Shandong University | Advanced Modern Algebra

Lecture 10 & 11: Galois Theory

Apr. 28, 2023

Lecturer: Bin Guan

This lecture refers to Chapter 14 in [1]. All the equation numbers without reference labels are from this book.

1 The Fundamental Theorem of Galois Theory

Let K/F be an extension of fields. Let $\mathrm{Aut}(K/F)$ be the collection of automorphisms of K which fix F. An extension E/F is called **Galois** if it is algebraic, normal and separable. In this case $\mathrm{Aut}(E/F)$ is called the **Galois group** of the extension and is denoted by $\mathrm{Gal}(E/F)$.

Recall that we already have

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}, \quad \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}, \quad \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$$

where $\omega = \zeta_3 = \frac{1}{2}(-1 + \sqrt{-3})$. We also have the following properties (cf. [1] §14.1 Propositions 1, 3, 4): for any field extension K/F,

- $\mathrm{Aut}(K/F)$ is a group under composition.
- For any $H \leq \mathrm{Aut}(K/F)$, $\mathrm{Inv}(H) \coloneqq \{\alpha \in K \mid \sigma\alpha = \alpha \text{ for any } \sigma \in H\}$ is a subfield of K containing F, called the **fixed field** of H.

The association of groups to fields and fields to groups defined above is inclusion reversing, namely

- if $F_1 \subseteq F_2 \subseteq K$ are two subfields of K then $\mathrm{Aut}(K/F_1) \geq \mathrm{Aut}(K/F_2)$; and
- if $H_1 \leq H_2 \leq \mathrm{Aut}(K)$ are two subgroups of automorphisms, then $\mathrm{Inv}(H_1) \supseteq \mathrm{Inv}(H_2)$.

Given a subfield F of K, the associated group is the collection of automorphisms of K which fix F. Given a group of automorphisms of K, the associated extension is defined by taking F to be the fixed field of the automorphisms.

We first state (without proof) the fundamental relation between the orders of subgroups of the automorphism group of a field K and the degrees of the extensions over their fixed fields.

Theorem ([1] §14.2 Theorem 9)**.** *Let K be a field, H be a finite subgroup of* $\mathrm{Aut}(K)$*. Then*

$$[K : \mathrm{Inv}(H)] = |H|.$$

Corollary ([1] §14.2 Corollary 10 & Theorem 13)**.** *Let K/F be any finite extension. Then*

$$|\operatorname{Aut}(K/F)| \leq [K:F].$$

Moreover, when K/F is finite, TFAE (the following are equivalent):

(1) $|\operatorname{Aut}(K/F)| = [K:F]$*;*

(2) $F = \operatorname{Inv}(\operatorname{Aut}(K/F))$*;*

(3) K is the splitting field of some separable polynomial over F (i.e., K/F is a finite Galois extension);

(4) every irreducible polynomial with coefficients in F which has a root in K is separable and has all its roots in K.

Proof. Let $G = \operatorname{Aut}(K/F)$. We have $F \subseteq \operatorname{Inv}(G) \subseteq K$, and by the above theorem,

$$[K:\operatorname{Inv}(G)] = |G|, \quad \text{and hence} \quad [K:F] = [K:\operatorname{Inv}(G)][\operatorname{Inv}(G):F] \leq |G|,$$

which proves the first part of the corollary and proves (1) $\Leftrightarrow$ (2).

(3) $\Rightarrow$ (1): §14.1 Corollary 6.

(1) $\Rightarrow$ (4) $\Rightarrow$ (3): We leave the proof as an exercise.

(3) $\Leftrightarrow$ (4): §13.4 Exercise 5. □

Corollary ([1] §14.2 Corollary 11)**.** *Let $G \leq \operatorname{Aut}(K)$ be a finite subgroup of automorphisms of a field K. Then every automorphism of K fixing $\operatorname{Inv}(G)$ is contained in G, i.e.,*

$$\operatorname{Aut}(K/\operatorname{Inv}(G)) = G,$$

so that $K/\operatorname{Inv}(G)$ is Galois, with Galois group G.

Proof. By definition $\operatorname{Inv}(G)$ is fixed by all the elements of G, so we have $G \leq \operatorname{Aut}(K/\operatorname{Inv}(G))$ (and the question is whether this containment is proper). Hence $|G| \leq |\operatorname{Aut}(K/\operatorname{Inv}(G))|$ and

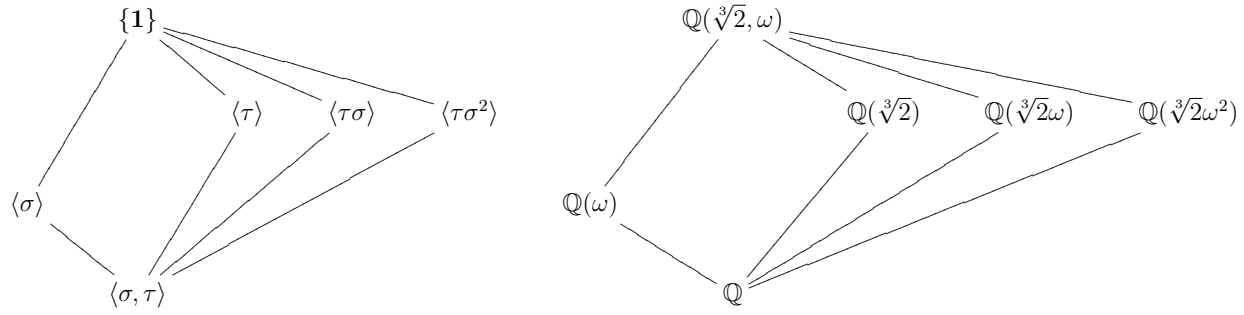
$$[K:\operatorname{Inv}(G)] \overset{\text{Theorem 9}}{=} |G| \leq |\operatorname{Aut}(K/\operatorname{Inv}(G))| \overset{\text{Corollary 10}}{\leq} [K:\operatorname{Inv}(G)],$$

and it follows that we must have equalities throughout, proving the corollary. □

Corollary ([1] §14.2 Corollary 12)**.** *If $G_1 \neq G_2$ are distinct finite subgroups of automorphisms of a field K, then their fixed fields are also distinct.*

