PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

Mohamed Boudiaf University of M'sila
Faculty of Mathematics and Computer Science
Department of Mathematics

Master's Thesis

Field : Mathematics and Computer Science
Major : Mathematics
Option : Algebra and Discrete Mathematics

Title

Symmetry and Galois Theory .

Presented by :
Miss Naili Roukia

BOUDAOUD Abdelmadjid	Prof,	University of M'sila	**Chair**.
Douadi MIHOUBI	Prof,	University of M'sila	**Supervisor**.
Ghadbane Nacer	M.C.A,	University of M'sila	**Examiner**.

Academic Year 2025/2026

Acknowledgements

First and foremost, I would like to thank "ALLAH", the Almighty, for granting me this research topic, as well as the health, courage, and determination to undertake and successfully complete this work.

I express my deepest gratitude to my supervisor, "Dr. Douadi MIHOUBI", for proposing this thesis topic and for his invaluable guidance, insightful advice, continuous support, and encouragement throughout the realization of this work.

I would also like to extend my sincere thanks to the members of the defense committee for doing me the honor of examining and evaluating this dissertation.

Finally, I am profoundly grateful to my parents for their unconditional love, endless sacrifices, and unwavering support. My heartfelt thanks also go to my brother "Moussa", my sisters "Amel" and "Akila", my entire family, and all my friends who have encouraged and supported me throughout my academic journey.

Thank You All

Dedication

..... I Dedicate This Work .....

A

To every student who has cho

A

To my beloved father, for his encouragement, motivation, and unwavering support throughout my academic journey.

A

To my dear mother, for her endle
for my phy

A

To my brother, Moussa, for his support, encouragement, and pre
whenever I needed it.

A

To my sisters, Amel and Akila, for their love, kindne
and unwavering support.

A

To my uncle, for his valuable advice, assistance, and support in computer-related matters.

A

To all the members of my family and to all my friends, who
and friendship have been a source of strength and inspiration.

✳ ✳ ✳

Naili Roukia

Abstract

It is said that if numbers measure the physical magnitudes of objects (lengths, volumes, masses, ...), then groups measure the degrees of symmetry of geometric figures. Namely, to any figure F, we associate a group called the symmetry group of this figure, i.e., the geometric transformations f that leave the figure globally invariant, i.e., an isometry:

$$f(F) = F$$

and which preserves the distance $d(f(p), f(q)) = d(p, q)$ for any pair of points (p, q) belonging to the figure F. A figure is said to be asymmetric if its symmetry group is the trivial group $\{id_F\}$, whereas, for example, the symmetry group of a regular polygon with n sides is the dihedral group D_{2n} (n rotations + n reflections), and the symmetry group of a circle is of infinite order (the circle has an infinite number of rotations around its center that leave it globally invariant).

Another point of view of symmetry, called arithmetic symmetry, is the study of solvability by radicals, i.e., the expressibility of the roots of the equation

$$a_n x^n + \cdots + a_1 x + a_0 = 0$$

where the coefficients a_i are generally in the field of rational numbers $\mathbb{Q}$, using the operators $(+, -, \times, \boldsymbol{\nabla}\cdot, \sqrt{\cdot})$ plus the coefficients of the equation.

It is shown (Galois theory) that the equation in question is solvable by radicals if and only if the permutation group of its roots is solvable in the sense of group theory.

There is a chain of subgroups from $\{e\}$ up to G (the Galois group of the roots), each one normal in the next, $\{e\} \triangleleft N_1 \triangleleft N_2 \triangleleft \cdots \triangleleft N_n = G$, and each quotient $\frac{N_1}{\{e\}}, \frac{N_2}{N_1}, \ldots, \frac{G}{N_n}$ along the chain is abelian.

In this Master's thesis work in Algebra and Discrete Mathematics, we aim to clarify, through examples, the meaning of solvability by radicals of an equation of degree n.

Keywords: Galois theory, solvability by radicals, symmetry group, polynomial equations, solvable groups.

Résumé

On dit que si les nombres mesurent les grandeurs physiques des objets (longueurs, volumes, masses, ...), alors les groupes mesurent les degrés de symétrie des figures géométriques, à savoir qu'à toute figure F, on associe un groupe dit le groupe de symétrie de cette figure, c.-à-d. les transformations géométriques f qui laissent la figure globalement invariante, c.-à-d. une isométrie :

$$f(F) = F$$

Qui préserve la distance $d(f(p), f(q)) = d(p, q)$ pour tout couple de points (p, q) appartenant à la figure F. Une figure est dite asymétrique si son groupe de symétrie est le groupe trivial $\{id_F\}$, alors que, par exemple, le groupe de symétrie d'un polygone régulier de n côtés est le groupe diédral D_{2n} (n rotations + n réflexions), le groupe de symétrie d'un cercle est d'ordre infini (le cercle a une infinité de rotations autour de son centre qui le laissent invariant globalement).

Un autre point de vue de la symétrie, dite symétrie arithmétique, est l'étude de la résolubilité par radicaux, c.-à-d. l'exprimabilité des racines de l'équation

$$a_n x^n + \cdots + a_1 x + a_0 = 0$$

où les coefficients a_i sont généralement dans le corps des rationnels $\mathbb{Q}$, par les opérateurs $(+, -, \times, \boldsymbol{\nabla}\cdot, \sqrt{\cdot})$ plus les coefficients de l'équation.

On montre (théorie de Galois) que l'équation en question est résoluble par radicaux si et seulement si le groupe des permutations de ses racines est résoluble au sens de la théorie des groupes.

There is a chain of subgroups from $\{e\}$ up to G (the Galois group of the roots), each one normal in the next, $\{e\} \triangleleft N_1 \triangleleft N_2 \triangleleft \cdots \triangleleft N_n = G$ and each quotient $\frac{N_1}{\{e\}}, \frac{N_2}{N_1}, \ldots, \frac{G}{N_n}$ along the chain is abelian.

Dans ce travail de mémoire de Master en Algèbre et Mathématiques Discrètes, on s'intéresse à clarifier à travers des exemples le sens de résolubilité par radicaux d'une équation de degré n.

Mots clés : Théorie de Galois, résolubilité par radicaux, groupe de symétrie, équations polynomiales, groupes résolubles.

Contents

List of Figures

Overview

Symmetry is considered one of the most profound and fascinating concepts in human thought. It is not merely a visual property that grants objects beauty and harmony, but rather a cosmic principle that links art, nature, and the exact sciences. Manifested in fine arts, fashion design, mineral crystals, architectural designs, and ornaments, symmetry emerges as an organizing force that gives the universe its balance.

In the mathematical context, symmetry underwent a radical transformation, shifting from a purely visual geometric idea based on reflection and rotation to a deep algebraic concept embodied in abstract algebraic structures through "Group Theory." Symmetry was no longer just an attribute of shapes; instead, the focus shifted to the study of transformation groups that preserve the properties of the mathematical structure. This very concept manifested in its finest form in "Galois Theory," which employed this algebraic symmetry to study and treat the roots of polynomial equations. So, what is Galois Theory, and what is its relationship to solvability by radicals?

Indeed, the interest in studying symmetry through Galois Theory extends beyond solving classical equations to being a fundamental pillar in exact and contemporary sciences. In physics and chemistry, algebraic symmetry structures provide the paradigm tools for understanding quantum mechanics and the molecular crystalline systems. Technologically, the scientific extension of this symmetry is vividly demonstrated in cryptography and Coding Theory, where cyber security and data protection algorithms fundamentally rely on fields and Galois algebraic structures. This imparts a significant value to this research in linking abstract algebra to modern technical applications.

In this dissertation, we study symmetry from two perspectives: the geometric perspective, focusing on the symmetry of shapes, and the algebraic perspective, through Galois Theory and its relation to solvability by radicals. Therefore, the dissertation is divided into three chapters: the first presents basic concepts of group theory; the second examines geometric symmetry in Euclidean space and in the vector spaces $\mathbb{R}^2$ and $\mathbb{R}^3$; and the third explores Galois Theory and its connection to solvability by radicals.

CHAPTER 1

Notions of Groups

1.1 Group

Definition 1.1

A **group** G is a set of objects $\{g, h, k, \ldots\}$ (not necessarily countable) together with a binary operation which associates with any ordered pair of elements g, h in G a third element gh. The binary operation (called **group multiplication**) is subject to the following requirements:

1. There exists an element e in G called the **identity element** such that:

$$ge = eg = g \quad \text{for all } g \in G.$$

2. For every $g \in G$ there exists in G an **inverse element** g^{-1} such that:

$$gg^{-1} = g^{-1}g = e.$$

3. **Associative law.** The identity $(gh)k = g(hk)$ is satisfied for all $g, h, k \in G$.

Thus, any set together with a binary operation which satisfies conditions (1)–(3) is called a group. If $gh = hg$ we say that the elements g and h **commute**. If all elements of G commute then G is a **commutative** or **abelian** group. If G has a finite number of elements it has **finite order** $n(G)$, where $n(G)$ is the number of elements. Otherwise, G has **infinite order**.

Example 1.1

The real numbers R with addition as the group Operation. The Operation of two elements r_1, r_2 is their sum $r_1 + r_2$. The identity is 0 and the inverse of an element is its negative. R is an infinite abelian group.

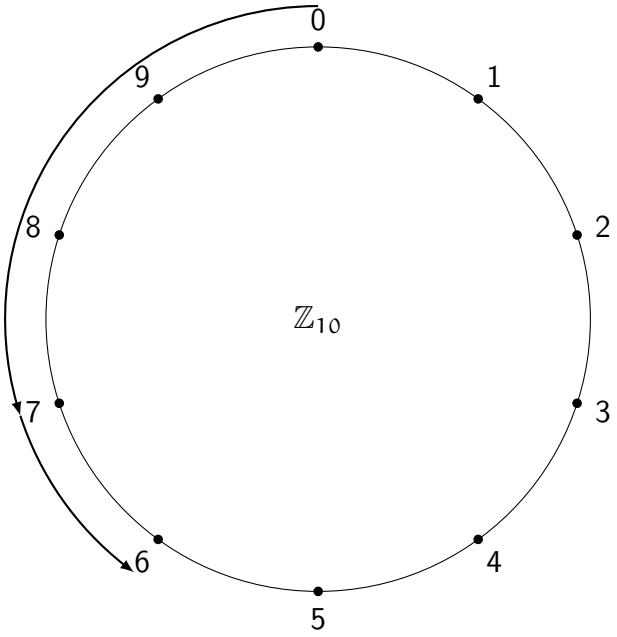
Example 1.2

The group containing two elements $\{0, 1\}$ with group multiplication given by $0 \cdot 0 = 0$, $0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$. The identity element is 1. This is an abelian group of order two. It has only two subgroups, $\{1\}$ and $\{0, 1\}$.

Example 1.3

The group of integers modulo n, denoted by $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{0,1,\ldots,n-1\},$, is a group under the addition operation defined by $\bar{x} \oplus \bar{y} = \overline{x+y} \equiv z(n)$.

The set $\mathbb{Z}_{10}$ is a group under addition. In $\mathbb{Z}_{10}$, we have $3 + 7 = 0$. Thus, the additive inverse of 3 is 7, and we write $-3 = 7$. Note how this is consistent with our computation on the $\mathbb{Z}_{10}$ clock. To find -3 on the $\mathbb{Z}_{10}$ clock, we first view -3 as $0 - 3$. Then, we start at 0 on the $\mathbb{Z}_{10}$ clock and move 3 units *counterclockwise*. We land on 7, so that $-3 = 7$ in $\mathbb{Z}_{10}$.



Theorem 1.1 (Uniqueness of the Identity)

In a group G, there is only one identity element.

Proof. Suppose both e and e' are identities of G. Then,

1. $ae = a$ for all a in G, and
2. $e'a = a$ for all a in G.

The choices of $a = e'$ in (1) and $a = e$ in (2) yield $e'e = e'$ and $e'e = e$. Thus, e and e' are both equal to $e'e$ and so are equal to each other. □

Because of this theorem, we may unambiguously speak of "the identity" of a group and denote it by e (because the German word for identity is *Einheit*).

Theorem 1.2 (Uniqueness of Inverses)

For each element a in a group G, there is a unique element b in G such that $ab = ba = e$.

Proof. Suppose b and c are both inverses of a. Then $ab = e$ and $ac = e$, so that $ab = ac$. Canceling the a on both sides gives $b = c$, as desired. □

Theorem 1.3

A nonempty subset H of a group G is a subgroup if and only if the following two conditions hold:

(1) If $h, k \in H$ then $hk \in H$.

(2) If $h \in H$ then $h^{-1} \in H$.

Example 1.4

Recall that $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ is a group under addition. Let $H = \{0, 2, 4, 6\}$ be a subset of $\mathbb{Z}_8$. The addition table for H is shown below:

+	0	2	4	6
0	0	2	4	6
2	2	4	6	0
4	4	6	0	2
6	6	0	2	4

We verify that H is also a group under addition:

(1) H is closed under addition, as every entry in the table (i.e., all possible sums) is an element of H.

(2) Addition in H is associative. After all, H uses addition in $\mathbb{Z}_8$, which is known to be associative.

(3) The element $0 \in H$ is the additive identity of H, because $0 + h = h$ and $h + 0 = h$ for all $h \in H$.

(4) Each element $h \in H$ has an additive inverse, which is also in H. Note that 2 and 6 are inverse pairs, while 0 and 4 are self-inverses.

Therefore, H is also a group, with the same operation as $\mathbb{Z}_8$.

In the example above, we say that H is a *subgroup* of $\mathbb{Z}_8$. Here's the definition.

