$$|\mathrm{Gal}(K/F)| \leq [K : F].$$

So $j = k$.

(2) *implies* (3). Let

$$L = \mathrm{Fix}(\mathrm{Gal}(K/F)).$$

By the definition of $L$, an automorphism $\varphi : K \to K$ fixes $F$ if and only if it fixes $L$. So

$$\mathrm{Gal}(K/L) = \mathrm{Gal}(K/F).$$

Then

$$\begin{aligned}
[K : F] &= |\mathrm{Gal}(K/F)| && \text{by the assumption in (2)} \\
&= |\mathrm{Gal}(K/L)| \\
&\leq [K : L] && \text{by Proposition 0.103} \\
&\leq [K : F] && \text{since } F \subseteq L \subseteq K.
\end{aligned}$$

Hence $[K : F] = [K : L]$. The tower theorem forces $L = F$.

(3) *implies* (4). For $\alpha$ in $K$, we will present its minimal polynomial $g$ in $F[X]$ in split form and without repeated roots in $K[X]$.

The orbit of $\alpha$ under $\mathrm{Gal}(K/F)$ is the set

$$\{\varphi(\alpha) : \varphi \in \mathrm{Gal}(K/F)\}.$$

Every one of these $\varphi(\alpha)$ is a root of $g$. Let

$$\alpha = \varphi_1(\alpha), \qquad \varphi_2(\alpha), \ldots, \qquad \text{and} \qquad \varphi_n(\alpha)$$

be an enumeration of the orbit of $\alpha$ without repetition. Put

$$h = (X - \varphi_1(\alpha))(X - \varphi_2(\alpha)) \cdots (X - \varphi_n(\alpha)).$$

This polynomial is split in $K[X]$ and has no repeated roots. For each $\varphi$ in $\mathrm{Gal}(K/F)$, we calculate the transformed polynomial

$$\varphi(h) = (X - \varphi\varphi_1(\alpha))(X - \varphi\varphi_2(\alpha)) \cdots (X - \varphi\varphi_n(\alpha)),$$

and $\varphi$ permutes the orbit

$$\{\varphi_1(\alpha), \ldots, \varphi_n(\alpha)\}.$$

So $\varphi(h) = h$. Thus the coefficients of $h$, when we expand it out, are fixed by every $\varphi \in \mathrm{Gal}(K/F)$. The coefficients of $h$ are therefore in $\mathrm{Fix}(\mathrm{Gal}(K/F))$, which we assumed was $F$. Thus $h \in F[X]$. Clearly $h(\alpha) = h(\varphi_1(\alpha)) = 0$. So the minimal polynomial $g$ divides $h$ in $F[X]$. But also each $\varphi_j(\alpha)$ is a root of $g$. Thus all the distinct factors $(X - \varphi_j(\alpha))$ appear in the splitting of $g$ in $K[X]$. That is, $h \mid g$ in $K[X]$. It follows that $g = h$, so $g$ splits in $K[X]$ with no repeated roots.

(4) *implies* (1). At least this one is easy. Since $[K : F]$ is finite, we have

$$K = F[\alpha_1, \ldots, \alpha_n]$$

for some $\alpha_j$ in $K$ that are algebraic over $F$. Let $g_j$ be the minimal polynomial of $\alpha_j$ in $F[X]$. Each $g_j$ is separable and splits over $K$, by assumption (4). Let

$$f = g_1 g_2 \cdots g_n.$$

This polynomial is clearly separable. Clearly $f$ splits over $K$. Since $K$ is already generated by roots of $f$, it follows that $K$ is the splitting field of $f$. □

**Definition 0.108** Any finite extension $K$ of $F$ that satisfies one of the conditions in Proposition 0.107, and therefore all of them, is called a **Galois extension**.

For example, all splitting fields of all polynomials in $\mathbb{Q}[X]$ are Galois extensions. Also every finite field $F$ of characteristic $p$ is a Galois extension of $\mathbb{Z}_p$, because $F$ is the splitting field of the separable polynomial $X^{p^n} - X$. Do not forget that all irreducibles over $\mathbb{Z}_p$ are separable. In other words, $\mathbb{Z}_p$ is perfect.

**Proposition 0.109** If $K$ is a finite Galois extension of $F$ and $E$ is an intermediate field (that is, $F \subseteq E \subseteq K$), then the following hold:

1. $K$ remains a Galois extension of $E$.
2. $\mathrm{Gal}(K/E)$ is a subgroup of $\mathrm{Gal}(K/F)$.
3. $|\mathrm{Gal}(K/E)| = [K : E]$.
4. $\mathrm{Fix}(\mathrm{Gal}(K/E)) = E$.

**Proof.** Let $f$ be a separable polynomial in $F[X]$ for which $K$ is the splitting field. Since $f \in E[X]$ and splits in $K[X]$, if $\alpha_1, \ldots, \alpha_n$ are its roots in $K$, then

$$K = F[\alpha_1, \ldots, \alpha_n] \subseteq E[\alpha_1, \ldots, \alpha_n] \subseteq K.$$

Hence $K = E[\alpha_1, \ldots, \alpha_n]$, so $K$ remains the splitting field of $f$ over $E$. Also $f$ remains separable in $E[X]$. Therefore $K/E$ is Galois. Applying Proposition 0.107 to $K/E$, we obtain

$$|\mathrm{Gal}(K/E)| = [K : E] \qquad \text{and} \qquad \mathrm{Fix}(\mathrm{Gal}(K/E)) = E.$$

The subgroup statement is immediate from the definitions. □

We have just seen that separable polynomials make Galois extensions. Next, we will look at an entirely different and more abstract way to make a Galois extension. The approach is due to Emil Artin (1898–1962), who in the early twentieth century developed the approach to Galois theory that is used these days.

Another hard result is coming up.

**Proposition 0.110 (Artin's theorem)** Suppose $K$ is a field and $H$ is a finite group of automorphisms of $K$. If

$$F = \mathrm{Fix}(H),$$

then the following hold:

1. $[K : F] = |H|$, the order of $H$.
2. $K$ is a Galois extension of $F$.
3. $\mathrm{Gal}(K/F) = H$.

**Proof.** This takes some effort. 😞 Buckle up!

Let $n = |H|$. The hardest part is to show that $[K : F] \leq n$. Suppose not, meaning that we have elements $\beta_1, \ldots, \beta_{n+1}$ in $K$ that are linearly independent over $F$. The homogeneous system

$$\varphi(\beta_1)x_1 + \varphi(\beta_2)x_2 + \cdots + \varphi(\beta_{n+1})x_{n+1} = 0, \tag{0.5}$$

taken over all $\varphi$ in $H$, has $n$ equations and $n + 1$ unknowns. Thus there is a nonzero solution $(x_1, \ldots, x_{n+1}) \in K^{n+1}$. Let $V$ be the null space of the system in (0.5). We know $\dim V \geq 1$.

Notice that if $(x_1, \ldots, x_{n+1}) \in V$ and $\psi \in H$, then $(\psi(x_1), \ldots, \psi(x_{n+1})) \in V$. To see this, apply $\psi$ to each equation in (0.5) to get

$$\psi \circ \varphi(\beta_1)\psi(x_1) + \cdots + \psi \circ \varphi(\beta_{n+1})\psi(x_{n+1}) = \psi(0) = 0$$

for all $\varphi$ in $H$. But as $\varphi$ varies over all of $H$, so does $\psi \circ \varphi$ vary over all of $H$. Thus $(\psi(x_1), \ldots, \psi(x_{n+1}))$ solves the system whenever $(x_1, \ldots, x_{n+1})$ does.

Of all the nonzero solutions in $V$, pick one with as few nonzero entries as possible. For simplicity, suppose this solution has the form

$$(x_1, x_2, \ldots, x_r, 0, 0, \ldots, 0),$$

where $1 \leq r \leq n+1$ and each $x_j \neq 0$ for $1 \leq j \leq r$. Divide by $x_r$ to obtain a solution

$$(x_1, x_2, \ldots, x_{r-1}, 1, 0, \ldots, 0).$$

We know $r \geq 1$. But if $r = 1$, then the equation in (0.5) with $\varphi = \mathrm{id}$ would give $\beta_1 \cdot 1 = 0$, contrary to the independence of the $\beta_j$ over $F$. So in fact $r \geq 2$.

Furthermore, some of these $x_j$ are not in $F$. For if all $x_j \in F$, the equation in (0.5) with $\varphi = \mathrm{id}$ would give

$$\beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_{r-1} x_{r-1} + \beta_r = 0,$$

contrary to the independence of the $\beta_j$ over $F$.

To keep notation simple, say $x_1 \notin F = \mathrm{Fix}(H)$. This means that there is a $\psi \in H$ such that $\psi(x_1) \neq x_1$. As we saw,

$$(\psi(x_1), \psi(x_2), \ldots, \psi(x_{r-1}), 1, 0, \ldots, 0) \in V.$$

Subtract $(x_1, x_2, \ldots, x_{r-1}, 1, 0, \ldots, 0)$, which is also in $V$, to get

$$(\psi(x_1) - x_1, \ldots, \psi(x_{r-1}) - x_{r-1}, 0, 0, \ldots, 0) \in V.$$

The first entry is nonzero, and the entry corresponding to the previous 1 is $1 - 1 = 0$. We have created a nontrivial solution of the system with fewer than the minimal number of nonzero entries, which is preposterous! Since this is impossible, we get that

$$[K : F] \leq n = |H|.$$

Clearly $H$ is a subgroup of $\mathrm{Gal}(K/F)$. Thus

$$\begin{aligned} n = |H| &\leq |\mathrm{Gal}(K/F)| \\ &\leq [K:F] && \text{by Proposition 0.103} \\ &\leq n && \text{by the part just completed.} \end{aligned}$$

Now we see that $|H| = |\mathrm{Gal}(K/F)|$, and since $H$ is a subgroup of $\mathrm{Gal}(K/F)$ we get

$$H = \mathrm{Gal}(K/F).$$

Also $|\mathrm{Gal}(K/F)| = [K:F]$. According to Proposition 0.107, $K$ is a Galois extension of $F$. □

Now the other half of the Galois correspondence pops out.

**Proposition 0.111** If $K$ is a Galois extension of $F$ and $H$ is any subgroup of $\mathrm{Gal}(K/F)$, then

$$\mathrm{Gal}(K/\mathrm{Fix}(H)) = H.$$

**Proof.** This follows from Artin's theorem. Let

$$E = \mathrm{Fix}(H).$$

By Proposition 0.110, applied to the group $H$ of automorphisms of $K$,

$$[K:E] = |H| \qquad \text{and} \qquad \mathrm{Gal}(K/E) = H.$$

The conclusion follows. □

## The Fundamental Theorem of Galois Theory

We have a finite degree Galois extension $K$ of $F$. Let $\mathscr{F}$ be the family of all subfields of $K$ that contain $F$, the intermediate fields. Let $\mathscr{H}$ be the family of all subgroups of $\mathrm{Gal}(K/F)$.

We have two mappings:

$$\begin{aligned} \mathrm{Gal}(K/-) : \mathscr{F} &\longrightarrow \mathscr{H} \\ E &\longmapsto \mathrm{Gal}(K/E), \end{aligned}$$

and

$$\begin{aligned} \text{Fix} : \mathscr{H} &\longrightarrow \mathscr{F} \\ H &\longmapsto \text{Fix}(H). \end{aligned}$$

Proposition 0.109 told us

$$\text{Fix}(\text{Gal}(K/E)) = E$$

for all $E \in \mathscr{F}$. Proposition 0.111 told us

$$\text{Gal}(K/\text{Fix}(H)) = H$$

for all $H \in \mathscr{H}$.

**Proposition 0.112 (Fundamental theorem of Galois theory)** The above mappings are one-to-one and onto and are the inverses of one another.

This result is very important, which explains the name. It is the cornerstone of Galois theory. It is the key to unlocking the mysteries of field extensions and their symmetries.

The one-to-one correspondence between the family $\mathscr{H}$ of subgroups of $\text{Gal}(K/F)$ and the family $\mathscr{F}$ of intermediate fields comes with a number of features to keep in mind:

1. If $H, N \in \mathscr{H}$ and $H \subseteq N$, then $\text{Fix}(H) \supseteq \text{Fix}(N)$.
2. If $E, L \in \mathscr{F}$ and $E \subseteq L$, then $\text{Gal}(K/E) \supseteq \text{Gal}(K/L)$.

So the Galois correspondence reverses inclusions.

3. If $E \in \mathscr{F}$, then $|\text{Gal}(K/E)| = [K : E]$. This is in Proposition 0.109.
4. If $H \in \mathscr{H}$, then $|H| = [K : \text{Fix}(H)]$. This is in Proposition 0.110.

## The Normality Connection

If $K$ is a Galois extension of $F$ and $\varphi \in \text{Gal}(K/F)$ and $E \in \mathscr{F}$, then obviously $\varphi(E) \in \mathscr{F}$ too.

What is the connection between $\text{Gal}(K/E)$ and $\text{Gal}(K/\varphi(E))$? Well, for each $\sigma \in \text{Gal}(K/F)$ we

see that $\sigma \in \mathrm{Gal}(K/\varphi(E))$ if and only if $\sigma$ fixes $\varphi(E)$, if and only if for all $\alpha \in E$,

$$\sigma\varphi(\alpha) = \varphi(\alpha),$$

if and only if for all $\alpha \in E$,

$$\varphi^{-1}\sigma\varphi(\alpha) = \alpha,$$

if and only if $\varphi^{-1}\sigma\varphi$ fixes $E$, if and only if

$$\varphi^{-1}\sigma\varphi \in \mathrm{Gal}(K/E).$$

We have just discovered that

$$\varphi^{-1}\mathrm{Gal}(K/\varphi(E))\varphi = \mathrm{Gal}(K/E).$$

Alternatively,

$$\mathrm{Gal}(K/\varphi(E)) = \varphi\mathrm{Gal}(K/E)\varphi^{-1}. \tag{0.6}$$

This leads to another interesting connection in the Galois correspondence:

**Proposition 0.113** If $K$ is a Galois extension of $F$ and $E$ is an intermediate field, the subgroup $\mathrm{Gal}(K/E)$ is normal in $\mathrm{Gal}(K/F)$ if and only if

$$\varphi(E) = E$$

for all $\varphi \in \mathrm{Gal}(K/F)$.

**Proof.** By (0.6), for each $\varphi \in \mathrm{Gal}(K/F)$ we have

$$\varphi\mathrm{Gal}(K/E)\varphi^{-1} = \mathrm{Gal}(K/\varphi(E)).$$

Therefore $\mathrm{Gal}(K/E)$ is normal in $\mathrm{Gal}(K/F)$ if and only if

$$\mathrm{Gal}(K/\varphi(E)) = \mathrm{Gal}(K/E)$$

for all $\varphi \in \mathrm{Gal}(K/F)$, which, by the Galois correspondence, is equivalent to

$$\varphi(E) = E$$

for all $\varphi \in \mathrm{Gal}(K/F)$. □

Now suppose $E$ is an intermediate field between $F$ and its Galois extension $K$, and that

$$\varphi(E) = E$$

for all $\varphi \in \mathrm{Gal}(K/F)$. In that case we get a group homomorphism

$$\begin{aligned} \Gamma : \mathrm{Gal}(K/F) &\longrightarrow \mathrm{Gal}(E/F) \\ \varphi &\longmapsto \varphi|_E, \end{aligned}$$

given by the restriction map:

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & K \\ | & & | \\ E & \xrightarrow{\varphi|_E} & E \\ | & & | \\ F & \xrightarrow{\mathrm{id}} & F \end{array}$$

This $\Gamma$ is onto. Because $K$ is Galois over $F$, choose $f \in F[X]$ for which $K$ is the splitting field. It remains the splitting field of $f$ over $E$: adjoining the roots of $f$ to $E \subseteq K$ still gives all of $K$. If $\sigma \in \mathrm{Gal}(E/F)$, then the $\sigma$-transfer of $f$ is again $f$, since every coefficient of $f$ lies in $F$ and $\sigma$ fixes $F$. The isomorphism extension theorem therefore extends $\sigma : E \to E$ to an $F$-automorphism $\varphi : K \to K$. Thus every element of $\mathrm{Gal}(E/F)$ lies in the image of $\Gamma$.

What is $\ker \Gamma$? We have $\varphi \in \ker \Gamma$ if and only if $\varphi|_E = \mathrm{id}$, if and only if $\varphi$ fixes $E$, if and only if $\varphi \in \mathrm{Gal}(K/E)$. So

$$\ker \Gamma = \mathrm{Gal}(K/E).$$

In summary:

**Proposition 0.114** If $E$ is an intermediate field between $F$ and its Galois extension $K$, and $\varphi(E) = E$ for all $\varphi \in \mathrm{Gal}(K/F)$, then the restriction map

$$\Gamma : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)$$

is a surjective group homomorphism whose kernel is $\mathrm{Gal}(K/E)$. By the first isomorphism theorem for groups,

$$\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E).$$

We now explore what it means to say that $\varphi(E) = E$ for all $\varphi \in \mathrm{Gal}(K/F)$.

If $E$ is itself a Galois extension of $F$, then $E$ is a splitting field of some polynomial in $F[X]$. Thus $E$ satisfies the normality theorem. In particular, $\varphi(E) = E$ for all $F$-automorphisms $\varphi : K \to K$, that is, for all $\varphi \in \mathrm{Gal}(K/F)$.

Conversely, suppose $\varphi(E) = E$ for all $\varphi \in \mathrm{Gal}(K/F)$. We prove that $E$ is a Galois extension of $F$. By Proposition 0.114, we have

$$|\mathrm{Gal}(E/F)| = |\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)|.$$

Then

$$\begin{aligned} |\mathrm{Gal}(E/F)| &= \frac{|\mathrm{Gal}(K/F)|}{|\mathrm{Gal}(K/E)|} && \text{by Lagrange's theorem} \\ &= \frac{[K:F]}{[K:E]} && \text{by the nature of the Galois correspondence} \\ &= [E:F] && \text{by the tower theorem.} \end{aligned}$$

We have just obtained Proposition 0.107(2), which characterizes Galois extensions. We can summarize the result as follows.