Proof. Suppose F_1 is the fixed field of G_1 and F_2 is the fixed field of G_2. If $F_1 = F_2$ then by definition F_1 is fixed by G_2. By the previous corollary any automorphism fixing F_1 is contained in G_1, hence $G_2 \leq G_1$. Similarly $G_1 \leq G_2$ and so $G_1 = G_2$. □

By the corollaries above we see that taking the fixed fields for distinct finite subgroups of $\operatorname{Aut}(K)$ gives distinct subfields of K over which K is Galois. Further, the degrees of the extensions are given by the orders of the subgroups. Recall that we have the diagram of subgroups of $\operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ and the diagram of known subfields for the splitting field of $x^3 - 2$:



where the subfields in the second diagram are precisely the fixed fields of the subgroups in the first diagram. A portion of the Fundamental Theorem states that these are all the subfields of $\mathbb{Q}(\sqrt[3]{2}, \omega)$.

Theorem ([1] §14.2 Theorem 14, Fundamental Theorem of Galois Theory)**.** *Let K/F be a Galois extension and set $G = \mathrm{Gal}(K/F)$. Then there is a bijection*

$$\left\{ \begin{array}{c} \textit{intermediate fields of } K/F \\ \textit{i.e. subfields } E \subseteq K \\ \textit{containing } F \end{array} \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \underset{\mathrm{Inv}(\cdot)}{\overset{\mathrm{Gal}(K/\cdot)}{\rightleftarrows}} \left\{ \textit{subgroups } H \leq G \quad \begin{array}{c} \{\mathbf{1}\} \\ | \\ H \\ | \\ G = \mathrm{Gal}(K/F) \end{array} \right\}$$

given by the correspondences

$$\begin{array}{ccc} E & \longmapsto & \mathrm{Gal}(K/E) \\ \mathrm{Inv}(H) & \longmapsfrom & H \end{array}$$

which are inverse to each other. Under this correspondence,

(1) (inclusion reversing) *If E_1, E_2 correspond to H_1, H_2, respectively, then $E_1 \subseteq E_2$ if and only if $H_1 \geq H_2$.*

(2) *$[K : E] = |H|$ and $[E : F] = [G : H]$, the index of H in G:*

$$\begin{array}{lll} K & & \\ | & \} & |H| \\ E & & \\ | & \} & [G : H] \\ F & & \end{array}$$

(3) *K/E is always Galois, with Galois group $\mathrm{Gal}(K/E) = H$:*

$$\begin{array}{lll} K & & \\ | & \} & \mathrm{Gal}(K/E) = H \\ E & & \end{array}$$

(4) *E is Galois over F if and only if H is a normal subgroup in G. If this is the case, then the Galois group is isomorphic to the quotient group*

$$\mathrm{Gal}(E/F) \cong G/H.$$

*More generally, even if H is not necessarily normal in G, the isomorphisms of E (into a fixed algebraic closure of F containing K) which fix F are in one-to-one correspondence with the cosets $G/H = \{\sigma H \mid \sigma \in G\}$ of H in G. (If $\alpha \in K$, the elements $\sigma\alpha$ for $\sigma \in \mathrm{Gal}(K/F)$ are called the **conjugates**, or **Galois conjugates**, of α over F. If E is a subfield of K containing F, the field $\sigma(E)$ is called the **conjugate field** of E over F.)*

(5) *If E_1, E_2 correspond to H_1, H_2, respectively, then the intersection $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2 \rangle$ generated by H_1 and H_2, and the composite field E_1E_2 corresponds to the intersection $H_1 \cap H_2$. Hence the diagram of subfields of K containing F and the diagram of subgroups of G are "similar" (the diagram for one is the diagram for the other).*

Exercise. *If E is a intermediate fields of a Galois extension K/F, what is the relation between $\mathrm{Gal}(K/E)$ and $\mathrm{Gal}(K/\sigma(E))$ for $\sigma \in \mathrm{Gal}(K/F)$?*

Example. *Recall that the Galois group for the splitting field $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ of $x^3 - 2$ over $\mathbb{Q}$ is*

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = \mathbf{1},\ \sigma\tau = \tau\sigma^2 \rangle \cong S_3$$

where $\omega = \zeta_3 = \frac{1}{2}(-1 + \sqrt{-3})$.

Note that the subgroup $\langle \sigma \rangle$ generated by σ is the only proper normal subgroup in S_3, and that $\mathbb{Q}(\omega) = \mathrm{Inv}(\langle \sigma \rangle)$ is the only proper intermediate field of $K/\mathbb{Q}$ which is Galois over $\mathbb{Q}$.

The subgroup $\langle \tau \rangle$ generated by τ is not normal in S_3, and $\mathbb{Q}(\sqrt[3]{2}) = \mathrm{Inv}(\langle \tau \rangle)$ is not Galois over $\mathbb{Q}$. Moreover, $\sigma^0(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\sqrt[3]{2})$, $\sigma^1(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\sqrt[3]{2}\omega)$, $\sigma^2(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\sqrt[3]{2}\omega^2)$ are all the conjugate field of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$.