Theorem 1.4

$S(\mathbb{Z}_m)$ is a subgroup of $G(\mathbb{Z}_m)$.

Proof. We will show that $S(\mathbb{Z}_m)$ is closed under matrix multiplication. Assume $\alpha, \beta \in S(\mathbb{Z}_m)$. Then $\det \alpha = 1$ and $\det \beta = 1$. Thus, $\det(\alpha \cdot \beta) = \det \alpha \cdot \det \beta = 1 \cdot 1 = 1$. Hence, $\det(\alpha \cdot \beta) = 1$ and so $\alpha \cdot \beta \in S(\mathbb{Z}_m)$. Next, note that $\det \varepsilon = \det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1$ and thus $\varepsilon \in S(\mathbb{Z}_m)$. Lastly, suppose $\gamma \in S(\mathbb{Z}_m)$. Then $\det \gamma = 1$. Note that $\det\left(\gamma^{-1}\right) = (\det \gamma)^{-1} = 1^{-1} = 1$. Thus $\gamma^{-1} \in S(\mathbb{Z}_m)$. □

Theorem 1.5

Let $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in G(\mathbb{Z}_{13}) \mid a \in U_{13} \right\}$. Then H is a subgroup of $G(\mathbb{Z}_{13})$.

Proof. We will show that H is closed under matrix multiplication. Assume $\alpha, \beta \in H$. Then $\alpha = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ and $\beta = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}$, where $a, b \in U_{13}$. Thus $\alpha \cdot \beta = \begin{bmatrix} a \cdot b & 0 \\ 0 & a \cdot b \end{bmatrix}$, which is in H, since $a \cdot b \in U_{13}$. Next, note that $\varepsilon = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ with $a = 1 \in U_{13}$, and thus $\varepsilon \in H$. Lastly, suppose $\gamma = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} \in H$, where $c \in U_{13}$. To find γ^{-1}, let $\Delta = \det \gamma = c^2$ so that $\Delta^{-1} = c^{-2}$, which exists because $c \in U_{13}$. Then

$$\gamma^{-1} = \Delta^{-1} \cdot \begin{bmatrix} c & -0 \\ -0 & c \end{bmatrix} = c^{-2} \cdot \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} = \begin{bmatrix} c^{-1} & 0 \\ 0 & c^{-1} \end{bmatrix},$$

where $c^{-1} \in U_{13}$. Thus, $\gamma^{-1} \in H$. □

Remark 1.1

In the above proof, we used the fact that U_{13} is a multiplicative group. We stated that $a \cdot b \in U_{13}$, because $a, b \in U_{13}$ (i.e., closure). We also claimed that c^{-2} exists and $c^{-1} \in U_{13}$, since $c \in U_{13}$ (i.e., inverses).

Theorem 1.6

If G is a commutative group, then $H = \{g \in G \mid g^2 = \varepsilon\}$ is a subgroup of G.

Proof. We will first show that H is closed. Assume $a, b \in H$. Then $a^2 = \varepsilon$ and $b^2 = \varepsilon$. Since G is commutative, we have $(ab)^2 = a^2b^2 = \varepsilon \cdot \varepsilon = \varepsilon$. Hence, $(ab)^2 = \varepsilon$ and so $ab \in H$.

Next, note that $\varepsilon^2 = \varepsilon$ and thus $\varepsilon \in H$. Lastly, suppose $c \in H$. Then $c^2 = \varepsilon$. Note that $(c^{-1})^2 = (c^2)^{-1} = \varepsilon^{-1} = \varepsilon$. Thus $(c^{-1})^2 = \varepsilon$ so that $c^{-1} \in H$. □

Proposition 1.1

Let G be a group and let $H_1, H_2, \ldots, H_n$ be subgroups of G. Then $H_1 \cap H_2 \cap \cdots \cap H_n$ is a subgroup of G. More generally, if $\{H_\alpha\}$ is any collection of subgroups, then $\cap_\alpha H_\alpha$ is a subgroup.

Proof. For any group G and any subset $S \subseteq G$, there is a smallest subgroup of G that contains S, which is called the *subgroup generated by* S and denoted $\langle S \rangle$. When $S = \{a\}$ is a singleton, the subgroup generated by S is denoted by $\langle a \rangle$. We say that G is *generated by* S or that S *generates* G if $G = \langle S \rangle$.

A "constructive" view of $\langle S \rangle$ is that it consists of all possible prod- ucts $g_1 g_2 \cdots g_n$, where $g_i \in S$ or $g_i^{-1} \in S$. Another view of $\langle S \rangle$, which is sometimes useful, is that it is the intersection of the family of all sub- groups of G that contain S; this family is nonempty since G itself is such a subgroup.

The family of subgroups of a group G are partially ordered by set inclusion.[1] In fact, the family of subgroups forms what is called a *lattice*.[2] This means that, given two subgroups A and B of G there is a unique smallest subgroup C such that $C \supseteq A$ and $C \supseteq B$. In fact, the subgroup C is $\langle A \cup B \rangle$. Furthermore, there is a unique largest subgroup D such that $D \subseteq A$ and $D \subseteq B$; in fact, $D = A \cap B$. □

1.2 Cyclic Groups

Proposition 1.2

Let a be an element of a group G. The subgroup $\langle a \rangle$ generated by a is $\{a^k : k \in \mathbb{Z}\}$.

Proof. The formulas $a^k a^l = a^{k+l}$ and $(a^k)^{-1} = a^{-k}$ show that $\{a^k : k \in \mathbb{Z}\}$ is a subgroup of G containing $a = a^1$. Therefore, $\langle a \rangle \subseteq \{a^k : k \in \mathbb{Z}\}$. On the other hand, a subgroup is always is closed under taking integer powers, so $\langle a \rangle \supseteq \{a^k : k \in \mathbb{Z}\}$. □

Definition 1.2

Let a be an element of a group G. The set $\langle a\rangle = \{a^k : k \in \mathbb{Z}\}$ of powers of a is called the cyclic subgroup generated by a. If there is an element $a \in G$ such that $\langle a\rangle = G$, we say that G is a cyclic group. We say that a is a generator of the cyclic group.

Example 1.5

Take $G = \mathbb{Z}$, with addition as the group operation, and take any element $d \in \mathbb{Z}$. Because the group operation is addition, the set of powers of d with respect to this operation is the set of integer multiples of d, in the ordinary sense. For example, the third power of d is $d + d + d = 3d$.

Thus, $\langle d\rangle = d\mathbb{Z} = \{nd : n \in \mathbb{Z}\}$ is a cyclic subgroup of $\mathbb{Z}$. Note that $\langle d\rangle = \langle -d\rangle$.

$\mathbb{Z}$ itself is cyclic, $\langle 1\rangle = \langle -1\rangle = \mathbb{Z}$.

Example 1.6

Let C_n denote the set of n^{th} roots of unity in the complex numbers.

(a) $C_n = \{e^{2\pi ik/n} : 0 \leqslant k \leqslant n-1\}$.

(b) C_n is a cyclic group of order n with generator $\xi = e^{2\pi i/n}$.

Proof. C_n is a subgroup of the multiplicative group of nonzero complex numbers, as the product of two n^{th} roots of unity is again an n^{th} root of unity, and the inverse of an n^{th} root is also an n^{th} root or unity.

If z is an n^{th} root of unity in $\mathbb{C}$, then $|z|^n = |z^n| = 1$; thus $|z|$ is a positive n^{th} root of 1, so $|z| = 1$. Therefore, z has the form $z = e^{i\theta}$, where $\theta \in \mathbb{R}$. Then $1 = z^n = e^{in\theta}$. Hence $n\theta$ is an integer multiple of 2π, and $z = e^{2\pi ik/n}$ for some $k \in \mathbb{Z}$. These numbers are exactly the powers of $\xi = e^{2\pi i/n}$, which has order n. □

Theorem 1.7

(a) *Every subgroup of $\mathbb{Z}$ is cyclic.*

(b) *Even better, every subgroup of a cyclic group is cyclic.*

Proof of (a). Let H be a subgroup of $\mathbb{Z}$. If $H = \{0\}$ then H is cyclic. If $H \neq \{0\}$, then H contains a non-zero integer x, and since H is a subgroup it must also contain $-x$. So H contains a positive integer. Let d be the smallest posi- tive integer in H. We claim that d generates H. If $n \in H$, divide n by d to give $n = qd + m$ where q and m are integers and $0 \leqslant m < d$. In other words $m = n \pmod{d}$. We know that $n \in H$ and $d \in H$. As H is a subgroup $qd \in H$, hence $-qd \in H$, and therefore

$$m = n - qd = n + (-qd)$$

belongs to H. This contradicts our choice of d unless m is zero. Consequently $n = qd$, showing each element of H to be an integer multiple of d as required. □

Proof of (b). Let G be a cyclic group and K a subgroup of G which is not the trivial subgroup $\{e\}$. If x is a generator for G, then every element of G, and hence every element of K, is a power of x. Let $H = \{n \in \mathbb{Z} \mid x^n \in K\}$. One easily checks that H is a subgroup of $\mathbb{Z}$. By (a) H is cyclic and, if d generates H, then x^d generates K. This completes the proof. □

1.3 Quotient Groups

1.3.1 Coset

Definition 1.3 (Coset of H in G)

Let G be a group and let H be a subset of G. For any $a \in G$, the set $\{ah \mid h \in H\}$ is denoted by aH. Analogously, $Ha = \{ha \mid h \in H\}$ and $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. When H is a subgroup of G, the set aH is called the *left coset of* H *in* G *containing* a, whereas Ha is called the *right coset of* H *in* G *containing* a. In this case, the element a is called the *coset representative of* aH *(or* Ha*)*. We use $|aH|$ to denote the number of ele- ments in the set aH, and $|Ha|$ to denote the number of elements in Ha.

Example 1.7

Let $H = \{0, 3, 6\}$ in $\mathbb{Z}_9$ under addition. In the case that the group operation is addition, we

use the notation $a + H$ instead of aH. Then the cosets of H in $\mathbb{Z}_9$ are

$$0 + H = \{0, 3, 6\} = 3 + H = 6 + H,$$
$$1 + H = \{1, 4, 7\} = 4 + H = 7 + H,$$
$$2 + H = \{2, 5, 8\} = 5 + H = 8 + H.$$

The three preceding examples illustrate a few facts about cosets that are worthy of our attention. First, cosets are usually not subgroups. Second, aH may be the same as bH, even though a is not the same as b. Third, since in Example 1.8 $(12)H = \{(12), (132)\}$ whereas $H(12) = \{(12), (123)\}$, aH need not be the same as Ha.

These examples and observations raise many questions. When does $aH = bH$? Do aH and bH have any elements in common? When does $aH = Ha$? Which cosets are subgroups? Why are cosets important? The next lemma and theorem answer these questions. (Analogous results hold for right cosets.)

Lemma 1.1 (Properties of Cosets)

Ou un environnement personnalisé similaire *Let* H *be a subgroup of* G*, and let* a *and* b *belong to* G*. Then,*

1. $a \in aH$,
2. $aH = H$ *if and only if* $a \in H$,
3. $aH = bH$ *if and only if* $a \in bH$
4. $aH = bH$ *or* $aH \cap bH = \varnothing$,
5. $aH = bH$ *if and only if* $a^{-1}b \in H$,
6. $|aH| = |bH|$,
7. $aH = Ha$ *if and only if* $H = aHa^{-1}$,
8. aH *is a subgroup of* G *if and only if* $a \in H$.

1.3.2 Normal Subgroups

Definition 1.4 (Normal Subgroup)

A subgroup H of a group G is called a *normal* subgroup of G if $aH = Ha$ for all a in G. We denote this by $H \triangleleft G$.

Theorem 1.8 (Normal Subgroup Test)

A subgroup H of G is normal in G if and only if $xHx^{-1} \subseteq H$ for all x in G.

Proof. If H is normal in G, then for any $x \in G$ and $h \in H$ there is an h' in H such that $xh = h'x$. Thus, $xhx^{-1} = h'$, and therefore $xHx^{-1} \subseteq H$.

Conversely, if $xHx^{-1} \subseteq H$ for all x, then, letting $x = a$, we have $aHa^{-1} \subseteq H$ or $aH \subseteq Ha$. On the other hand, letting $x = a^{-1}$, we have $a^{-1}H(a^{-1})^{-1} = a^{-1}Ha \subseteq H$ or $Ha \subseteq aH$. □

Example 1.8

Every subgroup of an Abelian group is normal. (In this case, $ah = ha$ for a in the group and h in the subgroup.)

Example 1.9

The center $Z(G)$ of a group is always normal. [Again, $ah = ha$ for any $a \in G$ and any $h \in Z(G)$.]

Example 1.10

The alternating group A_n of even permutations is a normal subgroup of S_n. [Note, for example, that for $(12) \in S_n$ and $(123) \in A_n$, we have $(12)(123) \neq (123)(12)$ but $(12)(123) = (132)(12)$ and $(132) \in A_n$.]

Example 1.11

The subgroup of rotations in D_n is normal in D_n. (For any rotation r and any reflection f, we have $fr = r^{-1}f$, whereas for any rotations r and r', we have $rr' = r'r$.)

Theorem 1.9 (Factor Groups (O. Hölder, 1889))

Let G be a group and let H be a normal subgroup of G. The set $G/H = \{aH \mid a \in G\}$ is a group under the operation $(aH)(bH) = abH$.[†]

We point out that the converse of Theorem 1.9 is also true; that is, if the correspondence $aHbH = abH$ defines a group operation on the set of left cosets of H in G, then H is normal in G.

The next few examples illustrate the factor group concept.