**Proposition 0.115** For an intermediate field $E$ between $F$ and its Galois extension $K$, the following are equivalent:

1. $\mathrm{Gal}(K/E)$ is a normal subgroup of $\mathrm{Gal}(K/F)$.
2. $\varphi(E) = E$ for all $\varphi \in \mathrm{Gal}(K/F)$.
3. $E$ is itself a Galois extension of $F$.

When this occurs,

$$\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E).$$

**Remark 0.116** If we are in characteristic 0, separability is no longer an issue, and Galois extensions are those that are splitting fields.

So in characteristic 0, Galois extensions coincide with those that satisfy the normality theorem. These are commonly known as **normal extensions**. In characteristic 0, where Galois

theory was born, normal and Galois extensions are one and the same. We have just learned that if $E$ is an intermediate field between $F$ and its normal extension $K$, such $E$ is itself a normal extension of $F$ if and only if $\mathrm{Gal}(K/E)$ is a normal subgroup of $\mathrm{Gal}(K/F)$.

This leads to a chicken-and-egg type question. What came first: normal extensions or normal subgroups? Since the study of roots of polynomials led to the concept of a group, it is safe to say that normal extensions gave birth to the term normal subgroup. But for what it is worth, Galois himself never used the word "normal". Later scholars, perhaps in France or Germany, may be guilty of thrusting this overused word upon us.

## Practice With the Isomorphism Extension Theorem

The isomorphism extension theorem can be complicated to apply. Here is what it says:

Let $\varphi : F \to E$ be a field isomorphism, let $K$ be the splitting field of some $f \in F[X]$, let $L$ be the splitting field of $\varphi(f) \in E[X]$, let $\alpha \in K$ have minimal polynomial $g \in F[X]$, and let $\beta \in L$ have minimal polynomial $\varphi(g) \in E[X]$. Then there exists an isomorphism $\psi : K \to L$ such that $\psi|_F = \varphi$ and $\psi(\alpha) = \beta$.

$$\begin{array}{ccc} \alpha \in K & \xrightarrow{\psi} & L \ni \beta \\ \uparrow & & \uparrow \\ F & \xrightarrow{\varphi} & E \end{array}$$

Here, $K$ is the splitting field of $f$, $L$ is the splitting field of $\varphi(f)$, and the minimal polynomial of $\beta$ is $\varphi(g)$, where $g$ is the minimal polynomial of $\alpha$.

We now use this result to obtain $\mathbb{Q}$-automorphisms for the splitting field $K$ of $x^3 - 2$.

We have $K = \mathbb{Q}[\alpha, \omega]$, where $\alpha = \sqrt[3]{2}$ and $\omega = e^{(2\pi i)/3}$. We want to prove that there exists $\psi \in \mathrm{Gal}(K/\mathbb{Q})$ such that

$$\psi(\alpha) = \alpha\omega \qquad \text{and} \qquad \psi(\omega) = \omega^2.$$

Since $\alpha$ and $\alpha\omega$ are roots of the same irreducible polynomial $x^3 - 2$ in $\mathbb{Q}[x]$, we know there is an isomorphism

$$\varphi : \mathbb{Q}[\alpha] \to \mathbb{Q}[\alpha\omega]$$

such that $\varphi|_{\mathbb{Q}}$ is the identity map on $\mathbb{Q}$ and $\varphi(\alpha) = \alpha\omega$. Applying the isomorphism extension

theorem, take $F = \mathbb{Q}[\alpha]$ and $E = \mathbb{Q}[\alpha\omega]$. Then $K$ is the splitting field of $f = x^2 + x + 1$ over $F = \mathbb{Q}[\alpha]$.

Note that $\varphi(f) = f$. Therefore, the splitting field of $\varphi(f)$ over $E = \mathbb{Q}[\alpha\omega]$ is also $K$, and

$$L = \mathbb{Q}[\alpha\omega][\omega] = \mathbb{Q}[\alpha\omega, \omega] = \mathbb{Q}[\alpha, \omega] = K.$$

The polynomial $g \in F[X] = \mathbb{Q}[\alpha][X]$ to use is $x^2 + x + 1$ (the same as $f$ in this case). Notice that $\varphi(g) = g$ in $E[X] = \mathbb{Q}[\alpha\omega][X]$. For the theorem's temporary elements, take $a = \omega$, which is a root of $g$ in $K$, and take $b = \omega^2$, which is a root of $g$ in $L = K$. The isomorphism extension theorem applies to give us an automorphism

$$\psi : K \to K = L$$

such that

$$\psi|_{\mathbb{Q}[\alpha]} = \varphi \qquad \text{and} \qquad \psi(\omega) = \omega^2.$$

Hence $\psi(\alpha) = \varphi(\alpha) = \alpha\omega$, and $\psi(\omega) = \omega^2$. This $\psi \in \mathrm{Gal}(K/\mathbb{Q})$ is exactly the automorphism we wanted.

A big theorem coming later on will tell us that $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 6$ for this example. Once we know that, the above fussing with the isomorphism extension theorem will be unnecessary. After all, we know that every $\mathbb{Q}$-automorphism of $\mathbb{Q}[\alpha, \omega]$ *must* act in one of the following six ways on the generators $\alpha$ and $\omega$:

1. $\alpha \mapsto \alpha, \omega \mapsto \omega$
2. $\alpha \mapsto \alpha\omega, \omega \mapsto \omega$
3. $\alpha \mapsto \alpha\omega^2, \omega \mapsto \omega$
4. $\alpha \mapsto \alpha, \omega \mapsto \omega^2$
5. $\alpha \mapsto \alpha\omega, \omega \mapsto \omega^2$
6. $\alpha \mapsto \alpha\omega^2, \omega \mapsto \omega^2$

Once we learn that $\mathrm{Gal}(\mathbb{Q}[\alpha, \omega]/\mathbb{Q})$ must contain six automorphisms, it will be obvious that each of the six possibilities above is realized as a $\mathbb{Q}$-automorphism of $\mathbb{Q}[\alpha, \omega]$.

Would it not be nice to have an isomorphism extension theorem that simultaneously lets us lift the identity map on $\mathbb{Q}$ to an automorphism of $\mathbb{Q}[\alpha, \omega]$ such that $\alpha \mapsto \alpha\omega$ and $\omega \mapsto \omega^2$? That

would be so very nice, but alas, no such theorem is available.

# 6. Putting the Galois Correspondence to Work

## Galois Correspondence in the Setting of Finite Fields

Suppose $K$ is a finite field of characteristic $p$ and that $[K : \mathbb{Z}_p] = n$. Thus the size of $K$ is $p^n$. Also $K$ is the splitting field of $f = X^{p^n} - X$. In fact $K$ is the set of all roots of $f$. Furthermore, $f$ is separable, since $f' = -1$ which is coprime with $f$. This ensures that neither $f$ nor any of its irreducible factors in $\mathbb{Z}_p[X]$ have repeated roots in $K$.

Thus $K$ is a Galois extension of $\mathbb{Z}_p$. Consequently $n = [K : \mathbb{Z}_p] = |\mathrm{Gal}(K/\mathbb{Z}_p)|$. We could also show this by noting that $\mathrm{Gal}(K/\mathbb{Z}_p)$ is cyclic of order $n$ with the Frobenius map $\sigma : K \to K$ as its generator, where $\sigma(\alpha) = \alpha^p$.

Our prior knowledge of cyclic groups tells us that for every divisor $d$ of $n$ the subgroup $H = \langle \sigma^{n/d} \rangle$ generated by the automorphism $\sigma^{n/d}$ has order $d$, and *all* subgroups of $\mathrm{Gal}(K/\mathbb{Z}_p)$ are accounted for by the above process. So the **subgroup lattice** of $\mathrm{Gal}(K/\mathbb{Z}_p)$ matches up exactly with the lattice of divisors of $n$.

The divisor lattice for $n = 40$ is shown in Figure 11.

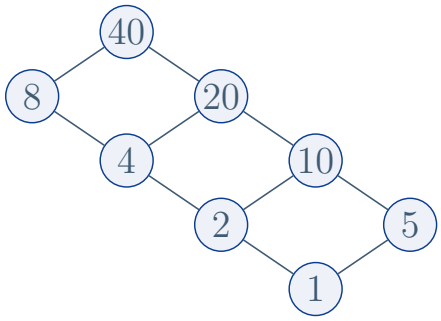



FIGURE 11

Each divisor $d$ of 40 represents a subgroup of $\mathrm{Gal}(K/\mathbb{Z}_p)$ of order $d$.

The Galois correspondence (that is, the fundamental theorem of Galois theory) tells us that

$\mathrm{Gal}(K/-)$ and Fix implement inclusion-reversing bijections between the family of subfields of $K$ (which all contain $\mathbb{Z}_p$ automatically) and the family of subgroups of $\mathrm{Gal}(K/\mathbb{Z}_p)$. The subfields of $K$ correspond exactly to the divisors of $n = [K : \mathbb{Z}_p]$ (exercise!). For every divisor $d$ of $n$, there is precisely one subfield $E$ of order $p^d$. This confirms the Galois correspondence.

If $H$ is a subgroup of $\mathrm{Gal}(K/\mathbb{Z}_p)$ and $|H| = d$, where $d \mid n$, then $\mathrm{Fix}(H)$ is a subfield of $K$ such that $[K : \mathrm{Fix}(H)] = d$. Equivalently,

$$[\mathrm{Fix}(H) : \mathbb{Z}_p] = \frac{n}{d},$$

so the size of $\mathrm{Fix}(H)$ is $p^{n/d}$, that is, $\mathrm{Fix}(H) = \mathbb{F}_{p^{n/d}}$.

For $n = 40$ and $d \mid 40$, let $H_d$ be the unique subgroup of $\mathrm{Gal}(K/\mathbb{Z}_p)$ of order $d$. Its subgroup lattice is shown in Figure 12.

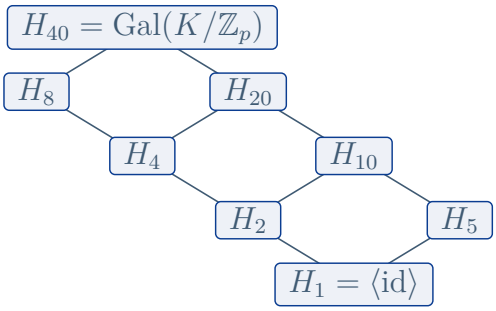



FIGURE 12

The corresponding subfield lattice appears in Figure 13.

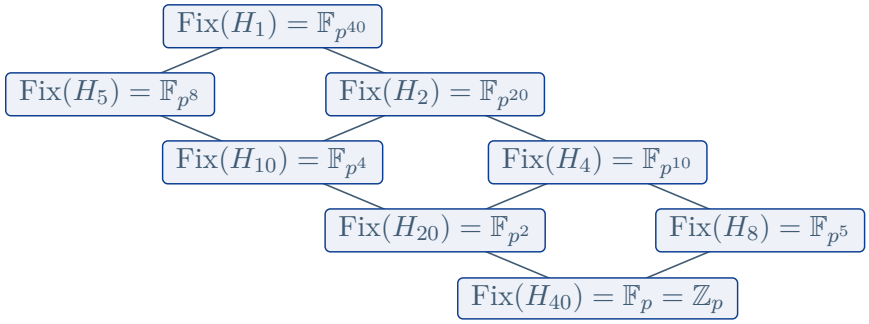



FIGURE 13

## The Fundamental Theorem of Algebra

**Proposition 0.117 (Fundamental theorem of algebra)** $\mathbb{C}$ is algebraically closed.

**Proof.** Suppose not, for a contradiction. Thus there is a proper algebraic extension $L$ of $\mathbb{C}$. Since $\mathbb{C}$ is algebraic over $\mathbb{R}$, $L$ is also algebraic over $\mathbb{R}$, by Proposition 0.49. Pick $\theta \in L \setminus \mathbb{C}$ and let $g \in \mathbb{R}[X]$ be its minimal polynomial over $\mathbb{R}$. This $g$ does not split in $\mathbb{C}[X]$: if

$$g = (X - \theta_1) \cdots (X - \theta_n)$$

with every $\theta_j \in \mathbb{C}$, then the root $\theta \in L$ would equal one of the $\theta_j$, contrary to our choice of $\theta$.

So let $K$ be the splitting field of $g$ as a polynomial in $\mathbb{C}[X]$ (even though $g \in \mathbb{R}[X]$). We have $\mathbb{R} \subsetneq \mathbb{C} \subsetneq K$. Observe that $K$ is also the splitting field of $(X^2 + 1)g$ as a polynomial in $\mathbb{R}[X]$. To see this, let $\theta_1, \ldots, \theta_n$ be the roots of $g$ in $K$. Then $\pm i, \theta_1, \ldots, \theta_n$ are the roots of $(X^2 + 1)g$ in $K$, and

$$K = \mathbb{C}[\theta_1, \ldots, \theta_n] = \mathbb{R}[\pm i, \theta_1, \ldots, \theta_n].$$

Thus $K$ is a Galois extension of $\mathbb{R}$. This means that

$$|\mathrm{Gal}(K/\mathbb{R})| = [K : \mathbb{R}] = [K : \mathbb{C}][\mathbb{C} : \mathbb{R}] = [K : \mathbb{C}] \cdot 2.$$

(Note: The tower of extensions is $K \supseteq \mathbb{C} \supseteq \mathbb{R}$ with $[K : \mathbb{C}] \geq 2$ and $[\mathbb{C} : \mathbb{R}] = 2$.) Thus 2 divides the order of $\mathrm{Gal}(K/\mathbb{R})$. Write $|\mathrm{Gal}(K/\mathbb{R})| = 2^j m$ where $m$ is odd and $j \geq 1$. By Sylow's theorem, $\mathrm{Gal}(K/\mathbb{R})$ has a subgroup $H$ of order $2^j$. Put $E = \mathrm{Fix}(H)$. By the nature of the Galois correspondence, $[K : E] = 2^j$ and $[K : \mathbb{R}] = 2^j m$. The tower theorem gives $[E : \mathbb{R}] = m$, an odd integer. If $\alpha \in E$, the degree $[\mathbb{R}(\alpha) : \mathbb{R}]$ divides $m$, and so $[\mathbb{R}(\alpha) : \mathbb{R}]$ is also odd. The minimal polynomial $h$ of $\alpha$ in $\mathbb{R}[X]$ has odd degree. From basic calculus, $h$ has a root in $\mathbb{R}$. Since $h$ is irreducible in $\mathbb{R}[X]$, it follows that $h$ is linear, and thus $\alpha \in \mathbb{R}$.

We have just shown that $E = \mathbb{R}$, and so $m = 1$. Thus $|\mathrm{Gal}(K/\mathbb{R})| = 2^j$. Since $\mathbb{C} \subsetneq K$, we can also see that $j \geq 2$. Since $\mathrm{Gal}(K/\mathbb{C})$ is a subgroup of $\mathrm{Gal}(K/\mathbb{R})$, Lagrange's theorem gives $|\mathrm{Gal}(K/\mathbb{C})| = 2^r$ for some $r$. In fact, since $K$ is a Galois extension of $\mathbb{C}$ we get $|\mathrm{Gal}(K/\mathbb{C})| = [K : \mathbb{C}] \geq 2$. So $r \geq 1$.

Every finite 2-group has a subgroup of each possible order dividing its own, so $\mathrm{Gal}(K/\mathbb{C})$ has a subgroup $H$ of order $2^{r-1}$. Then $[K : \mathrm{Fix}(H)] = 2^{r-1}$, by Artin's theorem. The tower theorem gives $[\mathrm{Fix}(H) : \mathbb{C}] = 2$. Now pick $\beta \in \mathrm{Fix}(H) \setminus \mathbb{C}$. The minimal polynomial of such $\beta$ is quadratic and irreducible in $\mathbb{C}[X]$. This is a contradiction because every quadratic $x^2 + bx + c$ in $\mathbb{C}[X]$ splits

as

$$\left(x - \underbrace{\frac{-b+\sqrt{b^2-4c}}{2}}_{\in\mathbb{C}}\right)\left(x - \underbrace{\frac{-b-\sqrt{b^2-4c}}{2}}_{\in\mathbb{C}}\right). \qquad \square$$

## The Primitive Element Theorem

This lovely result tells us that if $\mathrm{char}(F) = 0$ (for example, when $F = \mathbb{Q}$), then every finite degree extension $E$ of $F$ takes the form $E = F[\gamma]$ for a single $\gamma$ in $E$. Such an element $\gamma$ is called a **primitive element**, and such an extension is called a **simple extension**.

To get there, it helps to have the concept of the **normal closure**. Suppose $E$ is a finite degree extension of $F$. Say $E = F[\alpha_1, \ldots, \alpha_n]$ for some generators $\alpha_j$. Let $g_j$ be the minimal polynomial of $\alpha_j$ in $F[X]$, let $g = g_1 \cdots g_n \in F[X]$, and let $K$ be a splitting field of $g$ as a polynomial in $E[X]$. This latter item ensures that $F \subseteq E \subseteq K$. But $K$ is also a splitting field for $g$ as a polynomial in $F[X]$. To see this, let $\Delta$ be the set of roots of $g$ inside $K$ other than the $\alpha_1, \ldots, \alpha_n$. Then:

$$\begin{aligned} K &= E[\alpha_1, \ldots, \alpha_n, \Delta] && \text{by the way } K \text{ is defined} \\ &= F[\alpha_1, \ldots, \alpha_n][\alpha_1, \ldots, \alpha_n, \Delta] && \text{by what } E \text{ is} \\ &= F[\alpha_1, \ldots, \alpha_n, \Delta] && \text{by throwing away redundant } \alpha_j. \end{aligned}$$

We have built a splitting field $K$ of a special polynomial $g$ in $F[X]$ with the property that $F \subseteq E \subseteq K$.