Example. *The splitting field of $x^4 - 2$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt[4]{2}, i)$ where $i = \zeta_4$ is a square root of -1 in $\mathbb{C}$. The subfield $\mathbb{Q}(\sqrt[4]{2})$ is of degree 4 over $\mathbb{Q}$ (since $x^4 - 2$ is irreducible, being Eisenstein), and all the elements of this field are real. Hence $i \notin \mathbb{Q}(\sqrt[4]{2})$ and since i generates at most a quadratic extension of this field, the splitting field is of degree 8 over $\mathbb{Q}$.*

Any $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ maps $\sqrt[4]{2}$ to one of $\sqrt[4]{2}$, $\sqrt[4]{2}i$, $-\sqrt[4]{2}$, $-\sqrt[4]{2}i$, and maps i to i or $-i$. Since φ is completely determined by its action on these two elements, this gives only 8 possibilities and each of these possibilities is actually an automorphism.

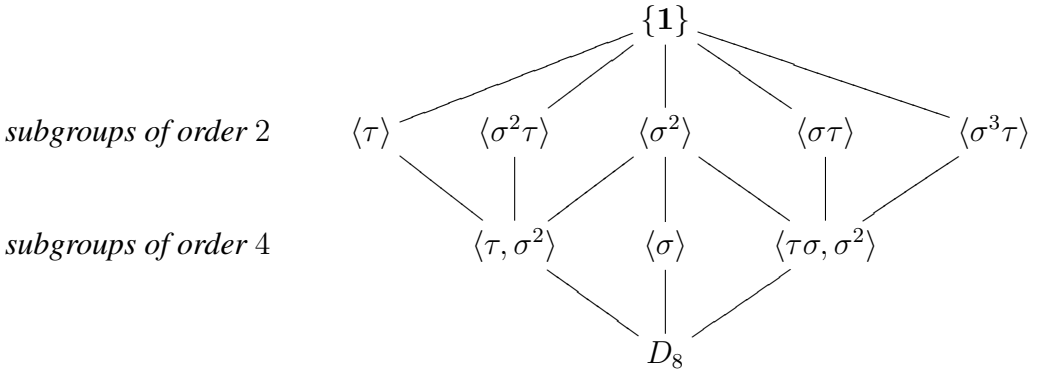
To give these automorphisms explicitly, let σ and τ be the automorphisms defined by

$$\sigma : \begin{cases} \sqrt[4]{2} & \mapsto & \sqrt[4]{2}i \\ i & \mapsto & i \end{cases} \qquad \tau : \begin{cases} \sqrt[4]{2} & \mapsto & \sqrt[4]{2} \\ i & \mapsto & -i. \end{cases}$$

One can verify that

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = \mathbf{1},\ \sigma\tau = \tau\sigma^{-1} \rangle \cong D_8.$$

All the subgroups of D_8 are shown in the following diagram (cf. [1] §2.5 Example (4)):



As an exercise, one can find all subfields of $\mathbb{Q}(\sqrt[4]{2}, i)$ by taking the fixed fields of all the subgroups, according to the Fundamental Theorem.

To study all subfields of $\mathbb{Q}(\sqrt[4]{2}, i)$ which are Galois over $\mathbb{Q}$ we need to find all the normal subgroups of D_8 (cf. [1] §3.1 Exercise 33):

$$\{\mathbf{1}\}, \quad \langle \sigma^2 \rangle, \quad \langle \tau, \sigma^2 \rangle, \quad \langle \sigma \rangle, \quad \langle \tau\sigma, \sigma^2 \rangle, \quad D_8.$$

The fixed fields of them are respectively

$$\mathbb{Q}(\sqrt[4]{2}, i), \quad \mathbb{Q}(\sqrt{2}, i), \quad \mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(i), \quad \mathbb{Q}(\sqrt{2}i), \quad \mathbb{Q};$$

and they are respectively the splitting fields over $\mathbb{Q}$ of

$$x^4 - 2, \quad (x^2 - 2)(x^2 + 1), \quad x^2 - 2, \quad x^2 + 1, \quad x^2 + 2, \quad x.$$

Exercise. *Let α be a root of $f(x) = x^6 + 3$ in an algebraic closure of $\mathbb{Q}$, and $K = \mathbb{Q}(\alpha)$. Show that $K/\mathbb{Q}$ is Galois and determine the Galois group of it. Find all the subfields E of K which are of degree 3 over $\mathbb{Q}$.*

2 Finite fields

Proposition ([1] §14.3 Proposition 15)**.** *(1) Any finite field is isomorphic to $\mathbb{F}_{p^n}$ for some prime p and some integer $n \geq 1$, where $\mathbb{F}_{p^n}$ is the splitting field over $\mathbb{F}_p$ of the polynomial $x^{p^n} - x$.*

(2) $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$, with cyclic Galois group

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$$

of order n generated by the Frobenius automorphism

$$\mathrm{Frob}_p : \mathbb{F}_{p^n} \xrightarrow{\sim} \mathbb{F}_{p^n}, \qquad \alpha \longmapsto \alpha^p.$$

(3) The subfields of $\mathbb{F}_{p^n}$ are all Galois over $\mathbb{F}_p$, and are in one-to-one correspondence with the divisors $d \mid n$. They are the fields $\mathbb{F}_{p^d}$, the fixed fields of $(\mathrm{Frob}_p)^d$.

Proof. We have shown (1) in the previous lecture (cf. [1] §13.5 p.549-550).

(2) Exercise.

(3) By the Fundamental Theorem, every subfield of $\mathbb{F}_{p^n}$ corresponds to a subgroup of $\mathbb{Z}/n\mathbb{Z}$. Hence for every divisor d of n there is precisely one subfield of $\mathbb{F}_{p^n}$ of degree d over $\mathbb{F}_p$, namely the fixed field of the subgroup generated by $(\mathrm{Frob}_p)^d$ of order n/d, and there are no other subfields. This field is isomorphic to $\mathbb{F}_{p^d}$, the unique finite field of order p^d.