Example 1.12

Let $4Z = \{0, \pm 4, \pm 8, \dots\}$. To construct $Z/4Z$, we first must determine the left cosets of $4Z$ in Z. Consider the following four cosets:

$$0 + 4Z = 4Z = \{0, \pm 4, \pm 8, \dots\},$$
$$1 + 4Z = \{1, 5, 9, \dots; -3, -7, -11, \dots\},$$
$$2 + 4Z = \{2, 6, 10, \dots; -2, -6, -10, \dots\},$$
$$3 + 4Z = \{3, 7, 11, \dots; -1, -5, -9, \dots\}.$$

We claim that there are no others. For if $k \in Z$, then $k = 4q + r$, where $0 \leqslant r < 4$; and, therefore, $k + 4Z = r + 4q + 4Z = r + 4Z$. Now that we know the elements of the factor group, our next job is to determine the structure of $Z/4Z$. Its Cayley table is

	$\mathbf{0 + 4Z}$	$\mathbf{1 + 4Z}$	$\mathbf{2 + 4Z}$	$\mathbf{3 + 4Z}$
$\mathbf{0 + 4Z}$	$0 + 4Z$	$1 + 4Z$	$2 + 4Z$	$3 + 4Z$
$\mathbf{1 + 4Z}$	$1 + 4Z$	$2 + 4Z$	$3 + 4Z$	$0 + 4Z$
$\mathbf{2 + 4Z}$	$2 + 4Z$	$3 + 4Z$	$0 + 4Z$	$1 + 4Z$
$\mathbf{3 + 4Z}$	$3 + 4Z$	$0 + 4Z$	$1 + 4Z$	$2 + 4Z$

Clearly, then, $Z/4Z \approx Z_4$. More generally, if for any $n > 0$ we let $nZ = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$, then Z/nZ is isomorphic to Z_n.

Example 1.13

Let $G = Z_{18}$ and let $H = \langle 6 \rangle = \{0, 6, 12\}$. Then $G/H = \{0+H, 1+H, 2+H, 3+H, 4+H, 5+H\}$. To illustrate how the group elements are combined, consider $(5 + H) + (4 + H)$. This should be one of the six elements listed in the set G/H. Well, $(5 + H) + (4 + H) = 5 + 4 + H = 9 + H = 3 + 6 + H = 3 + H$, since H absorbs all multiples of 6.

A few words of caution about notation are warranted here. When H is a normal subgroup of G, the expression $|aH|$ has two possible interpretations. One could be thinking of aH as a *set* of elements and $|aH|$ as the size of the set; or, as is more often the case, one could be thinking of aH as a group element of the factor group G/H and $|aH|$ as the order of the *element* aH in G/H. In Example 8, for instance, the *set* $3 + H$ has size 3, since $3 + H = \{3, 9, 15\}$. But the *group element* $3 + H$ has order 2, since $(3 + H) + (3 + H) = 6 + H = 0 + H$. As is usually the case when one notation has more than one meaning, the appropriate interpretation will be clear from the context.

Example 1.14

Let $\mathcal{H} = \{R_0, R_{180}\}$, and consider the factor group of the dihedral group D_4 (see page 32 for the multiplication table for D_4)

$$D_4/\mathcal{H} = \{\mathcal{H}, R_{90}\mathcal{H}, H\mathcal{H}, D\mathcal{H}\}.$$

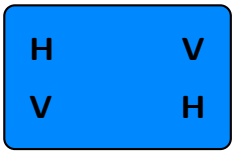
The multiplication table for $D_4/\mathcal{H}$ is given in Table 9.1. (Notice that even though $R_{90}H = D'$, we have used $D\mathcal{H}$ in Table 9.1 for $HR_{90}\mathcal{H}$ because $D'\mathcal{H} = D\mathcal{H}$.)

	$\mathcal{K}$	$R_{90}\mathcal{K}$	$H\mathcal{K}$	$D\mathcal{K}$
$\mathcal{K}$	$\mathcal{K}$	$R_{90}\mathcal{K}$	$H\mathcal{K}$	$D\mathcal{K}$
$R_{90}\mathcal{K}$	$R_{90}\mathcal{K}$	$\mathcal{K}$	$D\mathcal{K}$	$H\mathcal{K}$
$H\mathcal{K}$	$H\mathcal{K}$	$D\mathcal{K}$	$\mathcal{K}$	$R_{90}\mathcal{K}$
$D\mathcal{K}$	$D\mathcal{K}$	$H\mathcal{K}$	$R_{90}\mathcal{K}$	$\mathcal{K}$

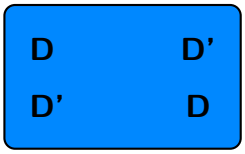
Table 1.1. Table 9.1

$D_4/\mathcal{H}$ provides a good opportunity to demonstrate how a factor group of G is related to G

itself. Suppose we arrange the heading of the Cayley table for D_4 in such a way that elements from the same coset of $\mathcal{H}$ are in adjacent columns (Table 9.2). Then, the multiplication table for D_4 can be blocked off into boxes that are cosets of $\mathcal{H}$, and the substitution that replaces a box containing the element x with the coset $x\mathcal{H}$ yields the Cayley table for $D_4/\mathcal{H}$.
For example, when we pass from D_4 to $D_4/\mathcal{H}$, the box



in Table 9.2 becomes the element $H\mathcal{H}$ in Table 9.1. Similarly, the box



becomes the element $D\mathcal{H}$, and so on.

	R_0	R_{180}	R_{90}	R_{270}	H	V	D	D'
R_0	R_0	R_{180}	R_{90}	R_{270}	H	V	D	D'
R_{180}	R_{180}	R_0	R_{270}	R_{90}	V	H	D'	D
R_{90}	R_{90}	R_{270}	R_{180}	R_0	D'	D	H	V
R_{270}	R_{270}	R_{90}	R_0	R_{180}	D	D'	V	H
H	H	V	D	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	H	D'	D	R_{180}	R_0	R_{270}	R_{90}
D	D	D'	V	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	D	H	V	R_{90}	R_{270}	R_{180}	R_0

Table 1.2. Table 9.2

In this way, one can see that the formation of a factor group G/H causes a systematic collapse of the elements of G. In particular, all the elements in the coset of H containing a collapse to the single group element aH in G/H.

Example 1.15

Let $G = U(32) = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$ and $H = U_{16}(32) = \{1, 17\}$. Then G/H is an Abelian group of order $16/2 = 8$. Which of the three Abelian groups of order 8 is it—Z_8, $Z_4 \oplus Z_2$, or $Z_2 \oplus Z_2 \oplus Z_2$? To answer this question, we need only determine the elements of G/H and their orders. Observe that the eight cosets

$$1H = \{1, 17\}, \quad 3H = \{3, 19\}, \quad 5H = \{5, 21\}, \quad 7H = \{7, 23\},$$
$$9H = \{9, 25\}, \quad 11H = \{11, 27\}, \quad 13H = \{13, 29\}, \quad 15H = \{15, 31\}$$

are all distinct, so that they form the factor group G/H. Clearly, $(3H)^2 = 9H \neq H$, and so $3H$ has order at least 4. Thus, G/H is not $Z_2 \oplus Z_2 \oplus Z_2$. On the other hand, direct computations show that both $7H$ and $9H$ have order 2, so that G/H cannot be Z_8 either, since a cyclic group of even order has exactly one element of order 2 (Theorem 4.4). This proves that $U(32)/U_{16}(32) \approx Z_4 \oplus Z_2$, which (not so incidentally!) is isomorphic to $U(16)$.

Theorem 1.10 (The G/Z Theorem)

Let G be a group and let $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic, then G is Abelian.

1.4 Groups Homomorphisms

Definition 1.5 (Group Homomorphism)

A *homomorphism* ϕ from a group G to a group $\overline{G}$ is a mapping from G into $\overline{G}$ that preserves the group operation; that is, $\phi(ab) = \phi(a)\phi(b)$ for all a, b in G.

Before giving examples and stating numerous properties of homomorphisms, it is convenient to introduce an important subgroup that is intimately related to the image of a homomorphism.

Definition 1.6 (Kernel of a Homomorphism)

The *kernel* of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G \mid \phi(x) = e\}$. The kernel of ϕ is denoted by Ker ϕ.

Definition 1.7 (Normal Subgroup)

A subgroup H of a group G is called a *normal* subgroup of G if $aH = Ha$ for all a in G. We denote this by $H \triangleleft G$.

Example 1.16

Let $\mathbf{R}^*$ be the group of nonzero real numbers under multiplication. Then the determinant mapping $A \to \det A$ is a homomorphism from $GL(2, \mathbf{R})$ to $\mathbf{R}^*$. The kernel of the determinant mapping is $SL(2, \mathbf{R})$.

Example 1.17

The mapping ϕ from $\mathbf{R}^*$ to $\mathbf{R}^*$, defined by $\phi(x) = |x|$, is a homomorphism with Ker $\phi = \{1, -1\}$.

Example 1.18

Let $\mathbf{R}[x]$ denote the group of all polynomials with real coefficients under addition. For any f in $\mathbf{R}[x]$, let f' denote the derivative of f. Then the mapping $f \to f'$ is a homomorphism from $\mathbf{R}[x]$ to itself. The kernel of the derivative mapping is the set of all constant polynomials.

Example 1.19

The mapping ϕ from Z to Z_n, defined by $\phi(m) = m \pmod n$, is a homomorphism (see Exercise 11 in Chapter 0). The kernel of this mapping is $\langle n \rangle$.

1.4.1 Properties of Homomorphisms

Theorem 1.11 (Properties of Elements Under Homomorphisms)

Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let g be an element of G. Then

1. ϕ carries the identity of G to the identity of $\overline{G}$.
2. $\phi(g^n) = (\phi(g))^n$ for all $n \in \mathbb{Z}$.
3. If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.
4. $\ker \phi$ is a subgroup of G.
5. $\phi(a) = \phi(b)$ if and only if $a \ker \phi = b \ker \phi$.

6. If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g \ker \phi$.

Since homomorphisms preserve the group operation, it should not be a surprise that they preserve many group properties.

Theorem 1.12 (Properties of Subgroups Under Homomorphisms)

Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let H be a subgroup of G. Then

1. $\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of $\overline{G}$.
2. If H is cyclic, then $\phi(H)$ is cyclic.
3. f H is Abelian, then $\phi(H)$ is Abelian.
4. If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$.
5. If $|\text{Ker } \phi| = n$, then ϕ is an n-to-1 mapping from G onto $\phi(G)$.
6. If $|H| = n$, then $|\phi(H)|$ divides n.
7. If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a subgroup of G.
8. If $\overline{K}$ is a normal subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a normal subgroup of G.
9. If ϕ is onto and Ker $\phi = \{e\}$, then ϕ is an isomorphism from G to $\overline{G}$.

1.5 group isomorphism

Definition 1.8 (Definition Group Isomorphism)

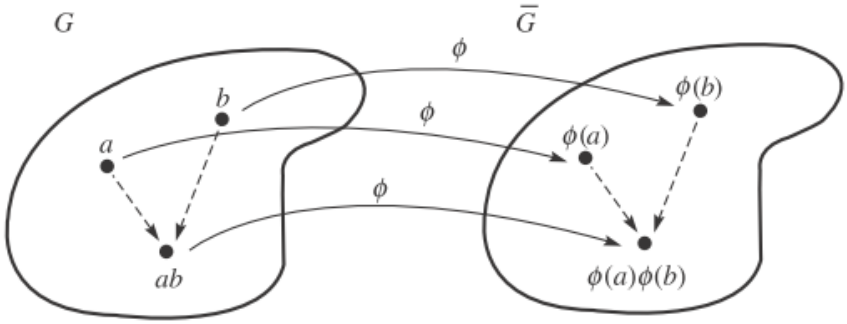
An *isomorphism* ϕ from a group G to a group $\overline{G}$ is a one-to-one mapping (or function) from G onto $\overline{G}$ that preserves the group operation. That is,

$$\phi(ab) = \phi(a)\phi(b) \quad \text{for all } a, b \text{ in } G.$$

If there is an isomorphism from G onto $\overline{G}$, we say that G and $\overline{G}$ are *isomorphic* and write

$G \approx \overline{G}$.

definition can be visualized as shown in Figure 6.1. The pairs of dashed arrows represent the group operations.



It is implicit in the definition of isomorphism that isomorphic groups have the same order. It is also implicit in the definition of isomorphism that the operation on the left side of the equal sign is that of G, whereas the operation on the right side is that of $\overline{G}$. The four cases involving $\cdot$ and $+$ are shown in Table 6.1.

Table 6.1

G Operation	$\overline{G}$ Operation	Operation Preservation
$\cdot$	$\cdot$	$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$
$\cdot$	$+$	$\phi(a \cdot b) = \phi(a) + \phi(b)$
$+$	$\cdot$	$\phi(a + b) = \phi(a) \cdot \phi(b)$
$+$	$+$	$\phi(a + b) = \phi(a) + \phi(b)$

There are four separate steps involved in proving that a group G is isomorphic to a group $\overline{G}$.

Step 1 "Mapping." Define a candidate for the isomorphism; that is, define a function ϕ from G to $\overline{G}$.

Step 2 "1–1." Prove that ϕ is one-to-one; that is, assume that $\phi(a) = \phi(b)$ and prove that $a = b$.

Step 3 "Onto." Prove that ϕ is onto; that is, for any element $\overline{g}$ in $\overline{G}$, find an element g in G such that $\phi(g) = \overline{g}$.

Step 4 "O.P." Prove that ϕ is operation-preserving; that is, show that $\phi(ab) = \phi(a)\phi(b)$ for all a and b in G.