Suppose now that $L$ is another splitting field of some other $f$ in $F[X]$ and such that $F \subseteq E \subseteq L$. By the normality theorem (Proposition 0.70), the minimal polynomial in $F[X]$ of every $\alpha$ in $L$ splits in $L[X]$. In particular, the minimal polynomials $g_j$ of the $\alpha_j$ split in $L[X]$. Thus $g$ splits in $L[X]$. So inside $L$, there exists a splitting field, say $M$, for $g$. But $\alpha_1, \ldots, \alpha_n$ are roots of $g$ inside $L$ because $E = F[\alpha_1, \ldots, \alpha_n] \subseteq L$. These roots are therefore inside $M$ over which $g$ still splits. So we get

$$F \subseteq E \subseteq M \subseteq L.$$

The relevant fields and inclusions are collected in Figure 14.

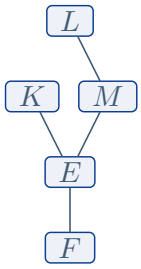



FIGURE 14

where $L$ is the splitting field of $f$ over $F$, $M$ is a splitting field of $g$ over $F$, and $K$ is the original splitting field of $g$ over $E$. Now $M$ remains a splitting field for $g$ over $E$, and $K$ was defined as a splitting field for $g$ over $E$. By the isomorphism extension theorem (Proposition 0.67), there is an $E$-isomorphism $\varphi : K \to M$.

Thus our $K$ is a splitting field for a polynomial in $F[X]$ such that $F \subseteq E \subseteq K$, and such that $K$ embeds by an $E$-map into any other splitting field $L$ over $F$ that happens to contain $E$. This special $K$ is called the **normal closure** of the extension $E$ over $F$.

The above discussion shows that any two normal closures for $E$ over $F$ are $E$-isomorphic. It also shows that if $L$ is a splitting field of some $f$ in $F[X]$ and $F \subseteq E \subseteq L \subseteq K$, then $L = K$: the inclusion gives $[L : E] \leq [K : E]$, while an $E$-embedding of $K$ into $L$ gives the reverse inequality. Thus normal closures are **minimal splitting fields** over $F$ that contain $E$.

We observe that if the minimal polynomial in $F[X]$ of every $\alpha$ in $E$ is separable (for example, when $\text{char}(F) = 0$), then the normal closure $K$ of $E$ over $F$ is a Galois extension of $F$. This is because the minimal polynomials $g_j$ in $F[X]$ of the generators $\alpha_j$ of $E$ over $F$ are separable, and thereby $g = g_1 \cdots g_n$ is separable. So $K$ being the splitting field of this $g$ is a Galois extension of $F$.

The benefits of the Galois correspondence apply to these normal closures!

**Proposition 0.118** If $E$ is an extension of finite degree over $F$ and the minimal polynomial in $F[X]$ of every $\alpha$ in $E$ is separable (for example, when $\text{char}(F) = 0$), then the number of intermediate fields between $F$ and $E$ is finite.

**Proof.** The normal closure $K$ of $E$ over $F$ is a Galois extension of $F$ and $F \subseteq E \subseteq K$. By the Galois correspondence, the number of fields between $F$ and $K$ equals the number of subgroups of $\text{Gal}(K/F)$. That number is finite since $|\text{Gal}(K/F)| = [K : F] < \infty$. The intermediate fields between $F$ and $E$ form a subcollection, so there are only finitely many of them as well. □

Here comes a fairly interesting result.

**Theorem 0.119 (Primitive element theorem)** A finite degree extension $E$ of $F$ is of the form $E = F[\gamma]$ for a single $\gamma$ in $E$ if and only if there are only finitely many fields between $F$ and $E$.

In particular, if $F$ has characteristic 0, then every finite degree extension $E$ of $F$ takes the form $E = F[\gamma]$ for a single $\gamma$ in $E$.

**Proof.** First suppose $E = F[\gamma]$, and let $m_F \in F[X]$ be the minimal polynomial of $\gamma$ over $F$. For every intermediate field $L$, let $m_L \in L[X]$ be the minimal polynomial of $\gamma$ over $L$. Since $E = L[\gamma]$, we have

$$[E : L] = \deg m_L,$$

and $m_L$ is a monic divisor of $m_F$ in $E[X]$. A fixed polynomial has only finitely many monic divisors in the polynomial ring over a field, so only finitely many polynomials $m_L$ can occur. Moreover, $m_L$ determines $L$. Indeed, let $L_0$ be the field generated over $F$ by the coefficients of $m_L$. Then $L_0 \subseteq L$, while $m_L(\gamma) = 0$ gives

$$[E : L_0] \leq \deg m_L = [E : L].$$

The tower theorem gives $[E : L_0] = [E : L][L : L_0]$, so $[L : L_0] = 1$ and $L = L_0$. Hence there are only finitely many intermediate fields.

For the converse, if $F$ is a finite field, then its extension $E$ of finite degree is also a finite field. In this case, any generator $\gamma$ of the cyclic group $E^*$ gives $E = F[\gamma]$. So now assume that $F$ is infinite. Suppose only a finite number of fields sit between $F$ and $E$. Since $E$ has finite degree over $F$, the field $E$ is generated by finitely many elements of $E$. For now, write $E = F[\alpha, \beta]$ using only two elements of $E$. As $\theta$ runs through the infinite field $F$, the subfields $F[\alpha + \theta\beta]$ must repeat. Thus $F[\alpha + \theta_1\beta] = F[\alpha + \theta_2\beta]$ for some $\theta_1, \theta_2 \in F$ with $\theta_1 \neq \theta_2$.

Hence $\alpha + \theta_1\beta \in F[\alpha + \theta_2\beta]$. Since $\alpha + \theta_2\beta \in F[\alpha + \theta_2\beta]$, their difference $(\theta_1 - \theta_2)\beta \in F[\alpha + \theta_2\beta]$. Since $\theta_1 - \theta_2 \in F$ and $\theta_1 - \theta_2 \neq 0$, we see that $\beta \in F[\alpha + \theta_2\beta]$, and then $\alpha = (\alpha + \theta_2\beta) - \theta_2\beta \in F[\alpha + \theta_2\beta]$. Thus $E = F[\alpha, \beta] = F[\alpha + \theta_2\beta]$. The element $\gamma$ we want is $\alpha + \theta_2\beta$. Now if $E = F[\alpha_1, \alpha_2, \alpha_3]$ with 3 generators, use the part just done to write

$$\begin{aligned} E &= F[\alpha_1, \alpha_2][\alpha_3] \\ &= F[\gamma_1][\alpha_3] && \text{for some } \gamma_1 \text{ in } E \\ &= F[\gamma_1, \alpha_3] \end{aligned}$$

$$= F[\gamma] \qquad \text{for some } \gamma \text{ in } E.$$

Likewise, we can reduce the number of generators to one when $E$ has $n$ generators. The particular statement about characteristic 0 is quite valuable. It follows from Proposition 0.118 and the proof we just completed. □

In some books we may find that the primitive element theorem is covered before the Galois correspondence, and then used to help prove it. This approach would bypass the need for Artin's theorem (Proposition 0.110). But why would we want to bypass a lovely result like Artin's theorem?

## The Symmetric Function Theorem

Let $K = L(t_1, t_2, \ldots, t_n)$ be the field of rational functions in the indeterminates $t_1, \ldots, t_n$, with coefficients in some field $L$. (The field $L$ will not matter in this discussion.) The group $S_n$ of permutations on $n$ letters becomes a group of automorphisms of $K$ as follows:

If $\sigma \in S_n$ and $f = f(t_1, t_2, \ldots, t_n) \in K$, let $\sigma f = f(t_{\sigma(1)}, t_{\sigma(2)}, \ldots, t_{\sigma(n)})$. In other words, $\sigma$ permutes the variables in $f$ in accordance with how $\sigma$ permutes the letters $1, 2, \ldots, n$.

**Example 0.120** If $n = 4$ and $\sigma$ is the cycle $(1\,2\,4)$, then $\sigma : f(t_1, t_2, t_3, t_4) \mapsto f(t_2, t_4, t_3, t_1)$. For instance,

$$\frac{t_1^2 t_2 + t_3 t_4^3 - t_1 t_2 t_3}{t_1 t_4 + 5 t_1 t_2 t_3 t_4} \mapsto \frac{t_2^2 t_4 + t_3 t_1^3 - t_2 t_4 t_3}{t_2 t_1 + 5 t_2 t_4 t_3 t_1}.$$

It should be clear that $S_n$ is a group of automorphisms of $K$. We also know that $S_n$ is a finite group of order $n!$. Let $F = \mathrm{Fix}(S_n)$. This is a subfield of $K$, and Artin's theorem tells us that $K$ is a Galois extension of $F$. A rational function $f(t_1, t_2, \ldots, t_n) \in F$ if and only if $f(t_{\sigma(1)}, t_{\sigma(2)}, \ldots, t_{\sigma(n)}) = f(t_1, \ldots, t_n)$ for all permutations of $1, 2, \ldots, n$. Such functions are called **symmetric**. They constitute the fixed field $F$.

Here are some important examples of symmetric functions:

- $s_0 = 1$, the constant function.
- $s_1 = t_1 + t_2 + \cdots + t_n$, that is, the sum of all variables.
- $s_2 = \sum_{1 \le i < j \le n} t_i t_j$, that is, the sum of all product pairs.

- $s_3 = \sum_{1\le i<j<k\le n} t_i t_j t_k$, that is, the sum of all triple products.
- ...
- $s_{n-1}$ = the sum of all products of $n-1$ distinct $t_j = \dfrac{t_1 t_2 \dots t_n}{t_1} + \dfrac{t_1 t_2 \dots t_n}{t_2} + \cdots + \dfrac{t_1 t_2 \dots t_n}{t_n}$.
- $s_n$ = the product of all $t_j = t_1 t_2 \dots t_n$.

$$
\begin{aligned}
s_0 &= 1 \\
s_1 &= t_1 + t_2 + \cdots + t_n = \sum_{j=1}^{n} t_j \\
s_2 &= \sum_{1\le i<j\le n} t_i t_j = \text{the sum of all product pairs} \\
s_3 &= \sum_{1\le i<j<k\le n} t_i t_j t_k = \text{the sum of all triple products} \\
&\vdots \\
s_{n-1} &= \text{the sum of all products of } n-1 \text{ distinct } t_j \\
&= \frac{t_1 t_2 \dots t_n}{t_1} + \frac{t_1 t_2 \dots t_n}{t_2} + \cdots + \frac{t_1 t_2 \dots t_n}{t_n} \\
s_n &= \text{the product of all } t_j \\
&= t_1 t_2 \dots t_n.
\end{aligned}
$$

For example, with $n = 4$ we get

$$s_2 = t_1t_2 + t_1t_3 + t_1t_4 + t_2t_3 + t_2t_4 + t_3t_4 \qquad \text{and} \qquad s_3 = t_1t_2t_3 + t_1t_2t_4 + t_1t_3t_4 + t_2t_3t_4.$$

The preceding functions are called the **elementary symmetric functions**. Here is a symmetric function that is not elementary:

$$\frac{t_1^3 + t_2^3 + t_3^3 + t_4^3}{t_1 t_2 t_3 t_4}.$$

The elementary symmetric functions generate a subfield of $F$, namely $E = L(s_0, s_1, s_2, \dots, s_n)$. Then we have the tower

$$E = L(s_0, s_1, \dots, s_n) \subseteq F = \mathrm{Fix}(S_n) \subseteq K = L(t_1, \dots, t_n).$$

(Here, $s_0 = 1$ could be omitted since $1 \in L$ already.)

It might be interesting to observe that the number of summands in $s_k$ is $\binom{n}{k}$, that is, the $k$th

binomial coefficient. In building a term $t_{i_1}t_{i_2}\dots t_{i_k}$ to contribute to the sum $s_k$, we need to choose $k$ of the variables $t_1,\dots,t_n$.

Getting back to Artin's theorem we see that

$$S_n = \mathrm{Gal}(K/F) \qquad \text{and so} \qquad [K:F] = |\mathrm{Gal}(K/F)| = n!.$$

Our goal is to prove that the inclusion $E \subseteq F$ in the tower in Figure 15 is in fact an equality:

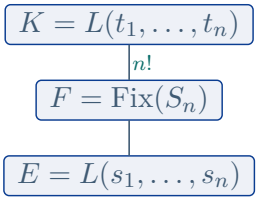



FIGURE 15

To see that $E = F$, it is enough to show that $[F:E] = 1$. The tower theorem shows that

$$[F:E] = 1 \text{ if and only if } [K:E] = n!.$$

Since $[K:E] \geq n!$ from the tower theorem, all we need to check is that $[K:E] \leq n!$. To that end, here is a little result about splitting fields in general. This is already obvious from Proposition 0.76, but we will include a short direct proof.

**Proposition 0.121** If $K$ is the splitting field of a polynomial $f \in F[x]$, and $n = \deg f$, then $[K:F] \leq n!$.

**Proof.** We prove this by induction on $n$. For $n = 1$, we have $K = F$ and $[K:F] = 1 \leq 1!$. Now let $f \in F[x]$ have degree $n$, and suppose the result holds for polynomials of degree $n-1$. Pick a root $\alpha$ of $f$ in $K$, put $E = F[\alpha]$, and write $f = (x-\alpha)g$ for some $g \in E[x]$. The field $K$ is also the splitting field of $g$ over $E$. Indeed, if $\alpha_2,\dots,\alpha_k$ are the roots of $g$, then

$$K = F[\alpha,\alpha_2,\dots,\alpha_k] = F[\alpha][\alpha_2,\dots,\alpha_k] = E[\alpha_2,\dots,\alpha_k].$$

(Here separability is not an issue, so $k$ need not be $n$.) Since $\deg g = n-1$, the inductive hypothesis yields $[K:E] \leq (n-1)!$. Then the tower theorem gives

$$[K:F] = [K:E][E:F] \leq (n-1)! \cdot n = n!$$

(Note: $[E : F] \leq n$ because $[E : F]$ is the degree of the minimal polynomial of $\alpha$, and that minimal polynomial has to divide $f$ because $\alpha$ is a root of $f$.) □

Getting back to the tower above, we will see that $[K : E] \leq n!$ by finding a polynomial $f$ in $E[x]$ with $\deg f = n$ and having $K$ as its splitting field. Then Proposition 0.121 will do it.

Here is that polynomial in $E[x]$:

$$f = (x - t_1)(x - t_2)(x - t_3) \cdots (x - t_n) \tag{0.7}$$

Obviously $\deg f = n$. On the surface $f$ seems to be in $K[x]$, but after a little reflection we see that

$$f = x^n - s_1 x^{n-1} + s_2 x^{n-2} - s_3 x^{n-3} + \cdots + (-1)^k s_k x^{n-k} + \cdots + (-1)^{n-1} s_{n-1} x + (-1)^n s_n$$

which is *definitely* in $E[x]$. For instance,

$$(x - t_1)(x - t_2)(x - t_3) = x^3 - (t_1 + t_2 + t_3)x^2 + (t_1 t_2 + t_1 t_3 + t_2 t_3)x - t_1 t_2 t_3.$$

One way to see that this formula holds is to note that the $(n-k)$th term of $f$ comes from choosing $n-k$ factors of $x$, one from each of $n-k$ brackets, and choosing the factors $-t_j$ from the remaining $k$ brackets.

Equation (0.7) shows that $f$ splits in $K[x]$. Finally, $K$ is the splitting field of $f$ because the roots of $f$ are $t_1, t_2, \ldots, t_n$, so the field $E[t_1, \ldots, t_n]$ generated by those roots, which sits inside $K = L(t_1, \ldots, t_n)$, must contain those roots and therefore contain $K$. Hence $E[t_1, \ldots, t_n] = K$.

Proposition 0.121 activates to yield

$$L(s_0, s_1, s_2, \ldots, s_n) = \mathrm{Fix}(S_n) = \text{the field of symmetric rational functions in } n \text{ variables.}$$

This famous result, which comes from Artin's theorem, is known as the **symmetric function theorem**. Here it is in concise form.

**Proposition 0.122 (Symmetric function theorem)** Every symmetric rational function in $n$ variables can be written as a rational function of the elementary symmetric functions.

Now, given a symmetric function, there are algorithms for expressing it in terms of the elementary

functions, but here is an example done *ad hoc*:

**Example 0.123** Take $r = t_1^2 + t_2^2 + t_3^2$ in $\mathrm{Fix}(S_3)$. Notice that

$$(t_1 + t_2 + t_3)^2 = t_1^2 + t_2^2 + t_3^2 + 2(t_1t_2 + t_1t_3 + t_2t_3).$$

So $s_1^2 = r + 2s_2$ and then

$$r = s_1^2 - 2s_2.$$

Here is an easier one:

**Example 0.124** Take $r = 1/t_1 + 1/t_2 + 1/t_3 + 1/t_4$ in $\mathrm{Fix}(S_4)$. Then

$$r = \frac{t_2t_3t_4 + t_1t_3t_4 + t_1t_2t_4 + t_1t_2t_3}{t_1t_2t_3t_4} = \frac{s_3}{s_4}.$$

Here is one that is not too bad:

**Example 0.125** $r = (t_1 - t_2)^2$ in $\mathrm{Fix}(S_2)$. Then

$$r = t_1^2 + t_2^2 - 2t_1t_2 = (t_1 + t_2)^2 - 4t_1t_2 = s_1^2 - 4s_2,$$

which turns out to be the discriminant of the quadratic polynomial

$$(x - t_1)(x - t_2) = x^2 - (t_1 + t_2)x + t_1t_2 = x^2 - s_1x + s_2.$$

Here is one more:

**Example 0.126** Take $r = t_1^2t_2^2 + t_1^2t_3^2 + t_2^2t_3^2$. Notice that

$$\begin{aligned} s_2^2 &= (t_1t_2 + t_1t_3 + t_2t_3)^2 \\ &= t_1^2t_2^2 + t_1^2t_3^2 + t_2^2t_3^2 + 2t_1^2t_2t_3 + 2t_1t_2^2t_3 + 2t_1t_2t_3^2 \\ &= r + 2t_1t_2t_3(t_1 + t_2 + t_3) \\ &= r + 2s_1s_3. \end{aligned}$$

So $r = s_2^2 - 2s_1s_3$.