Since the Galois group is abelian, every subgroup is normal, so each of the subfields $\mathbb{F}_{p^d}$ (d a divisor of n) is Galois over $\mathbb{F}_p$ (which is also clear from the fact that these are themselves splitting fields). □

The Galois group $\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p)$ is generated by the image of Frob_p in the quotient group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)/\langle(\mathrm{Frob}_p)^d\rangle$. If we denote this element again by Frob_p, we recover the Frobenius automorphism for the extension $\mathbb{F}_{p^d}/\mathbb{F}_p$. (Note, however, that Frob_p has order n in $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ and order d in $\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p)$.)

Proposition ([1] §14.3 Proposition 17)**.** *The finite field $\mathbb{F}_{p^n}$ is simple. In particular, there exists an irreducible polynomial of degree n over $\mathbb{F}_p$ for every $n \geq 1$.*

Proof. The multiplicative group $\mathbb{F}_{p^n}^\times$ is obviously a finite subgroup of the multiplicative group of a field. By [1] §9.5 Proposition 18, this is a cyclic group. If θ is any generator, then $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$. And by [1] §13.2 Proposition 11, the minimal polynomial of θ over $\mathbb{F}_p$ is an irreducible polynomial of degree n over $\mathbb{F}_p$. □

We have seen above that

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \qquad \text{if and only if} \qquad m \mid n.$$

In particular, given any two finite fields $\mathbb{F}_{p^{n_1}}$ and $\mathbb{F}_{p^{n_2}}$ there is a third finite field containing (an isomorphic copy of) them, namely $\mathbb{F}_{p^{n_1 n_2}}$. This gives us a partial ordering on these fields and allows us to think of their union. Since these give *all* the finite extensions of $\mathbb{F}_p$, we see that the union of $\mathbb{F}_{p^n}$ for all n is an algebraic closure of $\mathbb{F}_p$, unique up to isomorphism:

$$\overline{\mathbb{F}_p} \coloneqq \bigcup_{n \geq 1} \mathbb{F}_{p^n}.$$

This provides a simple description of the algebraic closure of $\mathbb{F}_p$.

3 Cyclotomic extensions and abelian extensions over $\mathbb{Q}$

We have already determined that the cyclotomic field $\mathbb{Q}(\zeta_n)$ of n^{th} roots of unity is a Galois extension of $\mathbb{Q}$ of degree $\varphi(n)$ where φ denotes the Euler totient function.

Any automorphism σ of this field is uniquely determined by its action on the primitive n^{th} root of unity ζ_n. This element must be mapped to another primitive n^{th} root of unity (recall these are the roots of the irreducible cyclotomic polynomial $\Phi_n(x)$). Hence, for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $\sigma(\zeta_n) = {\zeta_n}^a$ for some integer a, $1 \leq a < n$, relatively prime to n. Since there are precisely $\varphi(n)$ such integers a, it follows that in fact each of these maps is indeed an automorphism of $\mathbb{Q}(\zeta_n)$.

Note also that we can define σ_a for any integer a relatively prime to n by the same formula, and that σ_a depends only on the residue class of a modulo n. Moreover it is easy to verify that $\sigma_{ab} = \sigma_a \sigma_b$. This proves the following result.

Theorem ([1] §14.5 Theorem 26)**.** *The Galois group of the cyclotomic field $\mathbb{Q}(\zeta_n)$ of n^{th} roots of unity is isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. The isomorphism is given explicitly by*

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^\times & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ a \pmod n & \longmapsto & (\sigma_a : \zeta_n \mapsto {\zeta_n}^a). \end{array}$$

Example. *The field $\mathbb{Q}(\zeta_5)$ is Galois over $\mathbb{Q}$ with Galois group $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$. The elements of the Galois group are $\{\sigma_1 = \mathbf{1}, \sigma_2, \sigma_3, \sigma_4\}$ in the notation above. A generator for this cyclic group is $\sigma_2 : \zeta_5 \mapsto {\zeta_5}^2$ (since 2 has order 4 in $(\mathbb{Z}/5\mathbb{Z})^\times$).*

There is precisely one nontrivial subfield, a quadratic extension of $\mathbb{Q}$, the fixed field of the subgroup $\{\mathbf{1}, \sigma_4 = \sigma_{-1}\}$. An element in this subfield is given by

$$\zeta_5 + \sigma_{-1}\zeta_5 = \zeta_5 + \zeta_5^{-1}$$

since this element is clearly fixed by σ_{-1}. (In general, if K/F is a Galois extension and H is a finite subgroup of $\mathrm{Gal}(K/F)$, then $\sum_{\sigma \in H} \sigma\alpha$ and $\prod_{\sigma \in H} \sigma\alpha$ both lie in $\mathrm{Inv}(H)$ for any $\alpha \in K$.)

One can easily verify that $\mathbb{Q}(\zeta_5 + \zeta_5^{-1}) = \mathbb{Q}(\sqrt{5})$ (cf. the following exercise). It can be shown (using the classical Gauss sum) in general that, for p an odd prime, the field $\mathbb{Q}(\zeta_p)$ contains the quadratic field $\mathbb{Q}(\sqrt{\pm p})$, where the $+$ sign is correct if $p \equiv 1 \bmod 4$ and the $-$ sign is correct if $p \equiv 3 \bmod 4$ (cf. [1] §14.7 Exercise 11).

Exercise ([1] §14.5 Exercise 3)**.** *Determine the quadratic equation satisfied by $\alpha = \zeta_5 + \zeta_5^{-1}$, noticing that the element ζ_5 satisfies $\Phi_5(\zeta_5) = \zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0$. Determine the quadratic equation satisfied by ζ_5 over $\mathbb{Q}(\alpha)$ and use this to explicitly solve for the 5^{th} root of unity.*

Exercise ([1] §14.5 Exercise 7)**.** *Show that complex conjugation restricts to the automorphism $\sigma_{-1} \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of the cyclotomic field of n^{th} roots of unity. Show that the field $K^+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the subfield of real elements in $K = \mathbb{Q}(\zeta_n)$, called the* ***maximal real subfield*** *of K.*

The extension K/F is called an **abelian extension** if K/F is Galois and $\mathrm{Gal}(K/F)$ is an abelian group.