Before going any further, let's consider some examples.

Example 1.20

Let G be the real numbers under addition and let $\overline{G}$ be the positive real numbers under multiplication. Then G and $\overline{G}$ are isomorphic under the mapping $\phi(x) = 2^x$. Certainly, ϕ is a function from G to $\overline{G}$. To prove that it is one-to-one, suppose that $2^x = 2^y$. Then $\log_2 2^x = \log_2 2^y$, and therefore $x = y$. For "onto," we must find for any positive real number y some real number x such that $\phi(x) = y$; that is, $2^x = y$. Well, solving for x gives $\log_2 y$. Finally,

$$\phi(x + y) = 2^{x+y} = 2^x \cdot 2^y = \phi(x)\phi(y)$$

for all x and y in G, so that ϕ is operation-preserving as well.

Example 1.21

The mapping from $\mathbf{R}$ under addition to itself given by $\phi(x) = x^3$ is *not* an isomorphism. Although ϕ is one-to-one and onto, it is not operation-preserving, since it is not true that $(x + y)^3 = x^3 + y^3$ for all x and y.

Example 1.22

$U(10) \approx Z_4$ and $U(5) \approx Z_4$. To verify this, one need only observe that both $U(10) \text{and} U(5)$ are cyclic of order 4.

Example 1.23

There is no isomorphism from Q, the group of rational numbers under addition, to Q^*, the group of nonzero rational numbers under multiplication. If ϕ were such a mapping, there would be a rational number a such that $\phi(a) = -1$. But then

$$-1 = \phi(a) = \phi(\tfrac{1}{2}a + \tfrac{1}{2}a) = \phi(\tfrac{1}{2}a)\phi(\tfrac{1}{2}a) = [\phi(\tfrac{1}{2}a)]^2.$$

However, no rational number squared is -1.

1.5.1 Properties of Isomorphisms

Theorem 1.13 (Properties of Isomorphisms Acting on Elements)

Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. ϕ carries the identity of G to the identity of $\overline{G}$.
2. For every integer n and for every group element a in G, $\phi(a^n) = [\phi(a)]^n$.
3. For any elements a and b in G, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.
4. $G = \langle a \rangle$ if and only if $\overline{G} = \langle \phi(a) \rangle$.
5. $|a| = |\phi(a)|$ for all a in G (isomorphisms preserve orders).
6. For a fixed integer k and a fixed group element b in G, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in $\overline{G}$.
7. If G is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.

1.6 Symmetric group

1.6.1 Permutation group

In general, the permutations of a set X form a group S_X. If X is a finite set, we can assume $X = \{1,2,\ldots,n\}$. In this case we write S_n instead of S_X. The following theorem says that S_n is a group. We call this group the ***symmetric group on*** n ***letters***.

Theorem 1.14

The symmetric group on n letters, S_n, is a group with $n!$ elements, where the binary operation is the composition of maps.

Proof. The identity of S_n is just the identity map that sends 1 to 1, 2 to 2, ..., n to n. If $f : S_n \to S_n$ is a permutation, then f^{-1} exists, since f is one-to-one and onto; hence, every permutation has an inverse. Composition of maps is associative, which makes the group operation associative. We leave the proof that $|S_n| = n!$. □

Example 1.24

Consider the subgroup G of S_5 consisting of the identity permutation id and the permutations

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$
$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

The following table tells us how to multiply elements in the permutation group G.

$\circ$	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	id	μ	τ
τ	τ	μ	id	σ
μ	μ	τ	σ	id

Remark 1.2

Though it is natural to multiply elements in a group from left to right, functions are composed from right to left. Let σ and τ be permutations on a set X. To compose σ and τ as functions, we calculate $(\sigma \circ \tau)(x) = \sigma(\tau(x))$. That is, we do τ first, then σ. There are several ways to approach this inconsistency. *We will adopt the convention of multiplying permutations right to left.* To compute $\sigma\tau$, do τ first and then σ. That is, by $\sigma\tau(x)$ we mean $\sigma(\tau(x))$. (Another way of solving this problem would be to write functions on the right; that is, instead of writing $\sigma(x)$, we could write $(x)\sigma$. We could also multiply permutations left to right to agree with the usual way of multiplying elements in a group. Certainly all of these methods have been used.

Example 1.25

Permutation multiplication is not usually commutative. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix},$$

but

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

1.6.2 Cycle Notation

A permutation $\sigma \in S_X$ is a ***cycle of length*** k if there exist elements $a_1, a_2, \ldots, a_k \in X$ such that

$$\sigma(a_1) = a_2$$
$$\sigma(a_2) = a_3$$
$$\vdots$$
$$\sigma(a_k) = a_1$$

and $\sigma(x) = x$ for all other elements $x \in X$. We will write $(a_1, a_2, \ldots, a_k)$ to denote the cycle σ. Cycles are the building blocks of all permutations.

Example 1.26

The permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (162354)$$

is a cycle of length 6, whereas

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix} = (243)$$

is a cycle of length 3.

Not every permutation is a cycle. Consider the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1243)(56).$$

This permutation actually contains a cycle of length 2 and a cycle of length 4.

Example 1.27

It is very easy to compute products of cycles. Suppose that

$$\sigma = (1352)$$

$$\tau = (256).$$

We can think of σ as

$$1 \mapsto 3$$

$$3 \mapsto 5$$

$$5 \mapsto 2$$

$$2 \mapsto 1$$

and τ as

$$2 \mapsto 5$$

$$5 \mapsto 6$$

$$6 \mapsto 2$$

Hence, $\sigma\tau = (1356)$. If $\mu = (1634)$, then $\sigma\mu = (1652)(34)$.

Two cycles in S_X, $\sigma = (a_1, a_2, \ldots, a_k)$ and $\tau = (b_1, b_2, \ldots, b_l)$, are ***disjoint*** if $a_i \neq b_j$ for all i and j.

Example 1.28

The cycles (135) and (27) are disjoint; however, the cycles (135) and (347) are not. Calculating their products, we find that

$$(135)(27) = (135)(27)$$

$$(135)(347) = (13475).$$

The product of two two cycles that are not disjoint may reduce to something less complicated; the product of disjoint cycles cannot be simplified.

Proposition 1.3

Let σ and τ be two disjoint cycles in S_X. Then $\sigma\tau = \tau\sigma$.

Theorem 1.15

Every permutation in S_n can be written as the product of disjoint cycles.

Example 1.29

Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix}.$$

Using cycle notation, we can write

$$\sigma = (1624)$$

$$\tau = (13)(456)$$

$$\sigma\tau = (136)(245)$$

$$\tau\sigma = (143)(256).$$

Remark 1.3

From this point forward we will find it convenient to use cycle notation to represent permutations. When using cycle notation, we often denote the identity permutation by (1).

1.6.3 Transpositions

The simplest permutation is a cycle of length 2. Such cycles are called ***transpositions***. Since

$$(a_1, a_2, \ldots, a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_3)(a_1 a_2),$$

any cycle can be written as the product of transpositions, leading to the following proposition.

Proposition 1.4

Any permutation of a finite set containing at least two elements can be written as the product of transpositions.

Example 1.30

Consider the permutation

$$(16)(253) = (16)(23)(25) = (16)(45)(23)(45)(25).$$

As we can see, there is no unique way to represent permutation as the product of transpositions. For instance, we can write the identity permutation as $(12)(12)$, as $(13)(24)(13)(24)$, and in many other ways. However, as it turns out, no permutation can be written as the product of both an even number of transpositions and an odd number of transpositions. For instance, we could represent the permutation (16) by

$$(23)(16)(23)$$

or by

$$(35)(16)(13)(16)(13)(35)(56),$$

but (16) will always be the product of an odd number of transpositions.

Lemma 1.2

If the identity is written as the product of r transpositions,

$$id = \tau_1\tau_2\cdots\tau_r,$$

then r is an even number.

Proof. We will employ induction on r. A transposition cannot be the identity; hence, $r > 1$. If $r = 2$, then we are done. Suppose that $r > 2$. In this case the product of the last two transpositions, $\tau_{r-1}\tau_r$, must be one of the following cases:

$$(ab)(ab) = id$$

$$(bc)(ab) = (ac)(bc)$$

$$(cd)(ab) = (ab)(cd)$$

$$(ac)(ab) = (ab)(bc),$$

where a, b, c, and d are distinct.

The first equation simply says that a transposition is its own inverse. If this case occurs, delete $\tau_{r-1}\tau_r$ from the product to obtain

$$id = \tau_1\tau_2 \cdots \tau_{r-3}\tau_{r-2}.$$

By induction $r-2$ is even; hence, r must be even.

In each of the other three cases, we can replace $\tau_{r-1}\tau_r$ with the right-hand side of the corresponding equation to obtain a new product of r transpositions for the identity. In this new product the last occurrence of a will be in the next-to-the-last transposition. We can continue this process with $\tau_{r-2}\tau_{r-1}$ to obtain either a product of $r-2$ transpositions or a new product of r transpositions where the last occurrence of a is in τ_{r-2}. If the identity is the product of $r-2$ transpositions, then again we are done, by our induction hypothesis; otherwise, we will repeat the procedure with $\tau_{r-3}\tau_{r-2}$.

At some point either we will have two adjacent, identical transpositions canceling each other out or a will be shuffled so that it will appear only in the first transposition. However, the latter case cannot occur, because the identity would not fix a in this instance. Therefore, the identity permutation must be the product of $r-2$ transpositions and, again by our induction hypothesis, we are done. □

Theorem 1.16

If a permutation σ can be expressed as the product of an even number of transpositions, then any other product of transpositions equaling σ must also contain an even number of transpositions. Similarly, if σ can be expressed as the product of an odd number of transpositions, then any other product of transpositions equaling σ must also contain an odd number of transpositions.

Proof. Suppose that

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_m = \tau_1\tau_2 \cdots \tau_n,$$

where m is even. We must show that n is also an even number. The inverse of σ^{-1} is $\sigma_m \cdots \sigma_1$. Since

$$\mathrm{id} = \sigma\sigma_m \cdots \sigma_1 = \tau_1 \cdots \tau_n \sigma_m \cdots \sigma_1,$$

n must be even by Lemma 1.2. □

In light of Theorem 1.16, we define a permutation to be ***even*** if it can be expressed as an even number of transpositions and ***odd*** if it can be expressed as an odd number of transpositions.

1.7 The Alternating Groups

One of the most important subgroups of S_n is the set of all even permutations, A_n. The group A_n is called the ***alternating group on n letters***.

Theorem 1.17

The set A_n is a subgroup of S_n.

Proof. Since the product of two even permutations must also be an even permutation, A_n is closed. The identity is an even permutation and therefore is in A_n. If σ is an even permutation, then

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_r,$$

where σ_i is a transposition and r is even. Since the inverse of any transposition is itself,

$$\sigma^{-1} = \sigma_r \sigma_{r-1} \cdots \sigma_1$$

is also in A_n. □ □

Proposition 1.5

The number of even permutations in S_n, $n \geqslant 2$, is equal to the number of odd permutations; hence, the order of A_n is $n!/2$.

Proof. Let A_n be the set of even permutations in S_n and B_n be the set of odd permutations. If

we can show that there is a bijection between these sets, they must contain the same number of elements. Fix a transposition σ in S_n. Since $n \geqslant 2$, such a σ exists. Define

$$\lambda_\sigma : A_n \to B_n$$

by

$$\lambda_\sigma(\tau) = \sigma\tau.$$

Suppose that $\lambda_\sigma(\tau) = \lambda_\sigma(\mu)$. Then $\sigma\tau = \sigma\mu$ and so

$$\tau = \sigma^{-1}\sigma\tau = \sigma^{-1}\sigma\mu = \mu.$$

Therefore, λ_σ is one-to-one. We will leave the proof that λ_σ is surjective to the reader. □

Example 1.31

The group A_4 is the subgroup of S_4 consisting of even permutations. There are twelve elements in A_4:

$$(1) \quad (12)(34) \quad (13)(24) \quad (14)(23)$$

$$(123) \quad (132) \quad (124) \quad (142)$$

$$(134) \quad (143) \quad (234) \quad (243).$$

1.8 The Dihedral Groups

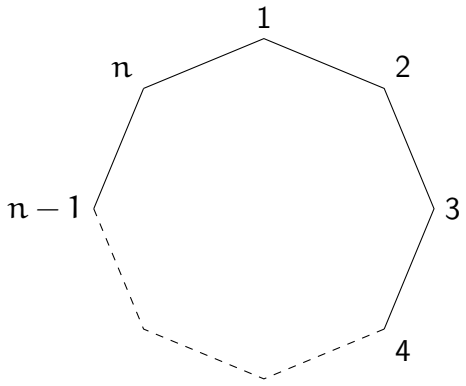


Fig. 1.1 . A regular n-gon

Another special type of permutation group is the dihedral group. Recall the symmetry group of an equilateral triangle. Such groups consist of the rigid motions of a regular n-sided polygon or n-gon. For $n = 3, 4, \ldots$, we define the ***nth dihedral group*** to be the group of rigid motions of a regular n-gon. We will denote this group by D_n. We can number the vertices of a regular n-gon by $1, 2, \ldots, n$ (Figure 1.1). Notice that there are exactly n choices to replace the first vertex. If we replace the first vertex by k, then the second vertex must be replaced either by vertex $k+1$ or by vertex $k-1$; hence, there are $2n$ possible rigid motions of the n-gon. We summarize these results in the following theorem.

Theorem 1.18

The dihedral group, D_n, is a subgroup of S_n of order $2n$.