## Galois Groups of Quadratics and Cubics

Here we need to divide by 2, so we assume that $\mathrm{char}(F) \neq 2$.

An irreducible $f = x^2 + bx + c$ in $F[x]$ is always separable because $f' = 2x + b \neq 0$. If $K$ is the splitting field of $f$ we get $f = (x - \alpha_1)(x - \alpha_2)$ where $\alpha_1, \alpha_2$ are the distinct roots of $f$ and $K = F[\alpha_1, \alpha_2]$. We can see that

$$b = -(\alpha_1 + \alpha_2) \qquad \text{and} \qquad c = \alpha_1\alpha_2.$$

Then

$$(\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = b^2 - 4c.$$

This familiar quantity is called the **discriminant** of $f$, which is clearly a square in $K$.

Let $\sqrt{b^2 - 4c}$ stand for $\alpha_1 - \alpha_2$ in $K$. Then

$$\frac{-b + \sqrt{b^2 - 4c}}{2} = \frac{\alpha_1 + \alpha_2 + (\alpha_1 - \alpha_2)}{2} = \alpha_1$$

and

$$\frac{-b - \sqrt{b^2 - 4c}}{2} = \frac{\alpha_1 + \alpha_2 - (\alpha_1 - \alpha_2)}{2} = \alpha_2.$$

We have rediscovered the familiar **quadratic formula** for the roots. Then, with $\delta = \sqrt{b^2 - 4c}$ in $K$, we see that $K = F[\delta]$, where the minimal polynomial of $\delta$ is $X^2 - (b^2 - 4c)$. Thus $[K : F] = 2$, and by the Galois correspondence $|\mathrm{Gal}(K/F)| = 2$. In addition to id, the other element in $\mathrm{Gal}(K/F)$ is determined by the transposition $\alpha_1 \leftrightarrow \alpha_2$.

There is not much else to say about quadratics. For something more interesting, we turn to irreducible cubics. We now assume that $\mathrm{char}(F) \neq 2, 3$, and the most important case is $\mathbb{Q}$.

Suppose $f = x^3 + ax^2 + bx + c$ is an irreducible, separable cubic in $F[x]$. Let $K$ be its splitting field containing the three distinct roots $\alpha_1, \alpha_2, \alpha_3$ of $f$. In $K[x]$, we have

$$f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3,$$

so

$$a = -(\alpha_1 + \alpha_2 + \alpha_3), \qquad b = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \qquad \text{and} \qquad c = -\alpha_1\alpha_2\alpha_3,$$

which are, up to sign, the elementary symmetric functions $s_1, s_2, s_3$ evaluated at the roots $\alpha_1, \alpha_2, \alpha_3$.

Since $\alpha_3 = -a-\alpha_1-\alpha_2$ we see that $K = F[\alpha_1, \alpha_2] = F[\alpha_1][\alpha_2]$. Then $[F[\alpha_1] : F] = 3$ because $f$ is irreducible. We have $f = (x-\alpha_1)g$ for some quadratic $g$ in $F[\alpha_1][x]$. Actually, $g = (x-\alpha_2)(x-\alpha_3)$ in $K[x]$.

If $\alpha_2 \in F[\alpha_1]$, so is $\alpha_3 = -a - \alpha_1 - \alpha_2 \in F[\alpha_1]$, and then $K = F[\alpha_1]$ and $[K : F] = 3$. On the other hand, if $\alpha_2 \notin F[\alpha_1]$, then $g$ is an irreducible quadratic in $F[\alpha_1][x]$, in which case $[K : F[\alpha_1]] = [F[\alpha_1][\alpha_2] : F[\alpha_1]] = 2$, and then $[K : F] = 6$, by the tower theorem. Since $K$ is a Galois extension,

$$|\mathrm{Gal}(K/F)| = [K : F] = 3 \text{ or } 6.$$

We also saw that if $\Delta = \{\alpha_1, \alpha_2, \alpha_3\}$ and $S(\Delta)$ is the group of permutations of $\Delta$, then the restriction

$$\begin{aligned} \Gamma : \mathrm{Gal}(K/F) &\longrightarrow S(\Delta) \\ \varphi &\longmapsto \varphi|_\Delta \end{aligned}$$

is an injective group homomorphism, whose image in $S(\Delta)$ is either a subgroup of order 3 or 6. But $S(\Delta)$ is just a poorly disguised version of the symmetric group $S_3$ of permutations on the three letters $\{1, 2, 3\}$.

The elements of $S_3$, in cycle notation, are

$$\mathrm{id}, (12), (13), (23), (123), (132).$$

The only subgroup of $S_3$ of order 3 is $A_3 = \{\mathrm{id}, (123), (132)\}$, which is the alternating group of even permutations, and also a cyclic group of order 3. The only subgroup of $S_3$ of order 6 is $S_3$ itself. Thus we get the following:

**Proposition 0.127** The Galois group of an irreducible cubic is either $A_3$ or $S_3$.

Note that if $f$ is a polynomial, we often refer to the Galois group of its splitting field simply as the **Galois group of $f$**.

**Example 0.128** The Galois group of $x^3 - 2$, whose splitting field is $K = \mathbb{Q}[\sqrt[3]{2}, e^{\pi i/3}]$, is $S_3$ (up to isomorphism). We checked this back in Example 0.102, and it also follows from the Galois correspondence since $[K : \mathbb{Q}] = 6$, so $|\mathrm{Gal}(K/\mathbb{Q})| = 6$.

**Exercise 0.129** The splitting field $K$ of $f = x^3 - 3x + 1$ has degree 3 over $\mathbb{Q}$, so the Galois group of $f$ is $A_3$.

In Exercise 0.129, how do we tell whether the Galois group is $A_3$ or $S_3$? For that we need the discriminant of the cubic $f$, which is the element

$$D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2.$$

(An analogous definition can be made for all polynomials, but we will stick with our irreducible cubic.) For any $\sigma \in \mathrm{Gal}(K/F)$, a quick inspection reveals that $\sigma(D) = D$, because $\sigma$ permutes the roots $\alpha_1, \alpha_2, \alpha_3$ and $D$ is a symmetric function of those roots. Thus we get $D \in \mathrm{Fix}(\mathrm{Gal}(K/F)) = F$.

Next, let $d = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$ in $K$. Clearly $d^2 = D$, and if $\sigma \in \mathrm{Gal}(K/F)$, we can see that $\sigma(d) = d$ when $\sigma$ is even and $\sigma(d) = -d$ when $\sigma$ is odd. (Note that since the $\alpha_1, \alpha_2, \alpha_3$ are distinct, $d \neq 0$, and since $\mathrm{char}(F) \neq 2$, we have $d \neq -d$.) So if $\mathrm{Gal}(K/F)$ restricts to $A_3$ inside $S(\Delta)$, we get $\sigma(d) = d$ for all $\sigma \in \mathrm{Gal}(K/F)$. Then $d \in \mathrm{Fix}(\mathrm{Gal}(K/F)) = F$. But if $\mathrm{Gal}(K/F)$ restricts to $S_3 = S(\Delta)$, then $d \notin \mathrm{Fix}(\mathrm{Gal}(K/F)) = F$.

After recalling that $d^2 = D$, we get the following cute result:

**Proposition 0.130** If $\mathrm{char}(F) \neq 2$, the Galois group of a separable irreducible cubic in $F[x]$ is

- $A_3$ when the discriminant $D$ has a square root in $F$.
- $S_3$ when the discriminant $D$ has no square root in $F$.

Although Proposition 0.130 is rather nice, there remains the nagging question of how to calculate $D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$ when the roots $\alpha_1, \alpha_2, \alpha_3$ of $f = x^3 + ax^2 + bx + c$ might not be known.

For instance, in the case of a quadratic $x^2 + bx + c$ we have no trouble writing down the discriminant $b^2 - 4c$ without any reference to the roots of $x^2 + bx + c$. But in the case of the cubic $f = x^3 + ax^2 + bx + c$, there is a nasty formula for $D$ in terms of the coefficients $a, b, c$, which almost nobody remembers. To get a more manageable formula, we use a little trick called the **Tschirnhausen transformation**.

Here we need $\mathrm{char}(F) \neq 3$. If $f(x) = x^3 + ax^2 + bx + c$, let $g(x) = f(x - a/3)$, which is the

Tschirnhausen transform. Then

$$\begin{aligned} g(x) &= \left(x - \frac{a}{3}\right)^3 + a\left(x - \frac{a}{3}\right)^2 + b\left(x - \frac{a}{3}\right) + c \\ &= x^3 - 3x^2\left(\frac{a}{3}\right) + 3x\left(\frac{a^2}{9}\right) - \frac{a^3}{27} + ax^2 - \frac{2a^2}{3}x + \frac{a^3}{9} + bx - \frac{ab}{3} + c \\ &= x^3 + px + q \end{aligned}$$

where $p, q$ are suitable coefficients in $F$. But the coefficient of $x^2$ is gone!

If $\alpha_1, \alpha_2, \alpha_3$ are the roots of $f$ in its splitting field $K$, then the roots of $g$ are

$$\beta_1 = \alpha_1 + \frac{a}{3}, \qquad \beta_2 = \alpha_2 + \frac{a}{3}, \qquad \text{and} \qquad \beta_3 = \alpha_3 + \frac{a}{3}.$$

Clearly $F[\alpha_1, \alpha_2, \alpha_3] = F[\beta_1, \beta_2, \beta_3] = K$. So $f$ and its Tschirnhausen transform $g$ have the same splitting field. Furthermore, the discriminants

$$(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 \qquad \text{and} \qquad (\beta_1 - \beta_2)^2(\beta_1 - \beta_3)^2(\beta_2 - \beta_3)^2$$

are equal. For these reasons it is both harmless — and preferable — to work with irreducible, separable cubics of type $g = x^3 + px + q$, where the $x^2$ term is gone.

We now compute $D$ for such $g$. We also have $g = (x - \beta_1)(x - \beta_2)(x - \beta_3)$, so

$$g'(x) = 3x^2 + p = (x - \beta_1)(x - \beta_2) + (x - \beta_1)(x - \beta_3) + (x - \beta_2)(x - \beta_3)$$

Plug in $x = \beta_1, \beta_2, \beta_3$, in turn, to get

$$3\beta_1^2 + p = (\beta_1 - \beta_2)(\beta_1 - \beta_3) \tag{0.8}$$
$$3\beta_2^2 + p = (\beta_2 - \beta_1)(\beta_2 - \beta_3) \tag{0.9}$$
$$3\beta_3^2 + p = (\beta_3 - \beta_1)(\beta_3 - \beta_2). \tag{0.10}$$

Multiply (0.8), (0.9), and (0.10) to see that

$$D = -(3\beta_1^2 + p)(3\beta_2^2 + p)(3\beta_3^2 + p)$$

By multiplying this out, we get

$$D = -\Big(27\beta_1^2\beta_2^2\beta_3^2 + 9p(\beta_1^2\beta_2^2 + \beta_1^2\beta_3^2 + \beta_2^2\beta_3^2) + 3p^2(\beta_1^2 + \beta_2^2 + \beta_3^2) + p^3\Big).$$

We also see that

$$g = x^3 - (\beta_1 + \beta_2 + \beta_3)x^2 + (\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3)x - \beta_1\beta_2\beta_3$$

and so

$$\beta_1 + \beta_2 + \beta_3 = 0, \qquad \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 = p, \qquad \text{and} \qquad \beta_1\beta_2\beta_3 = -q.$$

Using the standard symmetric identities with $t_1, t_2, t_3$ replaced by $\beta_1, \beta_2, \beta_3$, we get

$$\beta_1^2\beta_2^2 + \beta_1^2\beta_3^2 + \beta_2^2\beta_3^2 = (\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3)^2 - 2(\beta_1 + \beta_2 + \beta_3)(\beta_1\beta_2\beta_3) = p^2 - 2 \cdot 0 \cdot (-q) = p^2,$$

and

$$\beta_1^2 + \beta_2^2 + \beta_3^2 = (\beta_1 + \beta_2 + \beta_3)^2 - 2(\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3) = 0^2 - 2p = -2p.$$

So $D$ up above becomes

$$D = -(27q^2 + 9p(p^2) + 3p^2(-2p) + p^3) = -4p^3 - 27q^2.$$

This formula for the discriminant of $x^3 + px + q$ is worth memorizing (at least for exam purposes).

**Example 0.131** For $g = x^3 - 3x + 1$ in $\mathbb{Q}[x]$, we have

$$D = -4(-3)^3 - 27(1)^2 = 81$$

which is a perfect square in $\mathbb{Q}$.

So by Proposition 0.130, the Galois group for $g$ is $A_3$ and the degree of the splitting field over $\mathbb{Q}$ is 3.

**Example 0.132** For $g = x^3 - 4x + 2$, we get

$$D = -4(-4)^3 - 27(2)^2 = 148$$

which is not a perfect square in $\mathbb{Q}$. Thus, by Proposition 0.130, the Galois group for this is $S_3$.

**Example 0.133** If $g = x^3 + q$ is irreducible in $\mathbb{Q}[x]$, then $q \neq 0$ and $D = -27q^2$, which is not a square in $\mathbb{Q}$. Thus, by Proposition 0.130, the Galois group is $S_3$.

## The Galois Group of $X^n - 1$

The polynomial $X^n - 1$ in $\mathbb{Q}[x]$ has roots $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$ where $\zeta_n = e^{2\pi i/n}$. The set $T_n$ of these roots is a cyclic group generated by $\zeta_n$. The other generators of $T_n$ are $\zeta_n^k$, where $\gcd(k, n) = 1$. These generators are known as **primitive $n$th roots of unity**.

Let $\Lambda_n$ be the set of primitive $n$th roots of unity. Clearly, the splitting field of $X^n - 1$ is $K = \mathbb{Q}[\zeta]$ where $\zeta$ is any element of $\Lambda_n$. We want $\mathrm{Gal}(K/\mathbb{Q})$, and for that we need the minimal polynomial of such a $\zeta$ in $\Lambda_n$.

If $d \mid n$, then $X^d - 1 \mid X^n - 1$, and so the group $T_d$ of $d$th roots of 1 is a subgroup of $T_n$. Inside $T_d$, we have $\Lambda_d$, the set of primitive $d$th roots of unity that generate $T_d$. We can think of $\Lambda_d$ as the set of elements in $T_n$ whose order is $d$.

Clearly $T_n = \bigcup_{d|n} \Lambda_d$, and this union is disjoint. Then, in $K[X]$, we split $X^n - 1$ as

$$X^n - 1 = \prod_{\zeta \in T_n} (X - \zeta) = \prod_{d|n} \left( \prod_{\zeta \in \Lambda_d} (X - \zeta) \right). \tag{0.11}$$

The polynomial

$$\Phi_d(X) = \prod_{\zeta \in \Lambda_d} (X - \zeta)$$

is called the $d$th **cyclotomic polynomial**. (0.11) becomes

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

By rewriting this as

$$X^n - 1 = \left( \prod_{\substack{d|n \\ d<n}} \Phi_d(X) \right) \Phi_n(X),$$

we obtain a recursive method for calculating the $n$th cyclotomic polynomial from earlier ones.

We might also recall that if $n = p$ is prime, then all $\zeta$ in $T_p$ are primitive $p$th roots, except $\zeta = 1$. In this case, the factorization

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

tells us that $\Phi_p(X) = X^{p-1} + \cdots + X + 1$.

We can calculate the first few $\Phi_n$ recursively.

$$\begin{aligned}
\Phi_1 &= X - 1 \\
\Phi_2 &= X + 1 \\
\Phi_3 &= X^2 + X + 1 \\
\Phi_4 &= (X - i)(X + i) = X^2 + 1 \quad \text{because the primitive 4th roots are } \pm i \\
\Phi_5 &= X^4 + X^3 + X^2 + X + 1
\end{aligned}$$

To get $\Phi_6$, we can use

$$X^6 - 1 = \Phi_1\Phi_2\Phi_3\Phi_6 = (X - 1)(X + 1)(X^2 + X + 1)\Phi_6(X),$$

so

$$\Phi_6 = \frac{X^6 - 1}{(X - 1)(X + 1)(X^2 + X + 1)} = X^2 - X + 1.$$

Here the primitive 6th roots are $\omega = e^{2\pi i/6} = e^{\pi i/3}$ and $\bar{\omega} = e^{-\pi i/3} = \omega^5$. Figure 16 shows all six roots and highlights the notation just used.

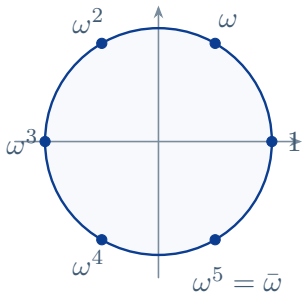



FIGURE 16

Then

$$\Phi_7 = X^6 + \cdots + X + 1,$$

and

$$\Phi_8 = \frac{X^8 - 1}{\Phi_1\Phi_2\Phi_4} = \frac{X^8 - 1}{(X - 1)(X + 1)(X^2 + 1)} = \frac{X^8 - 1}{X^4 - 1} = X^4 + 1.$$

One more!

$$\Phi_9 = \frac{X^9-1}{\Phi_1\Phi_3} = \frac{X^9-1}{(X-1)(X^2+X+1)} = \frac{X^9-1}{X^3-1} = X^6+X^3+1.$$

It gets messier as we go up.

The degree of $\Phi_n(X)$ is $|\Lambda_n| = \varphi(n)$, where $\varphi(n)$ is **Euler's totient function** at $n$: the number of integers $k$ from 1 to $n$ that are coprime with $n$, or equivalently, the number of units in the ring $\mathbb{Z}_n$. (Here $\varphi$ is not an automorphism.)