Since all the subgroups and quotient groups of abelian groups are abelian, we see by the Fundamental Theorem of Galois Theory that every subfield containing F of an abelian extension of F is again an abelian extension of F. By the results on composites of extensions (that the Galois group of the composite is isomorphic to a subgroup of the direct product of the Galois groups, cf. [1] §14.4 Proposition 21), we also see that the composite of abelian extensions is again an abelian extension.

Exercise ([1] §14.5 Exercise 10)**.** *Prove that $\mathbb{Q}(\sqrt[3]{2}) \not\subseteq \mathbb{Q}(\zeta_n)$ for any positive integer n.*

It is an open problem to determine which groups arise as the Galois groups of Galois extensions of $\mathbb{Q}$. Actually we have that, every *abelian* group appears as the Galois group of some extension of $\mathbb{Q}$, in fact as the Galois group of some subfield of a cyclotomic field.

Corollary ([1] §14.5 Corollary 28)**.** *Let G be any finite abelian group. Then there is a subfield K of a cyclotomic field with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.*

There is also a converse to this result:

Theorem (Kronecker–Weber)**.** *Let K be a finite abelian extension of $\mathbb{Q}$. Then K is contained in a cyclotomic extension of $\mathbb{Q}$.*

The abelian extensions of $\mathbb{Q}$ are the "easiest" Galois extensions (at least in so far as the structure of their Galois groups is concerned) and the previous result shows they can be classified by the cyclotomic extensions of $\mathbb{Q}$. For other finite extensions of $\mathbb{Q}$ as base field, it is more difficult to describe the abelian extensions. The study of the abelian extensions of an arbitrary finite extension F of $\mathbb{Q}$ is referred to as **class field theory**.

There is a classification of the abelian extensions of F by invariants associated to F which greatly generalizes the results on cyclotomic fields over $\mathbb{Q}$. In general, however, the construction of abelian extensions is not nearly as explicit as in the case of the cyclotomic fields. One case where such a description is possible is for the abelian extensions of an imaginary quadratic field ($Q(\sqrt{-D})$ for $D > 0$), where the abelian extensions can be constructed by adjoining values of certain elliptic functions (this is the analogue of adjoining the roots of unity, which are the values of the exponential function e^x for certain x). The study of the arithmetic of such abelian extensions and the search for similar results for non-abelian extensions are rich and fascinating areas of current mathematical research.

4 Galois groups of polynomials

Recall that the **Galois group** of a separable polynomial $f(x) \in F[x]$ is defined to be the Galois group of the splitting field of $f(x)$ over F.

If K is a finite Galois extension of F, then K is the splitting field for some separable polynomial $f(x)$ over F. Any automorphism $\sigma \in \mathrm{Gal}(K/F)$ maps a root of an irreducible factor of $f(x)$ to another root of the irreducible factor and σ is uniquely determined by its action on these roots (since they generate K over F). If we fix a labelling of the roots $\alpha_1, \ldots, \alpha_n$ of $f(x)$, we see that any $\sigma \in \mathrm{Gal}(K/F)$ defines a unique permutation of $\alpha_1, \ldots, \alpha_n$, hence defines a unique permutation of the subscripts $\{1, 2, \ldots, n\}$ (which depends on the fixed labelling of the roots). This gives an injection

$$\mathrm{Gal}(K/F) \hookrightarrow S_n$$

of the Galois group into the symmetric group on n letters which is clearly a homomorphism (both group operations are composition). We may therefore think of Galois groups as subgroups of symmetric groups.

Since the degree of the splitting field is the same as the order of the Galois group by the Fundamental Theorem, this explains from the group-theoretic side why the splitting field for a polynomial of degree n over F is of degree at most $n!$ over F (cf. [1] §13.4 Proposition 26).

Recall that the alternating group A_n is a normal subgroup of S_n of index 2. Hence $\mathrm{Gal}(K/F) \cap A_n$ is a normal subgroup of $\mathrm{Gal}(K/F)$ of index ≤ 2. It is obvious that $[\mathrm{Gal}(K/F) : \mathrm{Gal}(K/F) \cap A_n] = 1$ if and only if $\mathrm{Gal}(K/F) \leq A_n$.

Proposition ([1] §14.6 Corollary 31 & Proposition 34)**.** *Let $f(x) \in F[x]$ be a monic polynomial, $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x)$ in the splitting field for $f(x)$ over F. Let*

$$\sqrt{D} \coloneqq \prod_{i<j}(\alpha_i - \alpha_j), \qquad D \coloneqq (\sqrt{D})^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

Then

(1) $D \neq 0$ if and only if the roots of $f(x)$ are distinct.

(2) $D \in F$. In fact D is a polynomial in the coefficients of $f(x)$.

(3) If $\mathrm{char}(F) \neq 2$, the Galois group of a monic separable polynomial $f(x)$ is a subgroup of A_n if and only if $D \in F^2$, i.e., the discriminant D is the square of an element of F.

Because of (1) and (3), D is called the **discriminant** of the monic polynomial $f(x)$.

Proof. (1) is obvious.