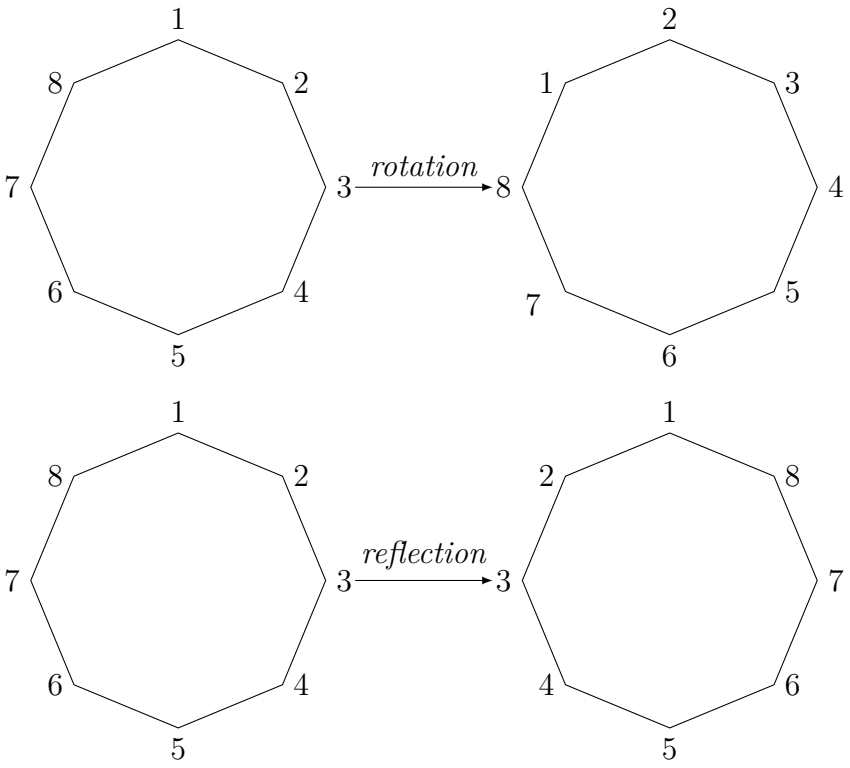


Fig. 1.2 . Rotations and reflections of a regular 8 -gon

Theorem 1.19

The group D_n, $n \geqslant 3$, consists of all products of the two elements r and s, satisfying the relations

$$r^n = id$$

$$s^2 = id$$

$$srs = r^{-1}.$$

Proof. The possible motions of a regular n-gon are either reflections or rotations (Figure 1.2). There are exactly n possible rotations:

$$\mathrm{id}, \frac{360^\circ}{n}, 2 \cdot \frac{360^\circ}{n}, \ldots, (n-1) \cdot \frac{360^\circ}{n}.$$

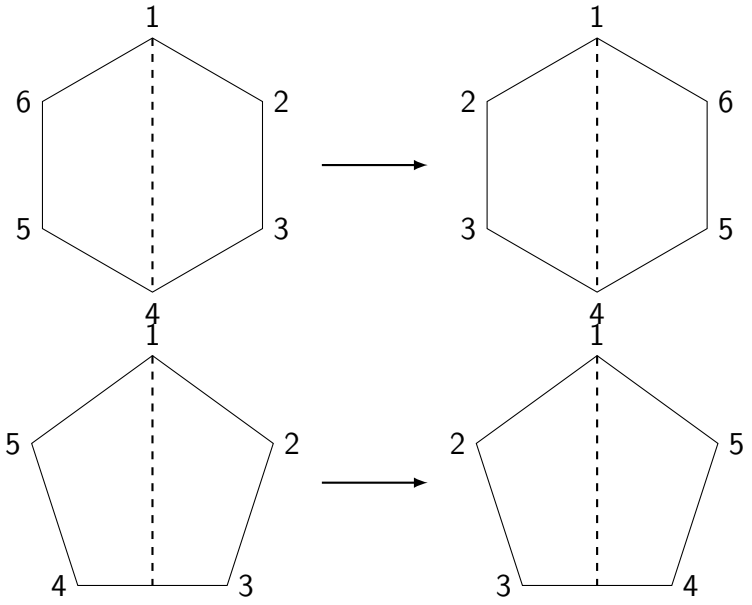


Fig. 1.3 . Types of reflections of a regular 5-gon

We will denote the rotation $360^\circ/n$ by r. The rotation r generates all of the other rotations. That is,

$$r^k = k \cdot \frac{360^\circ}{n}.$$

Label the n reflections $s_1, s_2, \ldots, s_n$, where s_k is the reflection that leaves vertex k fixed. There are two cases of reflection, depending on whether n is even or odd. If there are an even number of vertices, then 2 vertices are left fixed by a reflection. If there are an odd number of vertices, then only a single vertex is left fixed by a reflection (Figure ??). In either case, the order of s_k is two. Let $s = s_1$. Then $s^2 = \mathrm{id}$ and $r^n = \mathrm{id}$. Since any rigid motion t of the n-gon replaces the first vertex by the vertex k, the second vertex must be replaced by either $k+1$ or by $k-1$. If the second vertex is replaced by $k+1$, then $t = r^{k-1}$. If it is replaced by $k-1$, then $t = r^{k-1}s$. Hence, r and s generate D_n; that is, D_n consists of all finite products of r and s. We will leave the proof that $srs = r^{-1}$ as an exercise. □

Example 1.32

The group of rigid motions of a square, D_4, consists of eight elements. With the vertices numbered $1, 2, 3, 4$ (Figure 1.4), the rotations

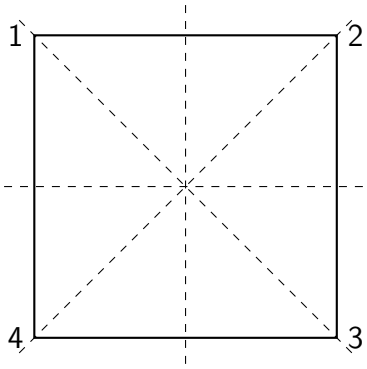


Fig. 1.4 . The group D_4

are

$$r = (1234)$$
$$r^2 = (13)(24)$$
$$r^3 = (1432)$$
$$r^4 = id$$

and the reflections are

$$s_1 = (24)$$
$$s_2 = (13).$$

The order of D_4 is 8. The remaining two elements are

$$rs_1 = (12)(34)$$
$$r^3s_1 = (14)(23).$$

1.9 The Motion Group of a Cube

We can investigate the groups of rigid motions of geometric objects other than a regular n-sided polygon to obtain interesting examples of permutation groups. Let us consider the group of rigid motions of a cube. One of the first questions that we can ask about this group is "what is its order?" A cube has 6 sides. If a particular side is facing upward, then there are four possible

rotations of the cube that will preserve the upward-facing side. Hence, the order of the group is $6 \cdot 4 = 24$. We have just proved the following proposition.

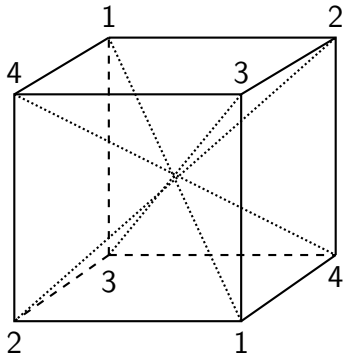


Fig. 1.5 . The motion group of a cube

Proposition 1.6

The group of rigid motions of a cube contains 24 elements.

Theorem 1.20

The group of rigid motions of a cube is S_4.

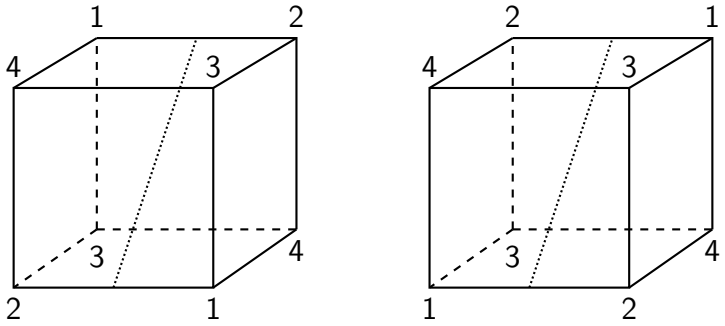


Fig. 1.6 . Transpositions in the motion group of a cube

Proof. From Proposition 1.6, we already know that the motion group of the cube has 24 elements, the same number of elements as there are in S_4. There are exactly four diagonals in the cube. If we label these diagonals 1, 2, 3, and 4, we must show that the motion group of the cube will give us any permutation of the diagonals (Figure 1.5). If we can obtain all of these permutations, then S_4 and the group of rigid motions of the cube must be the same. To obtain a transposition we can rotate the cube 180° about the axis joining the midpoints of opposite edges (Figure 1.6). There are six such axes, giving all transpositions in S_4. Since every element in S_4 is the product of a finite number of transpositions, the motion group of a cube must be S_4. □

CHAPTER 2

Geometric Symmetry

2.1 Isometries of a Euclidean Space

2.1.1 Orthogonal Matrices

Definition 2.1 (Orthogonal matrix)

We say that a matrix $A \in \mathscr{M}_n(\mathbb{R})$ is orthogonal if it satisfies the relation $A^T A = I_n$.

Remark 2.1

1. The definition amounts to saying that the columns (or rows) of A form an orthonormal basis of $\mathbb{R}^n$.

2. By definition, an orthogonal matrix A is invertible and we have $A^{-1} = A^T$.

Definition 2.2 (Orthogonal group of order n)

The orthogonal group of order n is the set of orthogonal matrices of $\mathscr{M}_n(\mathbb{R})$. It is denoted by $O_n(\mathbb{R})$ or $O(n)$.

Example 2.1

Here are some examples of orthogonal matrices

$$\frac{1}{2}\begin{pmatrix} \sqrt{2} & -\sqrt{2} \\ \sqrt{2} & \sqrt{2} \end{pmatrix} \in O_2(\mathbb{R}), \quad \frac{1}{3}\begin{pmatrix} 2 & 2 & 1 \\ 1 & -2 & 2 \\ 2 & -1 & -2 \end{pmatrix} \in O_3(\mathbb{R})$$

Theorem 2.1

The set $O_n(\mathbb{R})$ is a group, i.e.

(i) The matrix I_n belongs to $O_n(\mathbb{R})$,

(ii) For all $A \in O_n(\mathbb{R})$, we have $A^{-1} \in O_n(\mathbb{R})$,

(iii) For all $(A, B) \in O_n(\mathbb{R})^2$, we have $AB \in O_n(\mathbb{R})$.

Proposition 2.1

Let $\mathscr{B}$ be an orthonormal basis of E. A basis $\mathscr{C}$ of E is orthonormal if and only if the change-of-basis matrix $P_{\mathscr{B}}^{\mathscr{C}}$ is orthogonal.

I.B - Positive and negative orthogonal matrices

Proposition 2.2

If $A \in O_n(\mathbb{R})$, then $\det(A) = \pm 1$.

Definition 2.3 (Positive or negative orthogonal matrix)

An orthogonal matrix $A \in O_n(\mathbb{R})$ is said to be positive (or direct) if $\det(A) = 1$. Otherwise, it is said to be negative (or indirect).

Definition 2.4 (Special orthogonal group of order n)

The special orthogonal group of order n is the set of positive orthogonal matrices of $\mathscr{M}_n(\mathbb{R})$. It is denoted by $SO_n(\mathbb{R})$ or $SO(n)$.

Remark 2.2

Theorem 1 remains valid if we replace $O_n(\mathbb{R})$ with $SO_n(\mathbb{R})$.

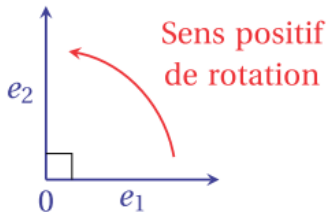
2.1.2 Orientation of the Euclidean space

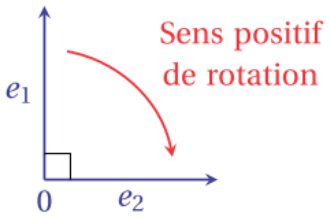
Definition 2.5 (Oriented Euclidean space)

An oriented Euclidean space is a Euclidean space in which an orthonormal basis $\mathscr{C}$ of E has been chosen.

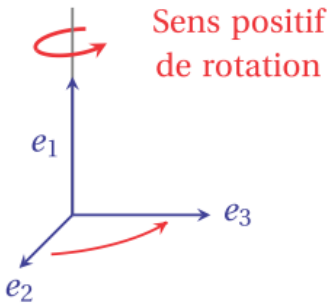
Remark 2.3

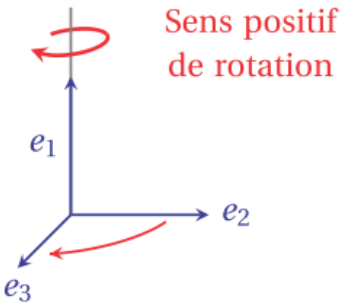
In other words, to orient a Euclidean space, we choose an orthonormal basis of it. In the plane, choosing an orientation amounts to choosing a positive direction of rotation of the plane.





In space, choosing an orientation amounts to choosing a positive direction of rotation around the half-line directed by the first vector of an orthonormal basis.





It can be observed that there are only two possible orientations for a Euclidean space.

Definition 2.6 (Direct and indirect basis)

Let E be a Euclidean space oriented by an orthonormal basis $\mathscr{C}$. An orthonormal basis $\mathscr{B}$ of E is said to be

1. direct if the change-of-basis matrix from $\mathscr{C}$ to $\mathscr{B}$ has determinant 1.
2. indirect if the change-of-basis matrix from $\mathscr{C}$ to $\mathscr{B}$ has determinant -1.