Our goal is to see that $\Phi_n(X) \in \mathbb{Z}[X]$ and is irreducible in $\mathbb{Q}[X]$. To begin with:

**Proposition 0.134** $\Phi_n(X) \in \mathbb{Z}[X]$.

**Proof.** We use induction on $n$. Clear for $n = 1$. Suppose $\Phi_d(X) \in \mathbb{Z}[X]$ for all $d < n$. We then have $X^n - 1 = g(X)\Phi_n(X)$ where $g(X) = \prod_{\substack{d|n \\ d<n}} \Phi_d(X)$. By the inductive assumption $g(X) \in \mathbb{Z}[X]$, and $g(X)$ is clearly monic. Now $X^n - 1, g(X) \in \mathbb{Q}[X]$ and $g(X) \mid X^n - 1$ in $K[X]$. By an old exercise (see assignment 1) we see that $g(X) \mid X^n - 1$ in $\mathbb{Q}[X]$. Thus $\Phi_n(X) \in \mathbb{Q}[X]$. In order to get $\Phi_n(X) \in \mathbb{Z}[X]$, we can use Gauss' lemma. There is a $c \in \mathbb{Q}$ such that $cg, 1/c\Phi_n \in \mathbb{Z}[X]$ and $X^n - 1 = (cg)(1/c\Phi_n)$. But $g, \Phi_n$ are monic. So the lead coefficients of $cg$ and $1/c\Phi_n$ are $c$ and $1/c$, respectively, which must lie in $\mathbb{Z}$. Thus $c = \pm 1$, and so $\Phi_n \in \mathbb{Z}[X]$. □

To get that $\Phi_n$ is irreducible in $\mathbb{Q}[X]$ is more serious business.

**Proposition 0.135** $\Phi_n$ is irreducible in $\mathbb{Q}[X]$.

**Proof.** We will prove that $\Phi_n$ is the minimal polynomial $g$ of $\zeta_n = e^{2\pi i/n}$. Since $\Phi_n(\zeta_n) = 0$, we see that $g \mid \Phi_n$ in $\mathbb{Q}[X]$. If we can show that $g = \Phi_n$, we will be done, since $g$ is irreducible. We claim that if $\zeta$ is a root of $g$ and $p$ is a prime with $p \nmid n$, then $\zeta^p$ is also a root of $g$.

This will help because the roots of $\Phi_n$ are $\zeta_n^k$ where $\zeta_n = e^{2\pi i/n}$ and $\gcd(k, n) = 1$. Each such $k$ takes the form $k = p_1 p_2 \dots p_r$, where the $p_j$ are primes and $p_j \nmid n$. Our $\zeta_n$ is a root of $g$, because $g$ is its minimal polynomial. From this claim, it will follow that $\zeta_n^{p_1}$ is a root of $g$, and then $\zeta_n^{p_1 p_2}$ is a root of $g$, and then $\zeta_n^{p_1 p_2 p_3}$ is a root of $g$, and so on until $\zeta_n^k$ is a root of $g$. Thus all roots of $\Phi_n$ will be roots of $g$. This will reveal that $\deg \Phi_n \leq \deg g$, and since $g \mid \Phi_n$ in $\mathbb{Q}[X]$ it will follow that $g = \Phi_n$.

So we need to prove the claim.

For $f = \sum_j a_j X^j$ in $\mathbb{Z}[X]$ and our prime $p$, let $\bar{f} = \sum_j \bar{a}_j X^j$ be its polynomial in $\mathbb{Z}_p[X]$. Here $\bar{a}_j$ is the residue of $a_j$ in $\mathbb{Z}_p$. Since

$$X^n - 1 = \Phi_n q \qquad \text{and} \qquad q = \prod_{\substack{d|n \\ d<n}} \Phi_d \in \mathbb{Z}[X],$$

we have $\overline{X^n - 1} = \overline{\Phi}_n \bar{q}$. The derivative $(X^n - 1)' = \bar{n} X^{n-1} \neq 0$ in $\mathbb{Z}_p[X]$ because $p \nmid n$. In fact the equation $\bar{n}^{-1} X(\bar{n} X^{n-1}) - (X^n - 1) = 1$ reveals that $\bar{n} X^{n-1}, X^n - 1$ are coprime in $\mathbb{Z}_p[X]$. Thus $X^n - 1$ has no repeated factors in $\mathbb{Z}_p[X]$. Since $\overline{\Phi}_n \mid X^n - 1$, it follows that $\overline{\Phi}_n$ has no repeated factor in $\mathbb{Z}_p[X]$.

We also had $g \mid \Phi_n$ in $\mathbb{Q}[X]$. Write $\Phi_n = gh$ with $h \in \mathbb{Q}[X]$. Because $\Phi_n$ is monic and integral, Gauss' lemma gives $g, h \in \mathbb{Z}[X]$. Now take a root $\zeta$ of $g$. Thus $\zeta$ is a root of $\Phi_n$, so it is a primitive $n$th root of unity; because $p \nmid n$, the same is true of $\zeta^p$. Therefore $0 = \Phi_n(\zeta^p) = g(\zeta^p) h(\zeta^p)$.

Suppose $g(\zeta^p) \neq 0$ and look for a contradiction. In that case $h(\zeta^p) = 0$. If $f$ is given by $f(X) = h(X^p)$, we see that $\zeta$ is a root of $f$. Since $g$ is the minimal polynomial of $\zeta$, we have

$$f = gk \text{ for some } k \in \mathbb{Q}[X].$$

Since $f, g$ are monic and in $\mathbb{Z}[X]$, Gauss' lemma teaches us that $k \in \mathbb{Z}[X]$. Then we get $\bar{f} = \bar{g}\bar{k}$ in $\mathbb{Z}_p[X]$. But $f(X) = h(X^p)$ leads to

$$\bar{f}(X) = \bar{h}(X^p) = (\bar{h}(X))^p$$

by Fermat's theorem in $\mathbb{Z}_p$ and the Frobenius map on $\mathbb{Z}_p[X]$. Thus $\bar{h}^p = \bar{g}\bar{k}$ in $\mathbb{Z}_p[X]$.

Now, any irreducible factor of $\bar{g}$ in $\mathbb{Z}_p[X]$ is also a factor of $\bar{h}$ in $\mathbb{Z}_p[X]$. But from $\Phi_n = gh$ in $\mathbb{Z}[X]$ we get $\overline{\Phi}_n = \bar{g}\bar{h}$ in $\mathbb{Z}_p[X]$. Now we see that $\overline{\Phi}_n$ has to have a repeated irreducible factor in $\mathbb{Z}_p[X]$, contrary to what we had shown. □

With the knowledge that $\Phi_n = \prod_{\zeta \in \Lambda_n} (X - \zeta)$ is the minimal polynomial of $\zeta_n = e^{2\pi i/n}$, several useful consequences follow. The set $\Lambda_n$ of primitive $n$th roots of unity consists precisely of the conjugates of $\zeta_n = e^{2\pi i/n}$. The splitting field of $X^n - 1$ is $\mathbb{Q}[\zeta]$, where $\zeta$ is any primitive $n$th root of unity. Also,

$$|\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})| = [\mathbb{Q}[\zeta] : \mathbb{Q}] = \varphi(n),$$

which is the number of elements in the multiplicative group $\mathbb{Z}_n^*$ of units in the ring $\mathbb{Z}_n$.

This now anticipates what $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ will look like.

**Proposition 0.136** If $K$ is the splitting field of $X^n - 1$ over $\mathbb{Q}$, then $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_n^*$.

**Proof.** The roots of $X^n - 1$ form the cyclic group $T_n$ of order $n$, which is generated by $\zeta_n = e^{2\pi i/n}$ or any one of its conjugates $\zeta$ in $\Lambda_n$ (i.e., the roots of $\Phi_n$). If $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, then $\sigma(T_n) = T_n$ because roots of $X^n - 1$ go to roots of $X^n - 1$. Let $\mathrm{Aut}(T_n)$ be the group of group-automorphisms of $T_n$. We get the restriction homomorphism

$$\Gamma : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}(T_n)$$

If $\sigma \in \ker(\Gamma)$, then $\sigma|_{T_n} = \mathrm{id}$ on $T_n$. Since $K = \mathbb{Q}[\zeta]$ for some $\zeta$ in $T_n$ (actually $\zeta \in \Lambda_n$), it follows that $\sigma = \mathrm{id}$ on $K$. Thus $\Gamma$ is injective. Now it is well known that for any cyclic group of order $n$, such as $T_n$, there is an isomorphism

$$\psi : \mathrm{Aut}(T_n) \cong \mathbb{Z}_n^*. \tag{0.12}$$

Then $\psi \circ \Gamma : \mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{Z}_n^*$ is an injective group homomorphism. But $|\mathrm{Gal}(K/\mathbb{Q})| = \varphi(n) = |\mathbb{Z}_n^*|$. Thus $\psi \circ \Gamma$ is a group isomorphism. □

To remind ourselves of (0.12): the group automorphisms $\tau$ of $T_n$ are in one-to-one correspondence with the integers $k$ such that $1 \le k < n$ and $\gcd(k, n) = 1$. These $k$ are the unique representatives of their residues $\bar{k}$ in $\mathbb{Z}_n^*$. The resulting correspondence $\tau \leftrightarrow \bar{k}$ is the isomorphism in (0.12).

We should note that $\mathrm{Gal}(K/\mathbb{Q})$ is an abelian group.

In the case $n$ is some prime $p$, our $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the cyclic group $\mathbb{Z}_p^*$ of nonzero elements in the field $\mathbb{Z}_p$.

**Example 0.137** In the case $n = 15$, $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ is an 8-element abelian group under multiplication modulo 15. The possible abelian groups of order $8 = 2^3$ are, up to isomorphism,

$$C_8, \qquad C_4 \times C_2, \qquad \text{and} \qquad C_2 \times C_2 \times C_2$$

where $C_j$ is the cyclic group of order $j$. Looking at $\mathbb{Z}_{15}^*$ we see that 2 has order 4 and there are no elements of order 8. So $\mathbb{Z}_{15}^* \cong C_4 \times C_2$. By determining the number of subgroups of $\mathbb{Z}_{15}^*$, we could (if we so desired) work out how many subfields are in $K$.

Let us look at — nay, *prove* — Proposition 0.136 again.

**Alternate proof of Proposition 0.136.** For each integer $k$ coprime with $n$, let $\bar{k}$ be its residue in $\mathbb{Z}_n$. Since $\gcd(k,n) = 1$ we get $\bar{k} \in \mathbb{Z}_n^*$, the group of units modulo $n$. Recall $K = \mathbb{Q}[\zeta]$ where $\zeta = e^{2\pi i/n}$. So let $\sigma_k$ be the automorphism of $K$ determined by the action

$$\sigma_k : \zeta \mapsto \zeta^k. \tag{0.13}$$

Automorphisms map elements to their conjugates. So every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ acts on $\zeta$ according to (0.13) for some $k$ coprime with $n$. By the isomorphism extension theorem, for every such $k$, there is a $\sigma_k \in \mathrm{Gal}(K/\mathbb{Q})$ that acts according to (0.13). Notice

$$\begin{aligned} \bar{k} = \bar{l} \text{ in } \mathbb{Z}_n^* &\text{ if and only if } k \equiv l \pmod{n} \\ &\text{if and only if } \zeta^k = \zeta^l \\ &\text{if and only if } \sigma_k = \sigma_l, \end{aligned}$$

where the last equivalence uses the fact that $\zeta$ has order $n$. This establishes the well-defined bijection

$$\begin{aligned} \Gamma : \mathbb{Z}_n^* &\longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \\ \bar{k} &\longmapsto \sigma_k. \end{aligned}$$

Then we observe that

$$\sigma_k \circ \sigma_l(\zeta) = \sigma_k(\zeta^l) = (\zeta^k)^l = \zeta^{kl} = \sigma_{kl}(\zeta)$$

Thus $\sigma_k \circ \sigma_l = \sigma_{kl}$. So

$$\Gamma(\bar{k}\bar{l}) = \Gamma(\overline{kl}) = \sigma_{kl} = \sigma_k\sigma_l = \Gamma(\bar{k})\Gamma(\bar{l})$$

Our $\Gamma$ is the desired isomorphism. □

## A Little Look Back at Cubics

Here is another way to see that if $f$ is an irreducible, separable cubic in $F[X]$, then the Galois group of its splitting field is either $A_3$ or $S_3$.

Let $K$ be the splitting field of $f$. Since $f$ is irreducible, we have $3 \mid [K : F]$. Indeed, pick a root $\alpha$ of $f$ in $K$ and look at the tower in Figure 17:


FIGURE 17

We also know that $[K : F] \leq 3! = 6$. So the only possible values for $[K : F]$ are 3 or 6. By the Galois correspondence, the only possible values of $|\mathrm{Gal}(K/F)|$ are 3 or 6.

If $\Delta = \{\alpha_1, \alpha_2, \alpha_3\}$ is the set of three distinct roots of $f$, then the restriction homomorphism

$$\pi : \mathrm{Gal}(K/F) \longrightarrow S(\Delta) = \text{the group of permutations of } \Delta$$

is injective. Indeed, if $\sigma \in \ker \pi$ then $\sigma$ fixes $\Delta$. Since $K = F[\Delta]$, $\sigma$ fixes $K$. So $\sigma = \mathrm{id}$ on $K$. So $\mathrm{Gal}(K/F)$ is embedded by $\pi$ as a subgroup of $S(\Delta)$, and this subgroup has order 3 or 6.

But $S(\Delta) = S_3$ is the group of permutations on 3 letters. The "letters" here are $\alpha_1, \alpha_2, \alpha_3$ (we could just call them $1, 2, 3$ if we wanted to). If $\mathrm{Gal}(K/F)$ has order 3, then

$$\mathrm{Gal}(K/F) \cong A_3 = \{\mathrm{id}, (123), (132)\}$$

the alternating group. If $\mathrm{Gal}(K/F)$ has order 6, then

$$\mathrm{Gal}(K/F) \cong S_3 = \text{the full group of permutations on 3 letters.}$$

## 7. Radical Extensions and Solvability

Throughout this last chapter, we make the assumption that our fields have characteristic 0. Later on, much can be adapted to characteristic $p$. Working in characteristic 0 lets us focus on the essential themes without worrying about separability.

Our goal is to prove the result that made Galois such a revered mathematician. Even with the Galois correspondence at our disposal, a great deal of difficult material remains. Stay buckled up, for we are about to embark on a long and winding road.

## Radical Extensions

**Definition 0.138** A tower of fields

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_k = K$$

is called a **radical tower** when each $F_{j+1} = F_j[\alpha_j]$ where $\alpha_j^{n_j} \in F_j$ for some positive $n_j$. So each $F_{j+1}$ in the tower comes from adjoining to $F_j$ a root of $x^{n_j} - a_j$ for some $a_j$ in $F_j$; in other words,

$$F_{j+1} = F_j[\sqrt[n_j]{a_j}] \text{ for some } a_j \text{ in } F_j.$$

The field $K$ that sits atop the tower is called a **radical extension** of $F$.

**Exercise 0.139** Find an extension $K$ of $F$ of finite degree that is not a radical extension. (This is more of a bonus problem than an exercise.)

We can see that the elements of a radical extension are built up from $F$ by repeated application of the operations

$$+, -, \cdot, \boldsymbol{\nabla}\cdot, \sqrt[n_1]{\ }, \sqrt[n_2]{\ }, \ldots, \sqrt[n_k]{\ }$$

In other words, they are built from the **radicals** $\sqrt[n]{\ }$ as well as the basic field operations.

For example, if $f = x^2 + bx + c$ in $\mathbb{Q}[x]$, the roots $(-b \pm \sqrt{b^2 - 4c})/2$ lie at the top of the radical tower

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{b^2 - 4c}],$$

which has just one inclusion.

As another example, let $f = x^3 + px + q$ be an irreducible cubic in $\mathbb{Q}[x]$. Put

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \qquad \text{and} \qquad v = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

choosing the cube roots coherently so that $uv = -p/3$. The famous **Cardano formula** (which time prevents us from proving) gives the three roots

$$u + v, \qquad \omega u + \omega^2 v, \qquad \text{and} \qquad \omega^2 u + \omega v,$$

where $\omega = e^{2\pi i/3}$.

There is no need to remember such an unwieldy formula, but it does reveal that the roots of $f$ sit in the radical extension $K$ given by the tower

$$\begin{aligned}\mathbb{Q} &\subseteq \mathbb{Q}[\sqrt{-3}] = F_0 \\ &\subseteq F_0\left[\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}\right] = F_1 \\ &\subseteq F_1\left[\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}\right] = F_2 \\ &\subseteq F_2\left[\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}\right] = K.\end{aligned}$$

**Definition 0.140** A polynomial $f$ in $F[x]$ is **solvable by radicals** if the roots of $f$ lie in a radical extension. Equivalently, the splitting field of $f$ is a subfield of a radical extension.

We just saw that quadratics and cubics are solvable by radicals, and so are quartics, even though time prevents us from showing this as well.

The problem of solving quintics (degree 5) by radicals was a centuries-old puzzle until Niels Henrik Abel found a quintic that was not solvable by radicals. But it was Évariste Galois who gave the complete answer as to when a polynomial can or cannot be solved by radicals. The problem has a fascinating history which deserves to be read at some time.

**Warning** Just because $f$ is solvable by radicals, it does not mean that the splitting field of $f$ is itself a radical extension – only that the splitting field sits inside a radical extension.

We now turn to the proof of Galois' theorem.

## Cyclic Extensions

**Definition 0.141** A finite Galois extension $K$ of $F$ is called a **cyclic extension** when $\mathrm{Gal}(K/F)$ is cyclic.

**Example 0.142** Let $p$ be a prime and let $K$ be the splitting field of $x^p - 1$ over $\mathbb{Q}$. We know that $K = \mathbb{Q}[\zeta_p]$ where $\zeta_p = e^{2\pi i/p}$. Moreover, $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_p^*$, the cyclic group of units in the field $\mathbb{Z}_p$.