(2) The discriminant D is a **symmetric function** in $\alpha_1, \ldots, \alpha_n$, i.e., it is fixed under any permutation of subscripts. The Fundamental Theorem on Symmetric Functions ([1] §14.6 Corollary 31) shows that any symmetric function in the variables $\alpha_1, \ldots, \alpha_n$ is a rational function in the **elementary symmetric functions** $s_1, \ldots, s_n$ defined by

$$\begin{aligned}
s_1 &\coloneqq \sum_{i=1}^{n} \alpha_i = \alpha_1 + \alpha_2 + \cdots + \alpha_n \\
s_2 &\coloneqq \sum_{i<j} \alpha_i\alpha_j = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \cdots + \alpha_{n-1}\alpha_n \\
&\vdots \\
s_n &\coloneqq \alpha_1\alpha_2\cdots\alpha_n
\end{aligned}$$

i.e., the i^{th} symmetric function s_i is the sum of all products of the α_j's taken i at a time. It is easy to see by induction that the coefficients of $f(x)$ are given by the elementary symmetric functions in the roots:

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n \in F[x].$$

So D is a polynomial in $s_1, \ldots, s_n \in F$.

(3) Let K be the splitting field for $f(x)$ over F, and $G \coloneqq \mathrm{Gal}(K/F) \hookrightarrow S_n$. By the definition of even permutations, for any $\sigma \in G$, σ is even if and only if $\sigma(\sqrt{D}) = \sqrt{D}$ in a field F of characteristic $\neq 2$, and hence

$$G \leq A_n \iff \text{every } \sigma \in G \text{ is even} \iff \sigma(\sqrt{D}) = \sqrt{D} \text{ for any } \sigma \in G \iff \sqrt{D} \in \mathrm{Inv}(G).$$

By the Fundamental Theorem of Galois theory, $\mathrm{Inv}(G) = F$, and this proves the proposition. □

We have the following diagram:

$$\mathrm{Gal}(K/F) \left\{ \begin{array}{l} K = F(\alpha_1, \ldots, \alpha_n) \\ \quad | \\ F(\sqrt{D}) \\ \quad | \\ F \end{array} \right\} \quad \mathrm{Gal}(K/F) \cap A_n$$

Example (Polynomials of degree 2)**.** *Consider the polynomial $x^2 + bx + c$ with roots α_1, α_2. The discriminant D for this polynomial is $(\alpha_1 - \alpha_2)^2$, which can be written as a polynomial in the elementary symmetric functions of the roots:*

$$D = (\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = s_1^2 - 4s_2 = b^2 - 4c,$$

the usual discriminant for this quadratic.

The polynomial has no multiple root if and only if $D = b^2 - 4c \neq 0$. The Galois group is a subgroup of S_2, the cyclic group of order 2. It is trivial (i.e., A_2 in this case) if and only if $b^2 - 4c$ is a rational square, which completely determines the possible Galois groups.

Note that this restates results we obtained previously by explicitly solving for the roots: if the polynomial is reducible (namely D is a square in F), then the Galois group is trivial (the splitting field is just F), while if the polynomial is irreducible the Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ since the splitting field is the quadratic extension $F(\sqrt{D})$.

Exercise. *Give an example to show that, the criterion in the above proposition does not work when* $\operatorname{char} F = 2$.

4.1 Galois group of a cubic

Suppose the cubic polynomial is

$$f(x) = x^3 + ax^2 + bx + c.$$

If we make the substitution $x = y - a/3$ the polynomial becomes

$$g(y) = y^3 + py + q$$

where

$$p = \frac{1}{3}(3b - a^2), \qquad q = \frac{1}{27}(2a^3 - 9ab + 27c).$$

The splitting fields for these two polynomials are the same since their roots differ by the constant $a/3 \in F$; and since the formula for the discriminant involves the differences of roots, we see that these two polynomials also have the same discriminant. We first compute the discriminant of this polynomial in terms of p and q.

The discriminant for any polynomial of degree n is very hard to calculate. For $n = 3$ our textbook [1] demonstrates an observation making the calculation easier. Let the roots of $g(y)$ be α, β, and γ. Note that

$$g(y) = y^3 + py + q = (y - \alpha)(y - \beta)(y - \gamma)$$

so that if we differentiate we have

$$g'(y) = 3y^2 + p = (y - \beta)(y - \gamma) + (y - \alpha)(y - \gamma) + (y - \alpha)(y - \beta).$$

We see that

$$D = [(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)]2 = -g'(\alpha)g'(\beta)g'(\gamma)$$

and hence

$$\begin{aligned} -D = g'(\alpha)g'(\beta)g'(\gamma) &= (3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p) \\ &= 27\alpha^2\beta^2\gamma^2 + 9p\left(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2\right) + 3p^2\left(\alpha^2 + \beta^2 + \gamma^2\right) + p^3. \end{aligned}$$

The corresponding expressions in the elementary symmetric functions of the roots were determined by the coefficients p and q. We obtain

$$-D = 27(-q)^2 + 9p(p^2) + 3p^2(-2p) + p^3 \qquad \text{so that} \qquad D = -4p^3 - 27q^2.$$

Expressing D in terms of a, b, c we obtain

$$D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

Exercise ([1] §14.6 Exercises 29 & 32 & 35)**.** *Let F be a field and $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^j$ be two polynomials in $F[x]$. The determinant*

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & \dots & a_0 & & & & \\ & a_n & a_{n-1} & \dots & a_0 & & & \\ & & a_n & a_{n-1} & \dots & a_0 & & \\ & & & \ddots & & & \ddots & \\ & & & & a_n & a_{n-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_0 & & & & \\ & b_m & b_{m-1} & \dots & b_0 & & & \\ & & b_m & b_{m-1} & \dots & b_0 & & \\ & & & \ddots & & & \ddots & \\ & & & & b_m & b_{m-1} & \dots & b_0 \end{vmatrix}$$

*of an $(n+m)\times(n+m)$ matrix with m rows involving the coefficients of $f(x)$ and n rows involving the coefficients of $g(x)$, is called the **resultant** of the two polynomials.*

(1) Prove that $f(x)$ and $g(x)$ have a common root if and only if $R(f,g) = 0$.