Example 2.2

If the space $\mathbb{R}^3$ is oriented by the standard basis (i, j, k), then the bases (i, j, k), (j, k, i) and (k, i, j) are direct, while the bases (i, k, j), (k, j, i) and (j, i, k) are indirect.

2.2 Linear isometries

2.2.1 General properties

Definition 2.7 (Linear isometry)

An endomorphism $\varphi \in \mathscr{L}(E)$ is a linear isometry if φ preserves the norm of vectors, i.e.

$$\forall x \in E, \quad \|\varphi(x)\| = \|x\|.$$

Example 2.3

The maps $\pm \mathrm{Id}_E \in \mathscr{L}(E)$ are linear isometries.

Definition 2.8 (Orthogonal group of a Euclidean space)

The orthogonal group of the Euclidean space E, denoted by $O(E)$, is the set of linear isometries of E.

Theorem 2.2

The set $O(E)$ is a group, i.e.

(i) The endomorphism Id_E belongs to $O(E)$,

(ii) For all $u \in O(E)$, the endomorphism u is an isomorphism and $u^{-1} \in O(E)$,

(iii) For all $(u, v) \in O(E)^2$, we have $u \circ v \in O(E)$.

Theorem 2.3 (Characterization theorem of linear isometries)

Let $\varphi \in \mathscr{L}(E)$. The following assertions are equivalent.

(i) The map φ is a linear isometry.

(ii) The map φ preserves the inner product, i.e.

$$\forall (x, y) \in E^2, \quad (\varphi(x) \mid \varphi(y)) = (x \mid y).$$

(iii) The image of an orthonormal basis of E under φ is an orthonormal basis.

(iv) The image of any orthonormal basis of E under φ is an orthonormal basis.

Proposition 2.3

Let $\mathscr{B}$ be an orthonormal basis of E and $u \in \mathscr{L}(E)$. The endomorphism u is a linear isometry if and only if the matrix $\mathrm{Mat}_{\mathscr{B}}(u)$ is orthogonal.

Remark 2.4

Thus, once an orthonormal basis of E has been fixed, the elements of $O(E)$ correspond bijectively with the elements of $O_n(\mathbb{R})$.

Proposition 2.4

If a vector subspace F of E is stable under a linear isometry $u \in \mathscr{L}(E)$, then $F^\perp$ is stable under u.

2.2.2 Positive and negative linear isometries

Proposition 2.5

If $u \in O(E)$, then $\det(u) = \pm 1$.

Definition 2.9 (Positive or negative linear isometry)

A linear isometry $u \in O(E)$ is said to be positive (or direct) if $\det(u) = 1$. Otherwise, it is said to be negative (or indirect).

Definition 2.10 (Special orthogonal group of a Euclidean space)

The special orthogonal group of the Euclidean space E is the set of positive linear isometries of E. It is denoted by $SO(E)$.

Remark 2.5

Theorem 2.2 remains valid if we replace $O(E)$ with $SO(E)$.

2.2.3 Orthogonal symmetries

Definition 2.11 (Orthogonal symmetry)

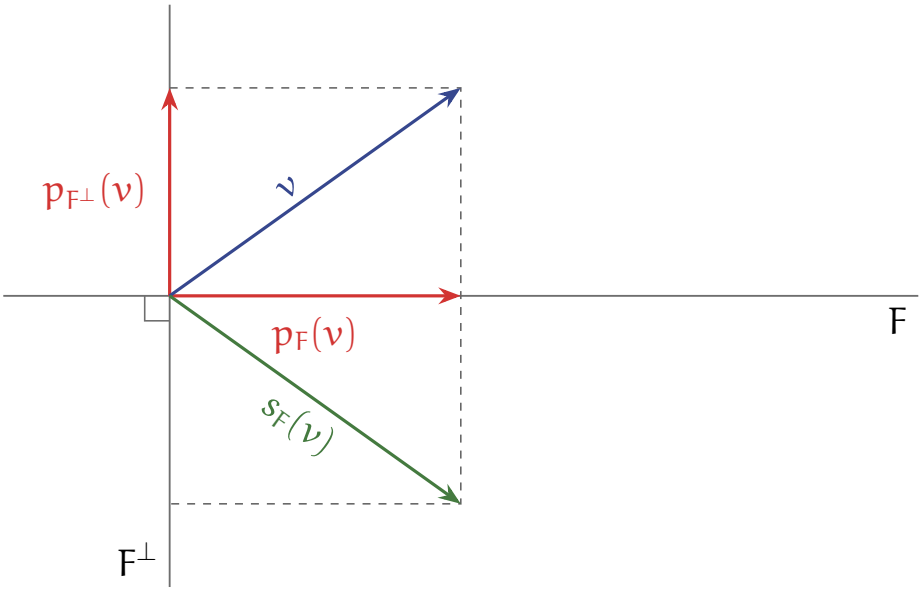
Let F be a vector subspace of E. The orthogonal symmetry with respect to F is the symmetry $s_F : E \to E$ with respect to F and parallel to $F^\perp$.

Remark 2.6

We have $s_F = p_F - p_{F^\perp} = 2p_F - \mathrm{Id}_E$.

Illustration

We can represent the orthogonal symmetry of a vector with the diagram below.



Example 2.4

In the previous chapter, we saw that the orthogonal projection onto

$$H = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\}$$

in $\mathbb{R}^3$ is defined by

$$p_H(x,y,z) = \left(\frac{2x-y-z}{3}, \frac{-x+2y-z}{3}, \frac{-x-y+2z}{3}\right).$$

From this we deduce that

$$s_H(x,y,z) = \left(\frac{x-2y-2z}{3}, \frac{-2x+y-2z}{3}, \frac{-2x-2y+z}{3}\right).$$

Proposition 2.6

Orthogonal symmetries are linear isometries.

Definition 2.12 (Reflection)

A reflection is an orthogonal symmetry with respect to a hyperplane.

2.3 Classification of linear isometries

2.3.1 Linear isometries of a Euclidean plane

In this part, we assume that E is a Euclidean plane oriented by an orthonormal basis $\mathscr{C} = (i,j)$.

Proposition 2.7

Let $u \in SO(E)$ be a positive isometry. There exists a real number $\theta \in \mathbb{R}$ such that for any direct orthonormal basis $\mathscr{B}$ of E, we have

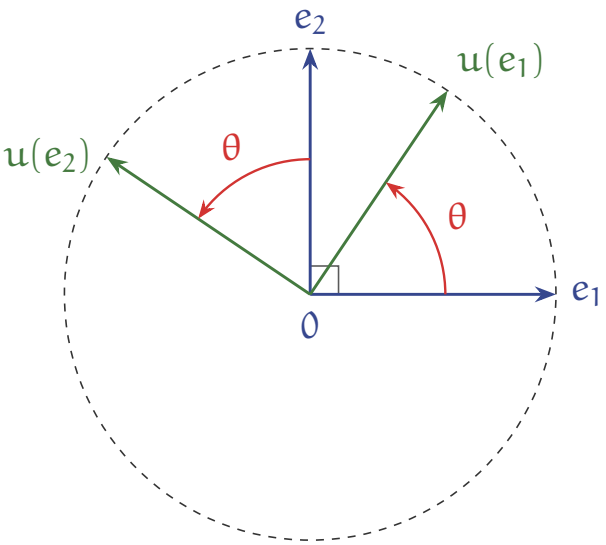
$$\mathrm{Mat}_{\mathscr{B}}(u) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

Illustration

If $\mathscr{B} = (e_1, e_2)$, we have by definition the relations

$$\begin{cases} u(e_1) &= \cos(\theta)e_1 + \sin(\theta)e_2 \\ u(e_2) &= -\sin(\theta)e_1 + \cos(\theta)e_2 \end{cases}$$

From this we deduce that u is a rotation of angle θ.



Remark 2.7

In particular, we verify in the proof that

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \in \mathscr{M}_2(\mathbb{R}) \;\middle|\; \theta \in \mathbb{R} \right\}.$$

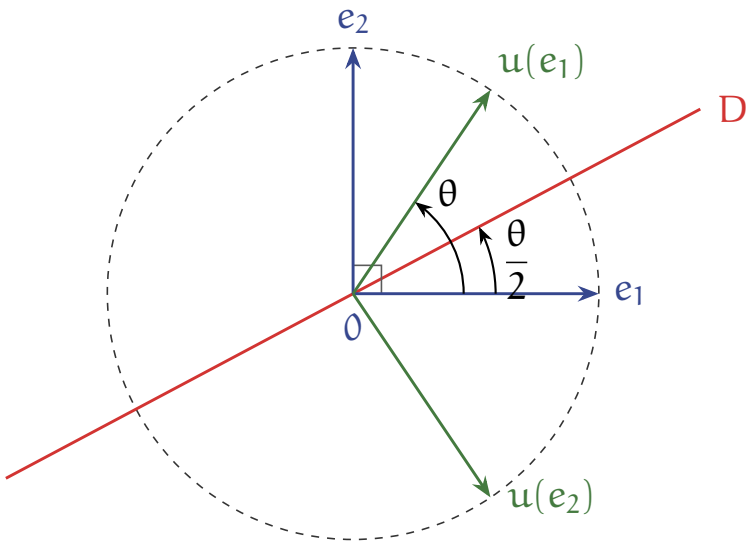
Proposition 2.8

Let $u \in \mathrm{O}(E) \setminus \mathrm{SO}(E)$ be a negative isometry. For any direct orthonormal basis $\mathscr{B}$ of E, there exists a real number $\theta \in \mathbb{R}$ such that

$$\mathrm{Mat}_{\mathscr{B}}(u) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}.$$

Illustration

As in the previous case, denoting $\mathscr{B} = (e_1, e_2)$, we can represent the situation on the graph below. From this we deduce that u is a reflection whose axis D is rotated by $\frac{\theta}{2}$ with respect to the line $\mathrm{Vect}(e_1)$.



Remark 2.8

In particular, we verify in the proof that

$$O_2(\mathbb{R}) \setminus SO_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix} \in \mathscr{M}_2(\mathbb{R}) \;\middle|\; \theta \in \mathbb{R} \right\}.$$

Remark 2.9

If we change the orientation of the plan chosen at the beginning, the real number θ is replaced by its opposite in the two preceding propositions. (Changing the orientation amounts to changing the chosen positive direction of rotation).

Conclusion

When E is a Euclidean plane, then

1. the elements of SO(E) are rotations;

2. the elements of $O(E) \setminus SO(E)$ are reflections.

2.3.2 Linear isometries in dimension 3

In this part, we assume that E is a Euclidean space of dimension 3 oriented by an orthonormal basis $\mathscr{C} = (i, j, k)$.

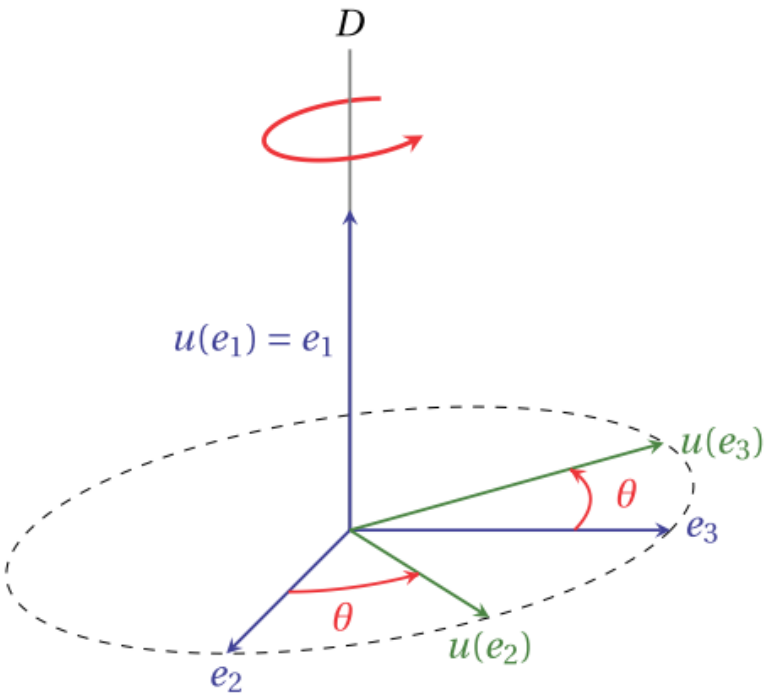
Proposition 2.9

Let $u \in SO(E)$ be a positive isometry. There exists a real number $\theta \in \mathbb{R}$ and a direct orthonormal basis $\mathscr{B}$ of E such that

$$\mathrm{Mat}_{\mathscr{B}}(u) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

Illustration

Denoting $\mathscr{B} = (e_1, e_2, e_3)$, we deduce that u is the rotation of axis D directed by the vector e_1 and of angle θ.