We now present an important circumstance that leads to cyclic extensions.

**Proposition 0.143** Let $n$ be a positive integer, and let $F$ be a field of characteristic 0 over which $x^n - 1$ splits. Let $K = F[\alpha]$ for some $\alpha$ such that $\alpha^n \in F$ (that is, $K$ is a radical extension of $F$ whose radical tower has one inclusion). Then the following hold:

1. $K = F[\alpha]$ is the splitting field of $x^n - \alpha^n$ over $F$, and is thereby a Galois extension of $F$.
2. There is an integer $d$ such that $d \mid n$, $\alpha^d \in F$ and $x^d - \alpha^d$ is the minimal polynomial of $\alpha$ over $F$.
3. The degree $[F[\alpha] : F] = d$.
4. The Galois group $\mathrm{Gal}(K/F)$ is cyclic of order $d$.

**Proof.** If $\alpha = 0$, then $K = F$ and all four claims hold with $d = 1$. We therefore assume $\alpha \neq 0$.

For (1), the polynomial $x^n - 1$, which splits in $F[x]$, is coprime with its derivative $nx^{n-1}$ since $F$ has characteristic 0. So $x^n - 1$ has $n$ roots in $F$, and they form a cyclic group. A generator $\zeta$ of this group is typically called a primitive $n$th root of unity. The distinct roots of $x^n - 1$ are $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$, all in $F$. Thus the distinct roots of $x^n - \alpha^n$ are

$$\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1}, \text{ all in } F[\alpha].$$

Hence $F[\alpha]$ is the splitting field of $x^n - \alpha^n$ over $F$.

For (2), let $d$ be the least positive integer such that $\alpha^d \in F$. We first check that $d \mid n$. Write $n = dq + r$ where $0 \leq r < d$. Then $\alpha^n = (\alpha^d)^q \alpha^r \in F$, and because $\alpha^d \neq 0$, we get $\alpha^r = \alpha^n/(\alpha^d)^q \in F$. The minimality of $d$ forces $r = 0$.

Now let $g \in F[x]$ be the minimal polynomial of $\alpha$. Since $\alpha$ is a root of $x^n - \alpha^n$, we get $g \mid x^n - \alpha^n$ in $F[x]$. So the roots of $g$ consist of some $\alpha\zeta^j$'s. Its constant term is therefore of the form $\pm\alpha^k\zeta^l$, where $k = \deg g$ and $l$ is some integer. This constant term lies in $F$, so $\alpha^k \in F$ because $\zeta^l \in F$. Since $\alpha$ is also a root of $x^d - \alpha^d$, we have $g \mid x^d - \alpha^d$ and hence $k \leq d$. The minimality of $d$ gives

$d \leq k$, so $k = d$ and $g = x^d - \alpha^d$.

For (3), the degree of the minimal polynomial now gives $[F[\alpha] : F] = d$.

For (4), since $F[\alpha]$ is a Galois extension of $F$ we get

$$|\mathrm{Gal}(F[\alpha]/F)| = [F[\alpha] : F] = \deg(x^d - \alpha^d) = d.$$

The roots of $x^d - \alpha^d$ are

$$\Delta = \{\alpha, \alpha\omega, \ldots, \alpha\omega^{d-1}\}$$

where $\omega = \zeta^{n/d}$ is a primitive $d$th root of 1, and $\omega \in F$. If $\sigma \in \mathrm{Gal}(F[\alpha]/F)$ we know $\sigma(\alpha) \in \Delta$. The map

$$\begin{aligned} \mathrm{Gal}(F[\alpha]/F) &\longrightarrow \Delta \\ \sigma &\mapsto \sigma(\alpha) \end{aligned}$$

is also injective, because $F$-maps that agree on the generator $\alpha$ must agree on $F[\alpha]$. Since $\mathrm{Gal}(F[\alpha]/F)$ and $\Delta$ both have $d$ elements, our correspondence $\sigma \mapsto \sigma(\alpha)$ is bijective. So the actions $\sigma : \alpha \mapsto \alpha\omega^j$ for $j = 0, \ldots, d-1$ capture all automorphisms in $\mathrm{Gal}(F[\alpha]/F)$. Define $\sigma \in \mathrm{Gal}(F[\alpha]/F)$ by $\sigma : \alpha \mapsto \alpha\omega$. Note $\sigma(\omega) = \omega$ since $\omega \in F$. Thus,

$$\begin{aligned} \sigma^2(\alpha) &= \sigma(\alpha\omega) = \alpha\omega\omega = \alpha\omega^2 \\ \sigma^3(\alpha) &= \sigma(\alpha\omega^2) = \alpha\omega\omega^2 = \alpha\omega^3 \\ &\vdots \\ \sigma^{d-1}(\alpha) &= \alpha\omega^{d-1} \\ \sigma^d(\alpha) &= \alpha\omega^d = \alpha. \end{aligned}$$

We have our generator $\sigma$ for the cyclic group $\mathrm{Gal}(F[\alpha]/F)$. □

## The Composite of Two Subfields

**Definition 0.144** If $E$ and $L$ are subfields of $K$, their **composite**, denoted by $EL$, is the smallest subfield of $K$ which contains both $E$ and $L$.

**Example 0.145** Let $E = \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{C}$ and $L = \mathbb{Q}[\sqrt[3]{2}, \omega] \subseteq \mathbb{C}$, where $\omega = e^{2\pi i/3}$. Then $EL = \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}, \omega]$.

More generally, if we have $F \subseteq E \subseteq K$ and $F \subseteq L = F[\alpha_1, \ldots, \alpha_n] \subseteq K$ with $\alpha_j$ algebraic over $F$, then $EL = E[\alpha_1, \ldots, \alpha_n]$. The inclusions are shown in Figure 18.

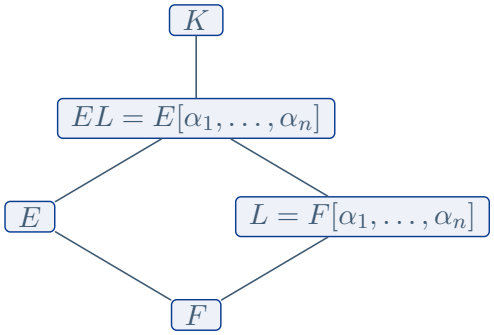



FIGURE 18

Here is a little result that we will need:

**Proposition 0.146** If $F \subseteq E \subseteq K$ and $F \subseteq L \subseteq K$, and $L$ is a Galois extension of $F$, then $EL$ is a Galois extension of $E$ and $\mathrm{Gal}(EL/E)$ is isomorphic to a subgroup of $\mathrm{Gal}(L/F)$.

**Proof.** The extension degrees needed in the proof are recorded in Figure 19.

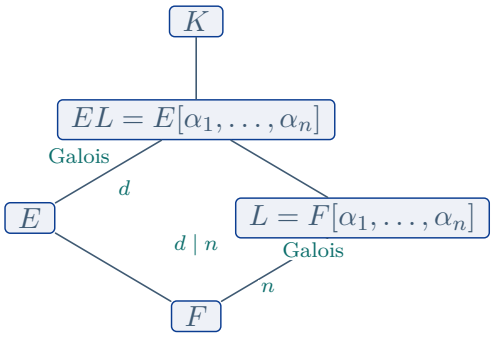



FIGURE 19

Being Galois, $L$ is the splitting field over $F$ of some polynomial $f \in F[X]$. Say $\alpha_1, \ldots, \alpha_n$ are the roots of $f$. Since $f \in F[X] \subseteq E[X]$, we can see that $EL = E[\alpha_1, \ldots, \alpha_n]$ is the splitting field of $f$ over $E$. So $EL$ is Galois over $E$.

Also, since $L$ is Galois over $F$, the normality theorem applies to $L$. That is, any automorphism $\sigma : EL \to EL$ which fixes $F$ is such that $\sigma(L) = L$. Define

$$\begin{aligned} \Gamma : \mathrm{Gal}(EL/E) &\longrightarrow \mathrm{Gal}(L/F) \\ \sigma &\longmapsto \sigma|_L. \end{aligned}$$

Note that $\sigma$ fixes $F$ because $\sigma$ fixes $E$. This $\Gamma$ is obviously a group homomorphism. Also if $\sigma \in \ker \Gamma$, then $\sigma|_L = \mathrm{id}$ on $L$. But $\sigma = \mathrm{id}$ on $E$ too. So $\sigma = \mathrm{id}$ on $EL = E[\alpha_1, \ldots, \alpha_n]$. Thus $\Gamma$ embeds $\mathrm{Gal}(EL/E)$ into $\mathrm{Gal}(L/F)$. □

## Radical Galois Extensions

The steps in the next result require some diligent but unavoidable bookkeeping.

**Proposition 0.147** If $F$ has characteristic 0, $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_k = K$ is a radical tower, and $L$ is the normal closure of $K$ over $F$, then $L$ also sits at the top of a radical tower.

**Proof.** Being in characteristic 0, we have $\gamma$ in $K$ such that $K = F[\gamma]$. Let $g$ be the minimal polynomial of $\gamma$ in $F[X]$. Then let $L$ be the splitting field of $g$ as a polynomial in $K[X]$. So $F \subseteq K \subseteq L$. Let $\gamma = \gamma_1, \gamma_2, \ldots, \gamma_n$ be the roots of $g$ in $L$.

$$\begin{aligned} L &= K[\gamma_1, \gamma_2, \ldots, \gamma_n], \quad \gamma_1 = \gamma \\ &= F[\gamma][\gamma_1, \gamma_2, \ldots, \gamma_n] \\ &= F[\gamma_1, \gamma_2, \ldots, \gamma_n], \end{aligned}$$

which makes $L$ the splitting field of $g$ over $F$ too. This $L$ is the normal closure of the extension $K$ of $F$. Being the splitting field of $g$ over $F$, our $L$ is a Galois extension of $F$. Now we need to build a radical tower running from $F$ to $L$. For each $j = 2, \ldots, n$ there is a $\sigma_j \in \mathrm{Gal}(L/F)$ such that $\sigma_j(\gamma) = \gamma_j$. This is because $L$ is the splitting field of the irreducible $g \in F[X]$ with roots $\gamma_1, \gamma_2, \ldots, \gamma_n$. So $\mathrm{Gal}(L/F)$ acts transitively on the roots. With these $\sigma_j$, build the following very big tower all inside $L$:

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_k = K = F[\gamma] = F[\gamma_1]$$

$$\begin{aligned}
&\subseteq F[\gamma_1]\sigma_2(F_0) \subseteq F[\gamma_1]\sigma_2(F_1) \subseteq F[\gamma_1]\sigma_2(F_2) \subseteq \dots \\
&\subseteq F[\gamma_1]\sigma_2(F_k) = F[\gamma_1]\sigma_2(F[\gamma]) = F[\gamma_1]F[\gamma_2] = F[\gamma_1,\gamma_2] \\
&= F[\gamma_1,\gamma_2]\sigma_3(F_0) \subseteq F[\gamma_1,\gamma_2]\sigma_3(F_1) \subseteq F[\gamma_1,\gamma_2]\sigma_3(F_2) \\
&\subseteq \cdots \subseteq F[\gamma_1,\gamma_2]\sigma_3(F_k) = F[\gamma_1,\gamma_2]\sigma_3(F[\gamma]) \\
&= F[\gamma_1,\gamma_2,\gamma_3] \subseteq \cdots \subseteq \\
&\subseteq F[\gamma_1,\dots,\gamma_{j-1}]\sigma_j(F_{i-1}) \subseteq F[\gamma_1,\dots,\gamma_{j-1}]\sigma_j(F_i) \\
&\subseteq \cdots \subseteq F[\gamma_1,\dots,\gamma_{n-1}]\sigma_n(F_k) \\
&= F[\gamma_1,\dots,\gamma_n] = L.
\end{aligned}$$

This is radical. Indeed, for each $i = 1,\dots,k$ there exists an $\alpha_i \in F_i$ and $n_i \geq 1$ such that $F_i = F_{i-1}[\alpha_i]$ and $\alpha_i^{n_i} \in F_{i-1}$. Looking at the general inclusion in the big tower, we see that

$$\sigma_j(F_i) = \sigma_j(F_{i-1}[\alpha_i]) = \sigma_j(F_{i-1})[\sigma_j(\alpha_i)],$$

so

$$F[\gamma_1,\dots,\gamma_{j-1}]\sigma_j(F_i) = F[\gamma_1,\dots,\gamma_{j-1}]\sigma_j(F_{i-1})[\sigma_j(\alpha_i)].$$

Moreover,

$$\sigma_j(\alpha_i)^{n_i} = \sigma_j(\alpha_i^{n_i}) \in \sigma_j(F_{i-1}) \subseteq F[\gamma_1,\dots,\gamma_{j-1}]\sigma_j(F_{i-1}).$$

Our big tower is radical. □

Next, we throw roots of unity into the soup.

**Proposition 0.148** Suppose $F$ has characteristic 0 and the following hold:

1. $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k = K$ is a radical tower and that $K$ is Galois over $F$.
2. $\alpha_i \in F_i$ and $n_i \geq 1$ for $i = 1,\dots,k$ and $F_i = F_{i-1}[\alpha_i]$ with $\alpha_i^{n_i} \in F_{i-1}$.
3. $n = n_1 n_2 \dots n_k$.
4. $L$ is the splitting field of $X^n - 1$ over $K$.
5. $\zeta$ in $L$ is a primitive $n$th root of 1.

Then the tower

$$F \subseteq F_0[\zeta] \subseteq F_1[\zeta] \subseteq \cdots \subseteq F_k[\zeta] = K[\zeta] = L$$

has these properties:

1. It is a radical tower.
2. $L$ is a Galois extension of $F$ and is thus a Galois extension of every $F_i[\zeta]$.
3. $F_i[\zeta]$ is Galois over $F_{i-1}[\zeta]$ and $\mathrm{Gal}(F_i[\zeta]/F_{i-1}[\zeta])$ is cyclic.
4. $F_0[\zeta]$ is Galois over $F$ and $\mathrm{Gal}(F_0[\zeta]/F)$ is abelian.

**Proof.** For (1), since $\zeta^n = 1 \in F$, the inclusion $F \subseteq F[\zeta] = F_0[\zeta]$ is radical. For $i = 1, \ldots, k$ we have $F_i = F_{i-1}[\alpha_i]$ and $\alpha_i^{n_i} \in F_{i-1}$. So $F_i[\zeta] = F_{i-1}[\zeta][\alpha_i]$ and $\alpha_i^{n_i} \in F_{i-1} \subseteq F_{i-1}[\zeta]$. Thus our tower is radical.

For (2), to see that $L$ is Galois over $F$, note that $K$ is the splitting field of some $f \in F[X]$. Thus $L$ is the splitting field of $(X^n - 1)f$ in $F[X]$. To make this explicit, observe that $L = K[\zeta] = F[\Delta, \zeta]$ where $\Delta$ is the set of roots of $f$. The other roots of $X^n - 1$ are powers of $\zeta$, and are therefore already in $F[\Delta, \zeta]$.

For (3), observe that each extension $F_i[\zeta]$ over $F_{i-1}[\zeta]$ fits the conditions of Proposition 0.143, because

$$F_i[\zeta] = F_{i-1}[\alpha_i][\zeta] = F_{i-1}[\zeta][\alpha_i],$$

with $\alpha_i^{n_i} \in F_{i-1} \subseteq F_{i-1}[\zeta]$, and $X^{n_i} - 1$ splits over $F_{i-1}[\zeta]$ since $n_i \mid n$ and $X^n - 1$ splits there. Hence Proposition 0.143 gives that $F_i[\zeta]$ is Galois over $F_{i-1}[\zeta]$ and $\mathrm{Gal}(F_i[\zeta]/F_{i-1}[\zeta])$ is cyclic.

For (4), note that the roots $1, \zeta, \ldots, \zeta^{n-1}$ lie in $F[\zeta]$, so $F[\zeta]$ is the splitting field of $X^n - 1$ over $F$. Thus $F[\zeta]$ is Galois over $F$. To see that $\mathrm{Gal}(F[\zeta]/F)$ is abelian, in characteristic 0 we use the compositum diagram in Figure 20.

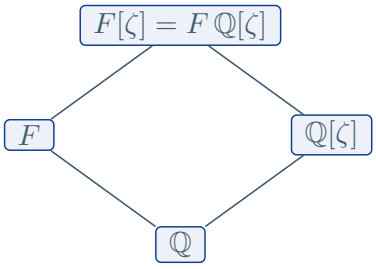



FIGURE 20

where $\zeta$ is a primitive root of $X^n - 1$. Since $F[\zeta]$ is the composite of $F$ and $\mathbb{Q}[\zeta]$, Proposition 0.146

shows that $\mathrm{Gal}(F[\zeta]/F)$ is isomorphic to a subgroup of $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$. Since $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \cong \mathbb{Z}_n^\times$ is abelian, it follows that $\mathrm{Gal}(F[\zeta]/F)$ is abelian. □

Combining Propositions 0.147 and 0.148, we obtain the following result.

**Proposition 0.149** If $F$ has characteristic 0 and $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k = K$ is a radical tower with $K$ on top, then there is a better radical tower $F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = L$ such that the following hold:

1. $K$ is a subfield of $L$.
2. $L$ is Galois over $F$, and thus Galois over each $E_j$.
3. Each $E_j$ is Galois over $E_{j-1}$.
4. Each $\mathrm{Gal}(E_j/E_{j-1})$ is abelian.

Here is one half of Galois' great theorem.

**Proposition 0.150** If $F$ has characteristic 0 and $f \in F[X]$ is solvable by radicals, then its Galois group is a solvable group.

The proof is a simple matter of putting the Galois correspondence to work in conjunction with Proposition 0.149. But first, it is a good idea to get familiar with solvable groups.