(2) Consider now the special case where $g(x) = f'(x)$ is the formal derivative of $f(x)$, and suppose the roots of $f(x)$ are $\alpha_1, \dots, \alpha_n$. Using the formula

$$R(f,f') = \prod_{i=1}^{n} f'(\alpha_i),$$

prove that the discriminant D of $f(x)$ satisfies

$$D = (-1)^{n(n-1)/2} R(f,f').$$

(3) Compute the discriminant of $x^3 + px + q$ using the propositions of resultants.

Now we determine the Galois group of $f(x) = x^3 + ax^2 + bx + c$.

If the cubic polynomial $f(x)$ is reducible, then it splits either into three linear factors or into a linear factor and an irreducible quadratic. In the first case the Galois group is trivial and in the second case the Galois group is $\cong \mathbb{Z}/2\mathbb{Z}$.

If the cubic polynomial $f(x)$ is irreducible then a root α of $f(x)$ generates an extension $F(\alpha) \cong F[x]/(f(x))$ of degree 3 over F, so the degree of the splitting field over F is divisible by 3. Since the Galois group is a subgroup of S_3, there are only two possibilities, namely A_3 or S_3. The Galois group is $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ if and only if the discriminant D is a square in F.

Example. *We have seen that the splitting field for $x^3 - 2$ over $\mathbb{Q}$ is Galois with Galois group S_3. The discriminant of $x^3 - 2$ is $D = -4 \cdot 0^3 - 27 \cdot (-2)^2 = -108$, which is not a square in $\mathbb{Q}$.*

Explicitly, let K be the splitting field of $f(x)$ over F, $\alpha_1, \alpha_2, \alpha_3$ be the roots of $f(x)$ in K. Then in $K[x]$,

$$x^3 + ax^2 + bx + c = f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

Since $a \in F$ and $-a = \alpha_1 + \alpha_2 + \alpha_3$, the third root α_3 is in the field generated by the first two roots. So we have a chain of extension fields

$$F \subsetneqq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \quad \text{and} \quad F(\alpha_1, \alpha_2) = F(\alpha_1, \alpha_2, \alpha_3) = K.$$

Let E denote the field $F(\alpha_1) \cong F[x]/(f(x))$. Since $f(x)$ is irreducible over F, $[L : F] = 3$. And since $\alpha_1 \in L$, the polynomial $f(x)$ factors in $L[x]$:

$$f(x) = (x - \alpha_1)q(x),$$

where $q(x)$ is the quadratic polynomial whose roots are α_2 and α_3. So K is obtained from L by adjoining a root of a quadratic polynomial. There are two cases: If $q(x)$ is irreducible over L, then $[K : L] = 2$ and $[K : F] = 6$; if $q(x)$ is reducible over L, then α_2 and α_3 are in L, $L = K$, and $[K : F] = 3$.

To distinguish these two cases, we need to decide whether or not the quadratic polynomial $q(x)$ is irreducible over the field $L = F(\alpha_1)$. Working in the field L is painful. We would rather make a computation in the field F. Fortunately, the discriminant D, which is an element in F, makes it possible to decide. If $D \in F^2$, then the splitting field of the irreducible cubic $f(x)$ is obtained by adjoining any single root α_1 of $f(x)$ to F. The resulting field $F(\alpha_1)$ is Galois over F of degree 3 with $\mathbb{Z}/3\mathbb{Z}$ as Galois group, and the other two roots can be written in the form $a + b\alpha_1 + c\alpha_1^2$ for some $a, b, c \in F$.

Example ([1] §14.6 Exercise 18)**.** *One can calculate that the discriminant of $f(x) = x^3 - 3x + 1$ is $D = -4(-3)^3 - 27 = 81 = 9^2$. So the Galois group of the splitting field of $f(x)$ is $A_3 \cong \mathbb{Z}/3\mathbb{Z}$.*

Let α be a root of $f(x) = x^3 - 3x + 1$. The Fundamental Theorem implies that the splitting field has extension degree 3. In particular the other roots of this polynomial can be written in the form $a + b\alpha + c\alpha^2$ for some $a, b, c \in \mathbb{Q}$.

Actually one can verify that $\zeta + \zeta^{-1}$ is a root of $f(x) = x^3 - 3x + 1$ when ζ is a primitive 9^{th} root of unity (so the three roots of $f(x)$ are precisely $\zeta_9 + \zeta_9^{-1}$, $\zeta_9^2 + \zeta_9^{-2}$ and $\zeta_9^4 + \zeta_9^{-4}$ and they are all real). It happens that if α is a root of $f(x)$, then $\alpha^2 - 2$ is another root (for $\alpha = \zeta + \zeta^{-1}$, we have $\alpha^2 - 2 = \zeta^2 + \zeta^{-2}$). This can also be checked by substituting into $f(x)$. So the splitting field is $\mathbb{Q}(\alpha)$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. (The third root is obviously in $\mathbb{Q}(\alpha)$ since the sum of all three roots is zero.) Recall that $\mathbb{Q}(\alpha)$ is the maximal real subfield of $\mathbb{Q}(\zeta_9)$.

If D is not the square of an element of F then the splitting field of $f(x)$ is of degree 6 over F, hence is the field $F(\alpha_1, \sqrt{D})$ for any one of the roots α_1 of $f(x)$. This extension is Galois over F with Galois group S_3, with generators given by

$$\sigma : \begin{cases} \alpha_1 & \mapsto & \alpha_2 \\ \sqrt{D} & \mapsto & \sqrt{D} \end{cases} \qquad \text{and} \qquad \tau : \begin{cases} \alpha_1 & \mapsto & \alpha_1 \\ \sqrt{D} & \mapsto & -\sqrt{D}. \end{cases}$$

We see that in both cases the splitting field for the irreducible cubic $f(x)$ is obtained by adjoining $\sqrt{D}$ and a root of $f(x)$ to F.