Proposition 2.10

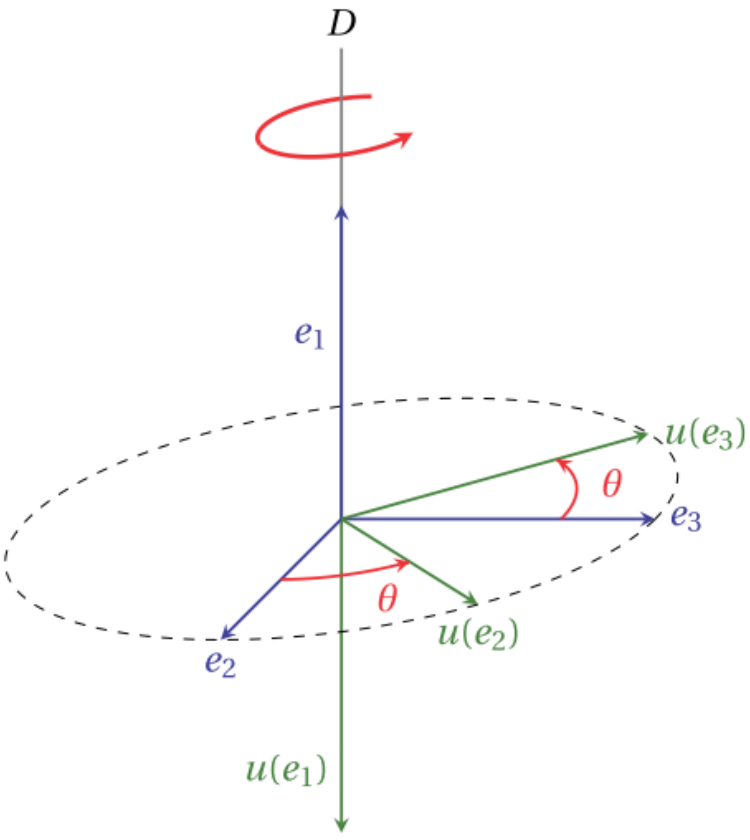
Let $u \in O(E) \setminus SO(E)$ be a negative isometry. There exists a real number $\theta \in \mathbb{R}$ and a direct orthonormal basis $\mathscr{B}$ of E such that

$$\mathrm{Mat}_{\mathscr{B}}(u) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

Illustration

Denoting $\mathscr{B} = (e_1, e_2, e_3)$, we deduce that the isometry u is the commutative composition between:

- the rotation of axis D directed by e_1 and of angle θ;
- the reflection with respect to the plane $D^{\perp} = \mathrm{Vect}(e_2, e_3)$.



Remark 2.10

In the case where the angle θ of the rotation is zero, the negative isometry u is simply the reflection with respect to the plane $D^{\perp} = \mathrm{Vect}(e_2, e_3)$.

2.4 Reduction of real symmetric matrices

Proposition 2.11

The eigenspaces of a real symmetric matrix are pairwise orthogonal for the standard inner product of $\mathbb{R}^n$.

Example 2.5

The eigenspaces of the real symmetric matrix

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

are

$$E_0 = \mathrm{Vect}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad \text{and} \quad E_2 = \mathrm{Vect}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

which are indeed orthogonal.

Theorem 2.4 (Spectral theorem)

Let $A \in \mathscr{M}_n(\mathbb{R})$ be a real symmetric matrix. There exist a diagonal matrix $D \in \mathscr{M}_n(\mathbb{R})$ and an orthogonal matrix $P \in O_n(\mathbb{R})$ such that

$$A = PDP^{-1} = PDP^{T}.$$

Remark 2.11

In other words, a real symmetric matrix is diagonalizable, has real eigenvalues, and the change-of-basis matrix can be chosen in $O_n(\mathbb{R})$.

WARNING

If the matrix A is symmetric with non-real coefficients, then it is not necessarily diagonalizable. For example, the matrix

$$A = \begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix} \in \mathscr{M}_2(\mathbb{C})$$

is symmetric, but it is not diagonalizable.

2.5 Methods

2.5.1 Studying a linear isometry in dimension 3

In this part, we assume that E is a 3-dimensional Euclidean space oriented by an orthonormal basis $\mathscr{C} = (i, j, k)$. We wish to study an element $u \in O(E)$. We begin by determining whether u is a positive or negative isometry by calculating its determinant.

2.5.1.1 Positive isometry

According to the course, we know that there exists a real number $\theta \in \mathbb{R}$ and a direct orthonormal basis $\mathscr{B} = (e_1, e_2, e_3)$ of E such that

$$\mathrm{Mat}_{\mathscr{B}}(u) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

The endomorphism u is the rotation of axis D directed by e_1 and of angle θ. The method below allows us to determine its characteristics.

Method: Study of a positive isometry of space

We assume that $u \neq \mathrm{Id}_E$ (otherwise $u = \mathrm{Id}_E$ and there is no study to be done).

1. We determine the axis D by using $D = E_1(u) = \mathrm{Ker}(\mathrm{Id}_E - u)$. We fix a unit vector e_1 in D.

2. To determine the angle $\theta \in \mathbb{R}$ of the rotation, we use the relation

$$\mathrm{Tr}(u) = 1 + 2\cos(\theta) \iff \cos(\theta) = \frac{\mathrm{Tr}(u) - 1}{2}.$$

   We deduce θ by using the fact that the sign of $\sin(\theta)$ is the same as that of the number $\det_{\mathscr{C}}(e_1, x, u(x))$ where $x \in E \setminus D$ is any vector.

3. To determine the vectors e_2 and e_3, we choose a unit vector e_2 orthogonal to e_1, and then we set $e_3 = e_1 \wedge e_2$.

Example 2.6

Let $u \in O(E)$ whose matrix in $\mathscr{C} = (i, j, k)$ is

$$A = \frac{1}{4}\begin{pmatrix} 3 & 1 & \sqrt{6} \\ 1 & 3 & -\sqrt{6} \\ -\sqrt{6} & \sqrt{6} & 2 \end{pmatrix}.$$

We will determine the characteristic elements of this isometry. We check that $\det(u) = \det(A) = 1$, so u is a positive isometry.

1. We obtain by calculation that $D = E_1(u) = \mathrm{Ker}(\mathrm{Id}_E - u) = \mathrm{Vect}(i + j)$, so we set

$$e_1 = \frac{1}{\sqrt{2}}(i + j).$$

2. If $\theta \in \mathbb{R}$ is the angle of the rotation u, we have

$$\mathrm{Tr}(u) = 1 + 2\cos(\theta) \iff \cos(\theta) = \frac{\mathrm{Tr}(u) - 1}{2} = \frac{2 - 1}{2} = \frac{1}{2}.$$

Moreover, we know that the number $\sin(\theta)$ has the same sign as

$$\det_{\mathscr{C}}(e_1, j, u(j)) = \frac{1}{4\sqrt{2}} \begin{vmatrix} 1 & 0 & 1 \\ 1 & 1 & 3 \\ 0 & 0 & \sqrt{6} \end{vmatrix} = \frac{\sqrt{3}}{4} > 0,$$

therefore u is the rotation of axis D directed by $i + j$ and of angle $\frac{\pi}{3}$.

3. If we wish to determine a direct orthonormal basis $\mathscr{B}$ adapted to the isometry u, we can take $e_2 = k$ which is orthogonal to e_1 and

$$e_3 = e_1 \wedge e_2 = \frac{1}{\sqrt{2}}(i - j).$$

2.5.1.2 Negative isometry

According to the course, we know that there exists a real number $\theta \in \mathbb{R}$ and a direct orthonormal basis $\mathscr{B} = (e_1, e_2, e_3)$ of E such that

$$\mathrm{Mat}_{\mathscr{B}}(u) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

The endomorphism u is the commutative composition between:

- the rotation of axis D directed by e_1 and of angle θ;
- the reflection with respect to the plane $D^{\perp} = \mathrm{Vect}(e_2, e_3)$.

The method below allows us to determine its characteristics.

Method: Study of a negative isometry of space

We assume that $u \neq -\mathrm{Id}_E$ (otherwise $u = -\mathrm{Id}_E$ and there is no study to be done).

1. We determine the axis D by using $D = E_{-1}(u) = \mathrm{Ker}(-\mathrm{Id}_E - u)$. We fix a unit vector e_1 in D.

2. To determine the angle $\theta \in \mathbb{R}$ of the rotation, we use the relation

$$\mathrm{Tr}(u) = -1 + 2\cos(\theta) \iff \cos(\theta) = \frac{\mathrm{Tr}(u)+1}{2}.$$

We deduce θ by using the fact that the sign of $\sin(\theta)$ is the same as that of the number $\det_{\mathscr{C}}(e_1, x, u(x))$ where $x \in E \setminus D$ is any vector.

3. To determine the vectors e_2 and e_3, we choose a unit vector e_2 orthogonal to e_1, and then we set $e_3 = e_1 \wedge e_2$.

Example 2.7

Let $u \in O(E)$ whose matrix in $\mathscr{C} = (i, j, k)$ is

$$A = \frac{1}{9}\begin{pmatrix} 7 & 4 & 4 \\ -4 & 8 & -1 \\ 4 & 1 & -8 \end{pmatrix}.$$

We check that $\det(u) = \det(A) = -1$, so u is a negative isometry.

1. We obtain by calculation that $D = E_{-1}(u) = \mathrm{Ker}(-\mathrm{Id}_E - u) = \mathrm{Vect}(i - 4k)$, so we set

$$e_1 = \frac{1}{\sqrt{17}}(i - 4k).$$

2. If $\theta \in \mathbb{R}$ is the angle of the rotation, we have

$$\mathrm{Tr}(u) = -1 + 2\cos(\theta) \iff \cos(\theta) = \frac{\mathrm{Tr}(u)+1}{2} = \frac{7/9+1}{2} = \frac{8}{9}.$$

Moreover, we know that the number $\sin(\theta)$ has the same sign as

$$\det_{\mathscr{C}}(e_1, i, u(i)) = \frac{1}{9\sqrt{17}} \begin{vmatrix} 1 & 1 & 7 \\ 0 & 0 & -4 \\ -4 & 0 & 4 \end{vmatrix} = \frac{16}{9\sqrt{17}} > 0,$$

therefore u is the commutative composition between:

- the rotation of axis D directed by $i - 4k$ and of angle $\text{Arccos}(8/9)$;
- the reflection with respect to the plane $D^{\perp} = \text{Vect}(j, 4i + k)$.

3. If we wish to determine a direct orthonormal basis $\mathscr{B}$ adapted to the isometry u, we can take $e_2 = j$ which is orthogonal to e_1 and

$$e_3 = e_1 \wedge e_2 = \frac{1}{\sqrt{17}}(4i + k).$$

2.5.2 Diagonalizing a real symmetric matrix

We consider a real symmetric matrix $A \in \mathscr{M}_n(\mathbb{R})$ that we wish to diagonalize such that the change-of-basis matrix P is orthogonal.

2.5.2.1 Method: Determining the orthogonal change-of-basis matrix

1. We determine the eigenspaces of A.
2. We construct orthonormal bases for each of the eigenspaces (using, for example, the Gram-Schmidt algorithm).
3. The matrix P is the matrix whose columns are the vectors of the found orthonormal bases.

Example 2.8

We will diagonalize the real symmetric matrix below with an orthogonal change-of-basis matrix.

$$A = \begin{pmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{pmatrix}.$$

The characteristic polynomial of A is

$$\chi_A(x) = (x+3)(x-3)^2.$$

The eigenspaces of the matrix A are

$$E_3(A) = \text{Vect}\left(\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}\right) \quad \text{and} \quad E_{-3}(A) = \text{Vect}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

By applying the Gram-Schmidt algorithm to the basis of $E_3(A)$ above, we deduce that an orthonormal basis of $E_3(A)$ is

$$\left(\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{6}}\begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix}\right).$$

By normalizing the vector in the basis of $E_{-3}(A)$ above, we obtain an orthonormal basis of

$E_{-3}(A)$ with the vector

$$\frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\1\end{pmatrix}.$$

We therefore have $A = PDP^{-1}$ with

$$D = \begin{pmatrix}3&0&0\\0&3&0\\0&0&-3\end{pmatrix}, \quad P = \frac{1}{\sqrt{6}}\begin{pmatrix}\sqrt{3}&1&\sqrt{2}\\-\sqrt{3}&1&\sqrt{2}\\0&-2&\sqrt{2}\end{pmatrix}.$$

Furthermore, by construction we have $P \in O_3(\mathbb{R})$, so

$$P^{-1} = P^T = \frac{1}{\sqrt{6}}\begin{pmatrix}\sqrt{3}&-\sqrt{3}&0\\1&1&-2\\\sqrt{2}&\sqrt{2}&\sqrt{2}\end{pmatrix}.$$

2.5.3 Studying a conic section

We place ourselves in a plane $\mathscr{P}$ equipped with an orthonormal coordinate system (O, i, j).

Definition 2.13 (Conic section)

A conic section in $\mathscr{P}$ is the set of points $M(x, y)$ satisfying an equation of the form

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

where $(a, b, c, d, e, f) \in \mathbb{R}^6$ satisfies $(a, b, c) \neq (0, 0, 0)$.

Proposition 2.12

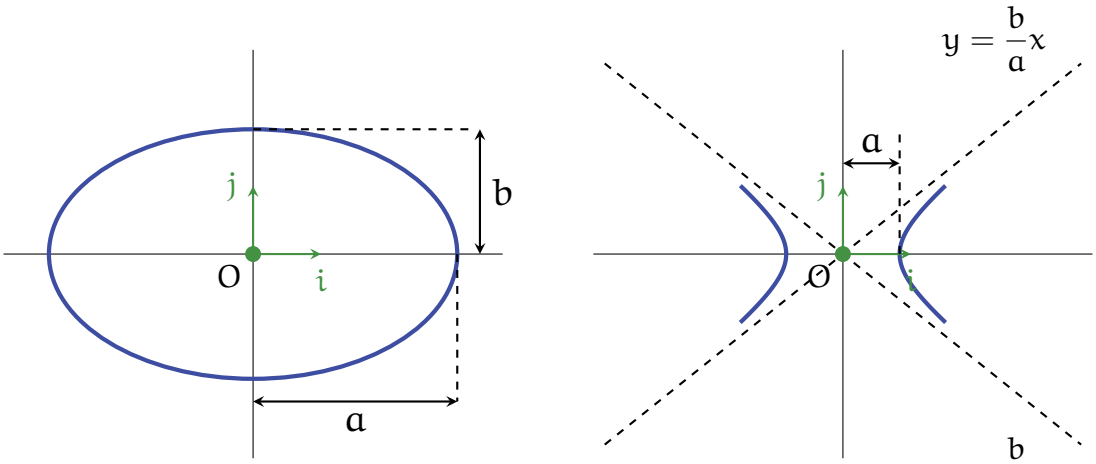
Let $(a, b) \in \mathbb{R}^2$ with $a > 0$ and $b > 0$.