## Solvable Groups

**Definition 0.151** A group $G$ is called **solvable** provided there is a descending chain of subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \langle 1 \rangle$$

such that $G_i$ is normal in $G_{i-1}$ and $G_{i-1}/G_i$ is abelian.

The term "solvable" will be justified after we prove Galois' theorem. There is an abundant theory of solvable groups out there.

**Example 0.152** $S_3$ is solvable because

$$S_3 \supset A_3 \supset \langle 1 \rangle$$

and $S_3/A_3$ is cyclic of order 2, and $A_3/\langle 1 \rangle = A_3$ is abelian.

**Example 0.153** Every abelian group is solvable.

**Example 0.154** $S_4$ is solvable. Indeed, let $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. We have the chain

$$S_4 \supset A_4 \supset V \supset \langle \mathrm{id} \rangle$$

where $A_4$ is normal in $S_4$ because it has index 2, and $V$ is normal in $A_4$. Actually, $V$ is normal in $S_4$. This is because any conjugate of a $\sigma$ in $S_n$ has the same cycle structure as $\sigma$. Moreover, $V$ consists of id plus all products of pairs of disjoint transpositions.

The quotients are abelian: $S_4/A_4$ has order $24/12 = 2$, $A_4/V$ has order $12/4 = 3$, and $V/\langle \mathrm{id} \rangle = V$ is abelian of order 4. Actually, $V$ is the Klein 4-group. ("$V$" is German for "*vier*", meaning "four".)

**Example 0.155** If $p$ is prime and $G$ has order $p^n$ (that is, $G$ is a $p$-group), then $G$ is solvable. We have no time for a proof.

**Example 0.156** Every group of odd order is solvable. This is the famous (and hard) **Feit–Thompson theorem**.

**Example 0.157** $A_5$ is not solvable. In fact, $A_5$, of order 60, is the smallest group which is not solvable. Indeed, we know (hopefully) that $A_5$ is simple; that is, $A_5$ has no normal subgroups except $\langle 1 \rangle$ and $A_5$. If we had a chain

$$A_5 \supset G_1 \supset G_2 \supset \cdots \supset \langle 1 \rangle$$

where $G_{j+1}$ was normal in $G_j$ with abelian quotients, then $G_1$ would have to be normal in $A_5$. So $G_1$ would be $\langle 1 \rangle$. But $A_5/\langle 1 \rangle \cong A_5$ is not abelian.

We will need two useful facts about solvable groups.

**Proposition 0.158** Every subgroup and every homomorphic image of a solvable group is solvable.

**Proof.** Let $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \langle 1 \rangle$ be such that $G_{j+1}$ is normal in $G_j$ and $G_j/G_{j+1}$ is abelian. Let $H$ be a subgroup of $G$. This gives the descending chain

$$H = G_0 \cap H \supseteq G_1 \cap H \supseteq G_2 \cap H \supseteq \cdots \supseteq G_n \cap H = \langle 1 \rangle$$

We need to check that $G_{j+1} \cap H$ is normal in $G_j \cap H$ and that $(G_j \cap H)/(G_{j+1} \cap H)$ is abelian. If $x \in G_{j+1} \cap H$ and $y \in G_j \cap H$, then $yxy^{-1} \in H$ obviously, and $yxy^{-1} \in G_{j+1}$ because $G_{j+1}$ is normal in $G_j$. Now we check that $(G_j \cap H)/(G_{j+1} \cap H)$ is abelian. Take the homomorphism

$$\begin{aligned} \varphi : G_j \cap H &\longrightarrow G_j/G_{j+1} \\ x &\longmapsto xG_{j+1}. \end{aligned}$$

Note that $x \in \ker \varphi$ if and only if $x \in G_{j+1}$ and $x \in H$, if and only if $x \in G_{j+1} \cap H$. Thus $\ker \varphi = G_{j+1} \cap H$. By the first isomorphism theorem for groups we get an embedding

$$\bar{\varphi} : (G_j \cap H)/(G_{j+1} \cap H) \longrightarrow G_j/G_{j+1}.$$

Thus $(G_j \cap H)/(G_{j+1} \cap H)$, being isomorphic to a subgroup of $G_j/G_{j+1}$, is abelian. In case any of the inclusions in the chain degenerate to an equality we can just drop one of the repeated groups. Thus subgroups of solvable groups are solvable. Next suppose $\varphi : G \to H$ is a surjective homomorphism. Apply $\varphi$ to the chain $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \langle 1 \rangle$ and get

$$H = \varphi(G) = \varphi(G_0) \supseteq \varphi(G_1) \supseteq \varphi(G_2) \supseteq \cdots \supseteq \varphi(G_n) = \varphi(\langle 1 \rangle) = \langle 1 \rangle.$$

Now we need $\varphi(G_{j+1})$ to be normal in $\varphi(G_j)$ and $\varphi(G_j)/\varphi(G_{j+1})$ to be abelian. Take $x \in G_{j+1}$ and $y \in G_j$. Then

$$\varphi(y)\varphi(x)\varphi(y)^{-1} = \varphi(yxy^{-1}).$$

Since $G_{j+1}$ is normal in $G_j$, we get that $yxy^{-1} \in G_{j+1}$. Thus $\varphi(y)\varphi(x)\varphi(y)^{-1} \in \varphi(G_{j+1})$, meaning that the latter is normal in $\varphi(G_j)$. To see that $\varphi(G_j)/\varphi(G_{j+1})$ is abelian, look at the group homomorphism

$$\begin{aligned} \psi : G_j &\longrightarrow \varphi(G_j)/\varphi(G_{j+1}) \\ x &\longmapsto \varphi(x)\varphi(G_{j+1}) \end{aligned}$$

which is clearly surjective. By the first isomorphism theorem, there is the isomorphism

$$\bar{\psi} : G_j/\ker\psi \xrightarrow{\cong} \varphi(G_j)/\varphi(G_{j+1})$$

given by $x\ker\psi \longmapsto \varphi(x)\varphi(G_{j+1})$. But $x \in G_{j+1} \implies \varphi(x) \in \varphi(G_{j+1}) \implies \varphi(x)\varphi(G_{j+1})$ is the identity in $\varphi(G_j)/\varphi(G_{j+1}) \implies x \in \ker\psi$. So $G_{j+1} \subseteq \ker\psi$. This ensures that the map

$$\begin{aligned} \theta : G_j/G_{j+1} &\longrightarrow G_j/\ker\psi \\ xG_{j+1} &\longmapsto x\ker\psi \end{aligned}$$

is well-defined, and surjective, and a homomorphism. Thus $\bar{\psi}\circ\theta : G_j/G_{j+1} \longrightarrow \varphi(G_j)/\varphi(G_{j+1})$ is a surjective group homomorphism. Since $G_j/G_{j+1}$ is abelian, so is its image $\varphi(G_j)/\varphi(G_{j+1})$. Thus $H$ is solvable. □

**Example 0.159** We know $A_5$ is not solvable. Thus its containing group $S_5$ is also not solvable.

We now turn to the proof of Proposition 0.150.

**Proof of Proposition 0.150.** We have that $f \in F[x]$ is solvable by radicals. This means there is a radical tower

$$F = E_0 \subset E_1 \subset \cdots \subset E_n = L$$

such that $L$ contains the splitting field $K$ of $f$. By Proposition 0.149, we may choose the tower so that $L$ is Galois over $F$, each $E_j$ is Galois over $E_{j-1}$, and $\mathrm{Gal}(E_j/E_{j-1})$ is abelian. If any inclusion in the tower was an equality, we can drop redundant fields and get all inclusions to be proper. Apply the Galois correspondence to this tower to get a descending chain of groups:

$$\mathrm{Gal}(L/F) = \mathrm{Gal}(L/E_0) \supseteq \mathrm{Gal}(L/E_1) \supseteq \mathrm{Gal}(L/E_2) \supseteq \cdots \supseteq \mathrm{Gal}(L/E_n) = \mathrm{Gal}(L/L) = \langle \mathrm{id} \rangle.$$

The relevant portion of the radical tower is shown in Figure 21.

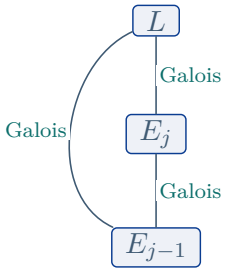


FIGURE 21

The Galois correspondence tells us that $\mathrm{Gal}(L/E_j)$ is a normal subgroup of $\mathrm{Gal}(L/E_{j-1})$ and

$$\mathrm{Gal}(L/E_{j-1})/\mathrm{Gal}(L/E_j) \cong \mathrm{Gal}(E_j/E_{j-1})$$

which is an abelian group. We just learned that $\mathrm{Gal}(L/F)$ is a solvable group. But we wanted $\mathrm{Gal}(K/F)$ to be solvable, where $K$ is the splitting field of $f$ also. The short tower in Figure 22 handles this last step.

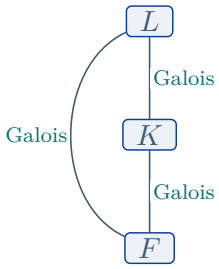



FIGURE 22

we have $\mathrm{Gal}(L/K)$ normal in $\mathrm{Gal}(L/F)$ and

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(L/F)/\mathrm{Gal}(L/K).$$

Thus $\mathrm{Gal}(K/F)$ is a homomorphic image of the solvable group $\mathrm{Gal}(L/F)$. By Proposition 0.158, $\mathrm{Gal}(K/F)$ is solvable. □

By now it should be clear how solvable groups got their name. According to this half of Galois' great theorem (Proposition 0.150), any polynomial $f$ whose Galois group is not a solvable group will never be solvable by radicals. For instance, if we get some $f$ in $\mathbb{Q}[x]$ with splitting field $K$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong S_5$, such an $f$ will not be solvable by radicals.

So let's get such an $f$.

**Proposition 0.160** Let $f \in \mathbb{Q}[x]$ be irreducible of prime degree $p$ and with splitting field $K$ inside $\mathbb{C}$. If all but two of the roots of $f$ are real numbers, then $\mathrm{Gal}(K/\mathbb{Q}) \cong S_p$.

**Proof.** We know that, for an irreducible polynomial, its degree divides the degree of its splitting field. Let $\alpha$ be a root of $f$ inside $K$. Since $f$ is irreducible, the minimal polynomial of $\alpha$ is $f$. Looking at the tower $\mathbb{Q} \subseteq \mathbb{Q}[\alpha] \subseteq K$, we see that $\deg f = [\mathbb{Q}[\alpha] : \mathbb{Q}]$ divides $[K : \mathbb{Q}]$. Thus $p \mid [K : \mathbb{Q}]$, and since $K$ is a Galois extension we have $[K : \mathbb{Q}] = |\mathrm{Gal}(K/\mathbb{Q})|$. So $p$ divides the order of $\mathrm{Gal}(K/\mathbb{Q})$. By Cauchy's theorem, $\mathrm{Gal}(K/\mathbb{Q})$ has an element $\sigma$ of order $p$. If $\Delta$ is the set of roots of $f$ in $K$, we have the restriction map

$$\begin{aligned} \pi : \mathrm{Gal}(K/\mathbb{Q}) &\longrightarrow S(\Delta) \\ \tau &\longmapsto \tau|_\Delta \end{aligned}$$

This group homomorphism is injective because $\tau|_\Delta = \mathrm{id}$ on $\Delta$ forces $\tau = \mathrm{id}$ on $K = \mathbb{Q}[\Delta]$. Identify $\mathrm{Gal}(K/\mathbb{Q})$ with its image $G$ under $\pi$. So $\mathrm{Gal}(K/\mathbb{Q}) = G$ is a subgroup of $S(\Delta)$, and $S(\Delta) = S_p$, the group of permutations on the set of roots $\Delta$, which has $p$ roots exactly. As noted, $G$ has an element $\sigma$ of order $p$. The conjugation map

$$\begin{aligned} \theta : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto \overline{z} \end{aligned}$$

restricts to an automorphism of $K$, because of the normality theorem. Thus $\theta$ permutes the set $\Delta$ of roots of $f$. But $\Delta$ has precisely two nonreal roots. If $a+ib$ with $b \neq 0$ is one of these nonreal roots then $\theta(a+ib) = a - ib \neq a + ib$ and $a - ib \notin \mathbb{R}$. So $\theta(a+ib)$ is the other nonreal root. This means that $\theta|_\Delta$ transposes two of the roots in $\Delta$ and fixes the other real roots in $\Delta$. So $G$ is a subgroup of $S(\Delta) = S_p$ containing both an element of order $p$, which has to be a $p$-cycle, and a transposition, that is, a 2-cycle. Because $p$ is prime, a $p$-cycle together with any transposition generates $S_p$. Thus our $G = S(\Delta)$. □

**Example 0.161** Here is an irreducible polynomial of degree 5 in $\mathbb{Q}[x]$ whose Galois group is $S_5$, so this polynomial cannot be solved by radicals.

According to Proposition 0.160, an irreducible polynomial of degree 5 with the root pattern in Figure 23 will do the job:

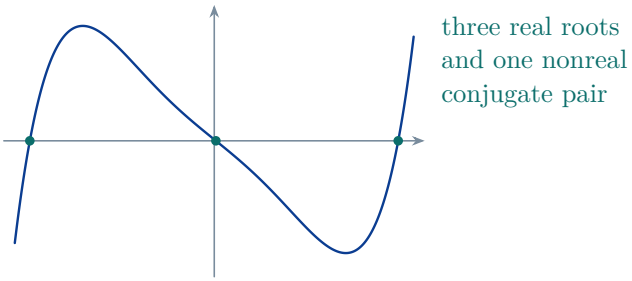



FIGURE 23

How about $f(x) = x^5 - 10x^3 - 135x + 5$?

By Eisenstein's criterion, $f$ is irreducible. Then

$$f'(x) = 5x^4 - 30x^2 - 135 = 5(x^4 - 6x^2 - 27) = 5(x^2 - 9)(x^2 + 3),$$

which reveals that $f$ increases from $-\infty$ to $-3$, decreases from $-3$ to 3, and increases from 3 to $+\infty$. Also,

$$f(-3) = (-3)^5 - 10(-3)^3 - 135(-3) + 5 = -243 + 270 + 405 + 5 > 0$$

while

$$f(3) = 3^5 - 10(3)^3 - 135(3) + 5 = 243 - 270 - 405 + 5 < 0.$$

The monotonicity and these two values show that $f$ has exactly three real roots, leaving one nonreal conjugate pair. Thus Proposition 0.160 gives the Galois group $S_5$, and $f$ is not solvable by radicals. Of course, $f$ was engineered to have a desirable derivative. The $+5$ was thrown in for Eisenstein.

## The General Polynomial of Degree $n$

Recall the field $K = L(t_1, \ldots, t_n)$ of rational functions in the variables $t_1, \ldots, t_n$. This is a Galois extension of $F = L(s_1, \ldots, s_n)$ where the $s_j$ are the elementary symmetric functions, which generate all symmetric functions. The extension $K$ over $F$ is Galois and $S_n$ is its Galois group.

Here $S_n$ acts on $K$ by permuting the $t_j$. The field $K$ is the splitting field of

$$f = (X - t_1)(X - t_2)\cdots(X - t_n) = X^n - s_1X^{n-1} + s_2X^{n-2} - \cdots + (-1)^n s_n \in F[X].$$

This $f$ is called the **general polynomial of degree $n$**. Why the name? Well, suppose $h = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ is any polynomial in $L[X]$.

After we factor $h$ in some splitting field, we get

$$h = (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n).$$

Then we get $h$ from $f$ by substituting $t_j = \alpha_j$, and then $s_j(t_1, \ldots, t_n)$ becomes $s_j(\alpha_1, \ldots, \alpha_n) = \pm a_j$.

Anyhow, since $n \geq 5$ implies that $S_n$ is not a solvable group, we see that the general polynomial is not solvable by radicals. This is known as **Abel's theorem**. There is no way to write the $t_j$ in terms of the $s_i$ using the operations of $+$, $-$, $\cdot$, $\div$, and $\sqrt[k]{\ }$ for various $k$, unlike the case $n = 2$, where

$$t_1 = \frac{s_1 + \sqrt{s_1^2 - 4s_2}}{2} \qquad \text{and} \qquad t_2 = \frac{s_1 - \sqrt{s_1^2 - 4s_2}}{2}.$$

The second half of Galois' great theorem is the converse of the first half. Of course, it will exploit the Galois correspondence! But first we need a few more results about both solvable groups and cyclic field extensions.

**Proposition 0.162** If $A$ is a finite abelian group, then there is a descending chain of subgroups

$$A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n = \langle 1 \rangle$$

such that $A_{i-1}/A_i$ has prime order and is thereby cyclic.

**Proof.** Let $A_1$ be a maximal proper subgroup of $A$. Then $A/A_1$ has prime order. For if not, there would be a subgroup $C$ of $A/A_1$ such that $\langle 1 \rangle \subsetneq C \subsetneq A/A_1$. The inverse image in $A$, under the usual projection $A \to A/A_1$, would then be a subgroup of $A$ properly between $A_1$ and $A$, contrary to the maximality of $A_1$. By induction, we then pick up a descending chain

$$A_1 \supset A_2 \supset A_3 \supset \cdots \supset \langle 1 \rangle$$

such that $A_{i-1}/A_i$ has prime order. This, together with the inclusion $A \supset A_1$, gives the desired descending chain starting at $A$. □

**Proposition 0.163** If $H$ is a normal subgroup of a finite group $G$ and $G/H$ is abelian,

then there is a descending chain of subgroups

$$G \supset G_1 \supset \cdots \supset G_n = H$$

such that $G_i$ is normal in $G_{i-1}$ and $G_{i-1}/G_i$ has prime order and is thereby cyclic.