Example. *$f(x) = x^3 + 3x + 1$ is irreducible over $\mathbb{Q}$, and its derivative is nowhere zero on the real line. Therefore $f(x)$ defines an increasing function of the real variable x that takes the value zero exactly once: $f(x)$ has one real root. This root does not generate the splitting field K, which also contains two complex roots. So $[K : \mathbb{Q}] = 6$.*

One can also calculate that the discriminant of $f(x)$ is $D = -4 \cdot 3^3 - 27 = -135 \notin \mathbb{Q}^2$ so the splitting field has Galois group S_3.

Exercise. *Give an example so that $f(x)$ is an irreducible cubic polynomial over $\mathbb{Q}$, with all three roots being real, but the splitting field of which has Galois group S_3.*

Exercise. *Let $\mathbb{F}$ be a finite field and $f(x)$ be an irreducible cubic polynomial over $\mathbb{F}$. Discuss the Galois group of its splitting field.*

4.2 Solution of cubic equations by radicals: Cardano's Formulas

Theorem ([1] §14.7 Propositions 36 & 37)**.** *Let F be a field of characteristic not dividing n which contains the n^{th} roots of unity. Then*

- *the extension $F(\sqrt[n]{a})$ for $a \in F$ is Galois over F with a cyclic Galois group (called a **cyclic extension**), of degree dividing n;*
- (Kummer Theory) *any cyclic extension of degree n over F is of the form $F(\sqrt[n]{a})$ for some $a \in F$. Such extensions are called **Kummer extensions**.*

Kummer's theorem leads to a formula for the roots of a cubic polynomial that was discovered in the sixteenth century by Cardano and Tartaglia. The derivation that we outline here (cf. [2] Example 16.11.4) isn't as short as Cardano's, but it is easier to remember because it is systematic.

We suppose that the quadratic coefficient of the cubic is zero, and to avoid denominators in the solution, we write it as

$$f(x) = x^3 + 3px + 2q.$$

Then the elementary symmetric functions are given by $s_1 = 0, s_2 = 3p, s_3 = -2q$, and the discriminant is $D = -2^2 3^3 (q^2 + p^3)$.

Let the roots be $\alpha_1, \alpha_2, \alpha_3$, numbered arbitrarily. With $\omega = \zeta_3 = e^{2\pi i/3}$, the elements (called the **Lagrange resolvents**)

$$s_1 = \alpha_1 + \alpha_2 + \alpha_3 = 0, \qquad \theta_1 \coloneqq \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \qquad \text{and} \qquad \theta_2 \coloneqq \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3$$

are eigenvectors for the cyclic permutation $\sigma = (1\ 2\ 3)$. Since $1 + \omega + \omega^2 = 0$, the sum of these resolvents is

$$\theta_1 + \theta_2 = s_1 + \theta_1 + \theta_2 = 3\alpha_1.$$

Notice that $\sigma\theta_1 = \omega^2\theta_1$, $\sigma\theta_2 = \omega\theta_2$, therefore the cubes θ_1^3 and θ_2^3 are fixed by σ (and hence by $\langle\sigma\rangle = \mathrm{Gal}(K(\omega)/\mathbb{Q}(\omega)) \cap A_3$). So according to Kummer's Theorem and [1] §14.6 Proposition 34 (by taking $F = \mathbb{Q}(\omega)$ and K to be the splitting field of $f(x)$ over $\mathbb{Q}$, $\mathrm{Gal}(K(\omega)/\mathbb{Q}(\omega)) \cap A_3 = \mathrm{Gal}(K(\omega)/\mathbb{Q}(\omega, \sqrt{D}))$), they can be written in terms of p, q, $\sqrt{D}$, and ω. When the cubes are written in this way, $u_1 = \theta_1 + \theta_2$ will be expressed as a sum of cube roots.

One makes the following computations. Let

$$A = \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1,$$
$$B = \alpha_2^2\alpha_1 + \alpha_3^2\alpha_2 + \alpha_1^2\alpha_3.$$

Then

$$A - B = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) = \sqrt{D},$$
$$A + B = s_1 s_2 - 3s_3 = 6q.$$

Also, $\alpha_1^3 + \alpha_2^3 + \alpha_3^3 = s_1^3 + 3s_1 s_2 + 3s_3 = -6q$. One solves for A, B and expands θ_1^3 and θ_2^3. The result of this computation is Cardano's formula:

$$\theta_1 = \sqrt[3]{-27q + \tfrac{3}{2}\sqrt{-3D}}, \qquad \theta_2 = \sqrt[3]{-27q - \tfrac{3}{2}\sqrt{-3D}};$$
$$\alpha_1 = \tfrac{1}{3}(\theta_1 + \theta_2) = \sqrt[3]{-q + \sqrt{q^2 + p^3}} + \sqrt[3]{-q - \sqrt{q^2 + p^3}},$$
$$\alpha_2 = \tfrac{1}{3}(\omega^2\theta_1 + \omega\theta_2), \qquad \alpha_3 = \tfrac{1}{3}(\omega\theta_1 + \omega^2\theta_2),$$

where the cube roots are chosen so that $\theta_1\theta_2 = -9p$. For instance, a root of $f(x) = x^3 + 3x + 2$ is $x = \sqrt[3]{-1+\sqrt{2}} - \sqrt[3]{-1-\sqrt{2}}$.

However, the formula is ambiguous. In the term $\sqrt[3]{-q+\sqrt{q^2+p^3}}$, the square root can take two values, and when a square root is chosen, there are three possible values for the cube root, giving six ways to read that term. There are also six ways to read the other term. But f has only three roots.

Other related exercises in [1]

§14.2 3 4 5 6 9 11 12 13 14 15 16 17 20
§14.3 1 3 4 8 10 11
§14.4 1 2 7 8
§14.5 2 5 6 11 12 13
§14.6 2 3 27 28 29 32 45

References

[1] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[2] M. Artin. *Algebra*. Pearson Education, Inc., Upper Saddle River, NJ, second edition, 2010.