**Proof.** Inside the finite abelian group $G/H$, pick a descending chain of subgroups

$$G/H = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n = \langle 1 \rangle = H/H.$$

such that each $A_{i-1}/A_i$ has prime order. Let $\varphi : G \to G/H$ be the usual projection. With $G_i = \varphi^{-1}(A_i)$, we get the descending chain

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = H.$$

Now we need to check that $G_i$ is normal in $G_{i-1}$ and $G_{i-1}/G_i \cong A_{i-1}/A_i$, which we know have prime order. The last isomorphism follows from the third isomorphism theorem, but here is the proof of the isomorphism directly. Since $\varphi$ is onto $G/H$ we get that

$$\varphi(G_i) = \varphi(\varphi^{-1}(A_i)) = A_i \text{ for all } i.$$

So we get the surjective homomorphism

$$\begin{aligned} \bar{\varphi} : G_{i-1} &\longrightarrow A_{i-1}/A_i \\ x &\mapsto \varphi(x)A_i. \end{aligned}$$

The element $x$ lies in $\ker \bar{\varphi}$ if and only if $\varphi(x) \in A_i$, if and only if $x \in \varphi^{-1}(A_i) = G_i$. That is, $\ker \bar{\varphi} = G_i$. By the first isomorphism theorem,

$$G_{i-1}/G_i \cong A_{i-1}/A_i, \text{ as desired.}$$

Note the above argument also showed that $G_i$ was normal in $G_{i-1}$, because $G_i = \ker \bar{\varphi}$ and all kernels are normal. □

**Proposition 0.164** If $G$ is a finite solvable group, then there is a descending chain

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_k = \langle 1 \rangle$$

such that each $H_i$ is normal in $H_{i-1}$ and $H_{i-1}/H_i$ has prime order and is thereby cyclic.

**Proof.** We do have a chain

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \langle 1 \rangle$$

such that each $G_i$ is normal in $G_{i-1}$, and $G_{i-1}/G_i$ is abelian. Now apply Proposition 0.163 to each normal subgroup $G_i$ inside $G_{i-1}$ to pick up the desired refinement of the given chain. □

## Independence of Characters

We now turn to a couple of key (but hard) results in field theory.

**Definition 0.165** If $G$ is any group and $E$ is any field, a **character** is a group homomorphism $\varphi : G \to E^*$, where $E^*$ is the group of units of $E$ under multiplication.

As an aside, if $G$ is finite, then every $x$ in $G$ satisfies $x^n = 1$ for some $n$. Therefore

$$\varphi(x)^n = \varphi(x^n) = \varphi(1) = 1$$

in $E$, so $\varphi(G)$ is a subgroup of the group of all roots of unity in $E$. For our purposes, however, $G$ will be $L^*$ for some infinite field $L$.

Given a list of characters $\varphi_1, \ldots, \varphi_n : G \to E^*$ and some scalars $a_1, \ldots, a_n$ in $E$, we can form an $E$-linear combination as a function $G \to E$:

$$\begin{aligned} \sum_j a_j \varphi_j : G &\longrightarrow E \\ u &\longmapsto \sum_j a_j \varphi_j(u). \end{aligned}$$

**Proposition 0.166** If $\varphi_1, \ldots, \varphi_n : G \to E^*$ is any number of distinct characters on $G$ and $a_j$ in $E$ are such that $\sum_j a_j \varphi_j = 0$ (the zero function on $G$), then all $a_j = 0$.

**Proof.** Suppose to the contrary that a nonzero combination of the $\varphi_j$ makes the zero function

on $G$. Take such a nonzero combination of minimal length. Thus we have

$$a_1\varphi_1 + a_2\varphi_2 + \cdots + a_n\varphi_n = 0. \tag{0.14}$$

Since $n$ is as small as possible to satisfy (0.14), all $a_j \neq 0$ in $E$. If $n = 1$, we have $a_1\varphi_1(u) = 0$ for all $u \in G$. So $a_1 = a_1 \cdot 1 = a_1\varphi_1(1) = 0$, which is false. (Here "1" has 3 different interpretations, but there should not be any confusion.) So $n \geq 2$. Next pick $v \in G$ such that $\varphi_1(v) \neq \varphi_2(v)$. For all $u \in G$ we have

$$a_1\varphi_1(vu) + a_2\varphi_2(vu) + \cdots + a_n\varphi_n(vu) = 0,$$

which, by the nature of characters, becomes

$$a_1\varphi_1(v)\varphi_1(u) + a_2\varphi_2(v)\varphi_2(u) + \cdots + a_n\varphi_n(v)\varphi_n(u) = 0, \quad \text{for all } u \in G. \tag{0.15}$$

Multiply (0.14) by $\varphi_1(v)$ to get

$$a_1\varphi_1(v)\varphi_1(u) + a_2\varphi_1(v)\varphi_2(u) + \cdots + a_n\varphi_1(v)\varphi_n(u) = 0, \quad \text{for all } u \in G.$$

Subtract this from (0.15) to get

$$a_2(\varphi_2(v) - \varphi_1(v))\varphi_2(u) + \cdots + a_n(\varphi_n(v) - \varphi_1(v))\varphi_n(u) = 0, \quad \text{for all } u \in G.$$

Since $\varphi_2(v) - \varphi_1(v) \neq 0$, this is a nonzero dependency relation among the $\varphi_j$ which is shorter than the shortest possible one. We conclude that the characters are linearly independent over $E$. □

Next comes a strange result, known as **Hilbert's Theorem 90**. The connection to Galois' theorem will fall into place later.

**Definition 0.167** If $K$ is a Galois extension of $F$ and $v \in K$, the **norm** of $v$ is defined as

$$N(v) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(v) \in K.$$

For any $\tau \in \mathrm{Gal}(K/F)$ we have

$$N(v) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \tau\sigma(v) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma\tau(v).$$

These equations are true because, as $\sigma$ runs over $\mathrm{Gal}(K/F)$, so do $\tau\sigma$ and $\sigma\tau$.

The first equation, along with the fact $\tau$ is an automorphism, reveals that $\tau(N(v)) = N(v)$. Thus

$$N(v) \in \text{Fix}(\text{Gal}(K/F)) = F.$$

The second equation reveals that $N(\tau(v)) = N(v)$ for all $\tau \in \text{Gal}(K/F)$. Multiplying the factors in the definition gives $N(uv) = N(u)N(v)$ and $N(u/v) = N(u)/N(v)$ for $u, v \in K$ with $v \neq 0$. Thus, for any $v \neq 0$ in $K$ and any $\tau \in \text{Gal}(K/F)$ we get

$$N\left(\frac{v}{\tau(v)}\right) = \frac{N(v)}{N(\tau(v))} = \frac{N(v)}{N(v)} = 1.$$

Hilbert's Theorem 90 tells us that if $\text{Gal}(K/F)$ is cyclic, then all elements in $K$ of norm 1 take the above form. The theorem uses the independence of characters.

**Proposition 0.168 (Hilbert's Theorem 90)** Suppose $K$ is Galois over $F$ with cyclic Galois group generated by $\tau$. If $v \in K$ and $N(v) = 1$, then $v = w/(\tau(w))$ for some $w \in K$.

**Proof.** Let $n = |\text{Gal}(K/F)|$. Thus $\text{id}, \tau, \tau^2, \ldots, \tau^{n-1}$ give the full Galois group. These are also characters from the group $K^*$ to $K^*$, so they are $K$-linearly independent. So the $K$-linear combination

$$\text{id} + v\tau + v\tau(v)\tau^2 + v\tau(v)\tau^2(v)\tau^3 + \cdots + v\tau(v)\tau^2(v)\ldots\tau^{n-2}(v)\tau^{n-1} \neq 0 \tag{0.16}$$

as a function $K^* \to K$. Pick $u \in K^*$ such that

$$u + v\tau(u) + v\tau(v)\tau^2(u) + v\tau(v)\tau^2(v)\tau^3(u) + \cdots + v\tau(v)\tau^2(v)\ldots\tau^{n-2}(v)\tau^{n-1}(u) \neq 0 \tag{0.17}$$

and call this element $w$. We want $v = w/(\tau(w))$. So calculate

$$\begin{aligned}\tau(w) &= \tau(u) + \tau(v)\tau^2(u) + \tau(v)\tau^2(v)\tau^3(u) + \cdots + \tau(v)\tau^2(v)\ldots\tau^{n-1}(v)\tau^n(u) \\ &= \tau(u) + \tau(v)\tau^2(u) + \tau(v)\tau^2(v)\tau^3(u) + \cdots + \underbrace{\tau(v)\tau^2(v)\ldots\tau^{n-1}(v)}_{=N(v)=1}\underbrace{\tau^n(u)}_{=u}\end{aligned}$$

Multiplying by $v$, we get

$$v\tau(w) = v\tau(u) + v\tau(v)\tau^2(u) + v\tau(v)\tau^2(v)\tau^3(u) + \cdots + v\tau(v)\tau^2(v)\ldots\tau^{n-1}(v)u.$$

The expression for $v\tau(w)$ is exactly the sum in (0.17), because the first term $u$ is shifted to the end and appears there as $N(v)u = u$. Hence $v\tau(w) = w$, so $v = w/(\tau(w))$. □

Hilbert's Theorem 90 has a way of appearing in algebra and number theory. For us it appears in the following corollary of Proposition 0.143.

**Proposition 0.169** Suppose $F$ has characteristic 0, $X^d - 1$ splits in $F[X]$, and $K$ is a Galois extension of $F$ for which the Galois group $\mathrm{Gal}(K/F)$ is cyclic of order $d$. Then there is an $\alpha \in K$ such that $K = F[\alpha]$, $\alpha^d \in F$, and $X^d - \alpha^d$ is the minimal polynomial of $\alpha$ over $F$. Thus the tower $F \subseteq K = F[\alpha]$ is radical.

**Proof.** Let $\omega$ be a primitive $d$th root of unity in $F$. Thus $1, \omega, \omega^2, \ldots, \omega^{d-1}$ are distinct in $F$. Since $1/\omega \in F$, we have

$$N\left(\frac{1}{\omega}\right) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma\left(\frac{1}{\omega}\right) = \left(\frac{1}{\omega}\right)^d = 1.$$

If $\tau$ generates $\mathrm{Gal}(K/F)$, Hilbert's Theorem 90 provides an $\alpha \in K$ such that

$$\frac{1}{\omega} = \frac{\alpha}{\tau(\alpha)}, \text{ and thus } \tau(\alpha) = \alpha\omega.$$

Then

$$\begin{aligned}
\tau^2(\alpha) &= \tau(\alpha\omega) \\
&= \tau(\alpha)\tau(\omega) \\
&= \alpha\omega^2 \quad (\text{since } \omega \in F \implies \tau(\omega) = \omega) \\
\tau^3(\alpha) &= \alpha\omega^3 \\
&\vdots \\
\tau^{d-1}(\alpha) &= \alpha\omega^{d-1} \\
\tau^d(\alpha) &= \alpha\omega^d = \alpha.
\end{aligned}$$

If $g$ is the minimal polynomial of $\alpha$, the $\tau^j(\alpha) = \alpha\omega^j$ must be roots of $g$, and for $j = 0, \ldots, d-1$, they are distinct. Hence, $[F[\alpha] : F] = \deg g \geq d = |\mathrm{Gal}(K/F)| = [K : F]$. But $F[\alpha] \subseteq K$. Together from the preceding inequality it follows that $\deg g = d$ and $K = F[\alpha]$. In addition,

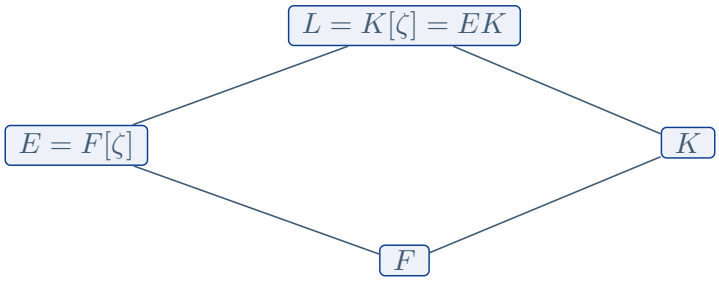
$$\tau(\alpha^d) = \tau(\alpha)^d = (\alpha\omega)^d = \alpha^d\omega^d = \alpha^d,$$

which shows that $\alpha^d \in \mathrm{Fix}(\mathrm{Gal}(K/F)) = F$. So $X^d - \alpha^d \in F[X]$. Since $\alpha$ is a root of $X^d - \alpha^d$ and $g$ is the minimal polynomial of $\alpha$ we see that $g \mid X^d - \alpha^d$ in $F[X]$. Then the fact $\deg g = d$ forces $g = X^d - \alpha^d$. All the details are done. □

This finally brings us to the second half of Galois' great theorem, and to the end of our course.

**Proposition 0.170** If $F$ has characteristic 0, $f \in F[X]$ has splitting field $K$, and $\mathrm{Gal}(K/F)$ is a solvable group, then $f$ is solvable by radicals.

**Proof.** Let $n = [K : F] = |\mathrm{Gal}(K/F)|$. Then let $L$ be the splitting field of $X^n - 1$ over $K$. If $\zeta$ is a primitive $n$th root of unity, we see that $L = K[\zeta]$, and with $E = F[\zeta]$ we have the following inclusions:



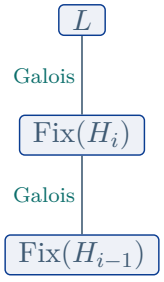

Clearly $K[\zeta]$ is the composite of $E$ and $K$. By Proposition 0.146, $L$ is Galois over $E$ and $\mathrm{Gal}(L/E)$ is isomorphic to a subgroup of $\mathrm{Gal}(K/F)$. Since the latter group is solvable, so is $\mathrm{Gal}(L/E)$. According to Proposition 0.163 there is a descending chain of subgroups

$$\mathrm{Gal}(L/E) = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_k = \langle 1 \rangle$$

such that $H_i$ is normal in $H_{i-1}$ and $H_{i-1}/H_i$ is cyclic. Apply the Galois correspondence to the Galois extension $L$ over $E$ to get a tower

$$E = \mathrm{Fix}(\mathrm{Gal}(L/E)) = \mathrm{Fix}(H_0) \subset \mathrm{Fix}(H_1) \subset \mathrm{Fix}(H_2) \subset \cdots \subset \mathrm{Fix}(H_k) = \mathrm{Fix}\langle 1 \rangle = L.$$

This is a radical tower. Why? Well for each $i$ we have the following situation:



The reason $L$ is a Galois extension of $\mathrm{Fix}(H_i)$ and of $\mathrm{Fix}(H_{i-1})$ is that $L$ is Galois over $E$ down at the bottom. Now look back at Proposition 0.115, with "$K = L$", "$F = \mathrm{Fix}(H_{i-1})$", and "$E = \mathrm{Fix}(H_i)$". Proposition 0.115 tells us that $\mathrm{Fix}(H_i)$ is Galois over $\mathrm{Fix}(H_{i-1})$ if and only if $\mathrm{Gal}(L/\mathrm{Fix}(H_i))$ is a normal subgroup of $\mathrm{Gal}(L/\mathrm{Fix}(H_{i-1}))$. But the Galois correspondence tells us that $H_i = \mathrm{Gal}(L/\mathrm{Fix}(H_i))$ and $H_{i-1} = \mathrm{Gal}(L/\mathrm{Fix}(H_{i-1}))$, and we are given that $H_i$ is normal in $H_{i-1}$. Hence $\mathrm{Fix}(H_i)$ is Galois over $\mathrm{Fix}(H_{i-1})$. In addition, Proposition 0.115 tells us that

$$\mathrm{Gal}(\mathrm{Fix}(H_i)/\mathrm{Fix}(H_{i-1})) \cong H_{i-1}/H_i,$$

which is given to be cyclic. To summarize, $\mathrm{Fix}(H_i)$ is a Galois extension of $\mathrm{Fix}(H_{i-1})$ with cyclic Galois group. In order to get that the tower

$$\mathrm{Fix}(H_{i-1}) \subset \mathrm{Fix}(H_i)$$

is radical, all we need to do is make sure Proposition 0.169 applies. The order of the Galois group of the above extension is the order of $H_{i-1}/H_i$, call it $d$. Clearly $d$ divides $|H_{i-1}|$. Also, $|H_{i-1}|$ divides $|\mathrm{Gal}(L/E)|$ because $H_{i-1}$ is a subgroup of $\mathrm{Gal}(L/E)$. But Proposition 0.146 tells us that $\mathrm{Gal}(L/E)$ is isomorphic to a subgroup of the original $\mathrm{Gal}(K/F)$, whose order was $n$. So the order $d$ of the Galois group of $\mathrm{Fix}(H_i)$ over $\mathrm{Fix}(H_{i-1})$ divides $n$. But these fields all contain $E = F[\zeta]$ and $X^n - 1$ splits over $E$. Since $d \mid n$, so does $X^d - 1$ split over $E$, and thus $X^d - 1$ splits over $\mathrm{Fix}(H_{i-1})$.

Proposition 0.169 applies to give an $\alpha_i$ in $\mathrm{Fix}(H_i)$ and an integer $n_i \geq 1$ (actually $\geq 2$) such that $\mathrm{Fix}(H_i) = \mathrm{Fix}(H_{i-1})[\alpha_i]$ and $\alpha_i^{n_i} \in \mathrm{Fix}(H_{i-1})$.

Our tower is radical! The original splitting field $K \subseteq L$. But for solvability of $f$ by radicals, the radical tower needed to start with $F$, while the tower started with $E$. At the bottom of the tower, include $F \subseteq E = F[\zeta]$ and note that $\zeta^n = 1 \in F$. So the full tower

$$F \subseteq E \subset \mathrm{Fix}(H_1) \subset \mathrm{Fix}(H_2) \subset \cdots \subset L$$

is radical and contains the splitting field $K$, and thereby the roots of $f$. □

Combining Propositions 0.150 and 0.170, we have Galois' great theorem, in all its glory:

**Theorem 0.171 (Galois' great theorem)** Suppose $f \in F[X]$ has splitting field $K$, where $F$ has characteristic 0. Then $f$ is solvable by radicals if and only if $\mathrm{Gal}(K/F)$ is a solvable group.