(i) The conic section having the equation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ is an ellipse whose center is the origin.

(ii) The conic section having the equation $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ is a hyperbola whose center is the origin.

Illustration

We can represent the two conic sections from the proposition.



Ellipse d'équation $\left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 = 1$

Hyperbole d'équation $\left(\frac{x}{a}\right)^2 - \left(\frac{y}{b}\right)^2 = 1$

Method: Studying a conic section

We consider a conic section of $\mathscr{P}$ whose equation is

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

1. We put the equation into matrix form

$$\begin{pmatrix} x & y \end{pmatrix} \underbrace{\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}}_{A} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} d & e \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + f = 0.$$

2. Since the matrix A is real symmetric, we can determine an orthogonal matrix $P \in O_2(\mathbb{R})$ and a diagonal matrix D such that $D = P^{-1}AP$.

3. We determine the equation of the conic section in the coordinate system (O, e_1, e_2) where (e_1, e_2) is the orthonormal basis of eigenvectors that has just been calculated. To do this, we perform the change of variable

$$\begin{pmatrix} x \\ y \end{pmatrix} = P \begin{pmatrix} u \\ v \end{pmatrix} \quad \underset{\text{Transposition}}{\Longleftrightarrow} \quad \begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} u & v \end{pmatrix} P^T$$

in the initial equation. We thus obtain a simple equation in the new orthonormal coordinate system (O, e_1, e_2) which allows us to identify the conic section.

Example 2.9

We wish to study the conic section $\mathscr{C}_1$ of $\mathscr{P}$ whose equation is

$$3x^2 - 2xy + 3y^2 - 8x + 8y + 6 = 0.$$

We begin by rewriting this equation in matrix form:

$$\begin{pmatrix} x & y \end{pmatrix} \underbrace{\begin{pmatrix} 3 & -1 \\ -1 & 3 \end{pmatrix}}_{A} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} -8 & 8 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + 6 = 0.$$

Since the matrix A is real symmetric, we can apply the diagonalization method seen in the previous section. We find that the eigenvalues of A are 2 and 4 and that the respective

associated eigenspaces are

$$E_2(A) = \text{Vect}\begin{pmatrix} 1 \\ \\ 1 \end{pmatrix} \quad \text{and} \quad E_4(A) = \text{Vect}\begin{pmatrix} -1 \\ \\ 1 \end{pmatrix}.$$

Thus, we can write $D = P^{-1}AP$ with the matrices

$$D = \begin{pmatrix} 2 & 0 \\ \\ 0 & 4 \end{pmatrix} \quad \text{and} \quad P = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ \\ 1 & 1 \end{pmatrix} \in O_2(\mathbb{R}).$$

We therefore define the vectors

$$e_1 = \frac{1}{\sqrt{2}}(i + j) \quad \text{and} \quad e_2 = \frac{1}{\sqrt{2}}(-i + j).$$

To obtain the equation of the conic section in the coordinate system (O, e_1, e_2), we perform the change of variable

$$\begin{pmatrix} x \\ \\ y \end{pmatrix} = P\begin{pmatrix} u \\ \\ v \end{pmatrix}$$

in the equation of the conic section. We obtain:

$$\begin{pmatrix} x & y \end{pmatrix} A \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} -8 & 8 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + 6 = 0$$

$$\iff \begin{pmatrix} u & v \end{pmatrix} P^T A P \begin{pmatrix} u \\ v \end{pmatrix} + \begin{pmatrix} -8 & 8 \end{pmatrix} P \begin{pmatrix} u \\ v \end{pmatrix} + 6 = 0$$

$$\iff \begin{pmatrix} u & v \end{pmatrix} D \begin{pmatrix} u \\ v \end{pmatrix} + \begin{pmatrix} 0 & 8\sqrt{2} \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} + 6 = 0$$

$$\iff 2u^2 + 4v^2 + 8\sqrt{2}v + 6 = 0$$

$$\iff u^2 + 2(v + \sqrt{2})^2 = 1.$$

Thus the studied conic section is an ellipse. Its center Ω has coordinates $(0, -\sqrt{2})$ in the coordinate system (O, e_1, e_2), hence $(1, -1)$ in the coordinate system (O, i, j).

We can sketch the conic section $\mathscr{C}_1$ by using its equation in the coordinate system (O, e_1, e_2).

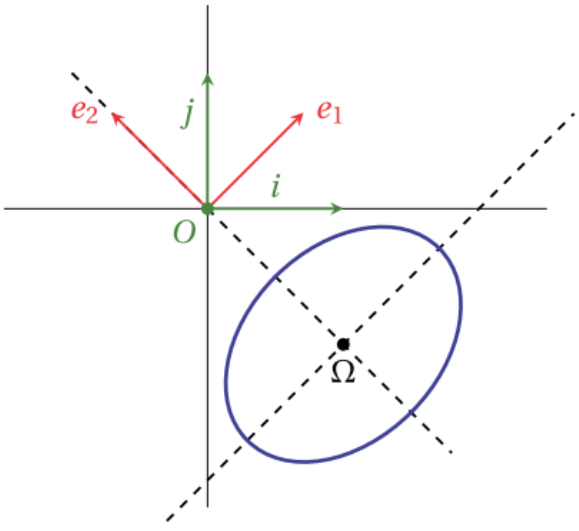


Fig. 2.1 . La conique $\mathscr{C}$

Example 2.10

We wish to study the conic section $\mathscr{C}_2$ of $\mathscr{P}$ whose equation is

$$16x^2 - 24xy + 9y^2 + 25x - 50y = 0.$$

We begin by rewriting this equation in matrix form:

$$\begin{pmatrix} x & y \end{pmatrix} \underbrace{\begin{pmatrix} 16 & -12 \\ -12 & 9 \end{pmatrix}}_{A} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 25 & -50 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 0.$$

The eigenvalues of A are 0 and 25 and the respective associated eigenspaces are

$$E_0(A) = \text{Vect} \begin{pmatrix} 3 \\ 4 \end{pmatrix} \quad \text{and} \quad E_{25}(A) = \text{Vect} \begin{pmatrix} -4 \\ 3 \end{pmatrix}.$$

Thus, we can write $D = P^{-1}AP$ with the matrices

$$D = \begin{pmatrix} 0 & 0 \\ 0 & 25 \end{pmatrix} \quad \text{and} \quad P = \frac{1}{5} \begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix} \in O_2(\mathbb{R}).$$

On we define the vectors

$$e_1 = \frac{1}{5}(3i + 4j) \quad \text{and} \quad e_2 = \frac{1}{5}(-4i + 3j).$$

To obtain the equation of the conic section in the coordinate system (O, e_1, e_2), we perform the change of variable

$$\begin{pmatrix} x \\ y \end{pmatrix} = P \begin{pmatrix} u \\ v \end{pmatrix}$$

in the equation of the conic section. We obtain:

$$\begin{pmatrix} x & y \end{pmatrix} A \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 25 & -50 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 0$$

$$\iff \begin{pmatrix} u & v \end{pmatrix} P^T A P \begin{pmatrix} u \\ v \end{pmatrix} + \begin{pmatrix} 25 & -50 \end{pmatrix} P \begin{pmatrix} u \\ v \end{pmatrix} = 0$$

$$\iff \begin{pmatrix} u & v \end{pmatrix} D \begin{pmatrix} u \\ v \end{pmatrix} + \begin{pmatrix} -25 & -50 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = 0$$

$$\iff 25v^2 - 25u - 50v = 0$$

$$\iff u = v^2 - 2v.$$

Thus the studied conic section is a parabola. Its vertex S has coordinates $(-1, 1)$ in the coordinate system (O, e_1, e_2), hence $(-7/5, -1/5)$ in the coordinate system (O, i, j).

We can sketch the conic section $\mathscr{C}_2$ by using its equation in the coordinate system (O, e_1, e_2).

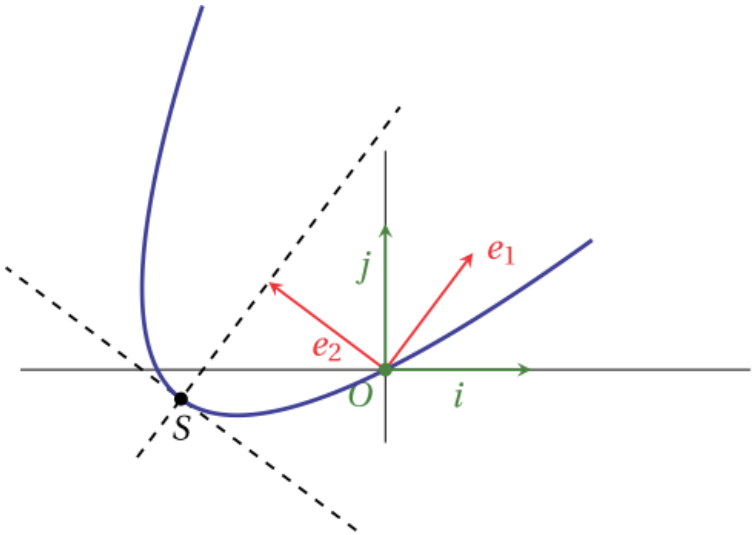


Fig. 2.2 . La conique $\mathscr{C}$

Conclusion:

To finish, here is the exhaustive list of the types of conic sections.

a) The empty set (example: $x^2 + y^2 = -1$),

b) A point (example: $x^2 + y^2 = 0$),

c) A line (example: $x^2 = 0$),

d) Two parallel lines (example: $x^2 = 1$),

e) Two intersecting lines (example: $x^2 - y^2 = 0$),

f) A parabola (example: $x^2 - y = 0$),

g) An ellipse (example: $x^2 + 2y^2 = 1$),

h) A hyperbola (example: $x^2 - 2y^2 = 1$).

CHAPTER 3

Symmetry and Galois Theory

3.1 Overview and some history

The quadratic formula is well-known. It gives us the two roots of a degree-2 polynomial $ax^2 + bx + c = 0$:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

There are formulas for cubic and quartic polynomials, but they are *very* complicated. For years, people wondered if there was a quintic formula. Nobody could find one.

In the 1830s, 19-year-old political activist Évariste Galois, with no formal mathematical training proved that no such formula existed.

He invented the concept of a **group** to solve this problem.

After being challenged to a dual at age 20 that he knew he would lose, Galois spent the last few days of his life frantically writing down what he had discovered.

In a final letter Galois wrote, "Later there will be, I hope, some people who will find it to their advantage to decipher all this mess."

Hermann Weyl (1885–1955) described Galois' final letter as: *"if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind."* Thus was born the field of group theory!

3.2 Arithmetic

Most people's first exposure to mathematics comes in the form of counting.

At first, we only know about the natural numbers, $\mathbb{N} = \{1, 2, 3, \dots\}$, and how to add them.

Soon after, we learn how to subtract, and we learn about negative numbers as well. At this point, we have the integers, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

Then, we learn how to divide numbers, and are introduced to fractions. This brings us to the rational numbers, $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0\}$.

Though there are other numbers out there (irrational, complex, etc.), we don't need these to do basic arithmetic.

Remark 3.1

To do arithmetic, we need *at least* the rational numbers.

3.3 Fields

Definition 3.1

A set F with addition and multiplication operations is a **field** if the following three conditions hold:

- F is an **abelian group** under addition.
- $F \setminus \{0\}$ is an **abelian group** under multiplication.
- The distributive law holds: $a(b + c) = ab + ac$.

Example 3.1

- The following sets are fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ (prime p).
- The following sets are *not* fields: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_n$ (composite n).

Definition 3.2

If F and E are fields with $F \subset E$, we say that E is an **extension** of F.

For example, $\mathbb{C}$ is an extension of $\mathbb{R}$, which is an extension of $\mathbb{Q}$.

$\mathbb{Q}(i)$: Another extension field of $\mathbb{Q}$

Example 3.2 (Question)

What is the *smallest* extension field F of $\mathbb{Q}$ that contains $i = \sqrt{-1}$?

This field must contain

$$-i, \quad \frac{2}{i}, \quad 6+i, \quad \left(i+\frac{3}{2}\right)^3, \quad \frac{i}{16+i}.$$

As before, we can write all of these as $a+bi$, where $a, b \in \mathbb{Q}$. Thus, the field "$\mathbb{Q}$ adjoin i" is

$$\mathbb{Q}(i) = \{a+bi \mid a, b \in \mathbb{Q}\} = \left\{ \frac{p}{q} + \frac{r}{s}i \;\middle|\; p, q, r, s \in \mathbb{Z},\ q, s \neq 0 \right\}.$$

Remark 3.2

- $\mathbb{Q}(i)$ is much smaller than $\mathbb{C}$. For example, it does not contain $\sqrt{2}$.
- $\mathbb{Q}(\sqrt{2})$ is a *subfield* of $\mathbb{R}$, but $\mathbb{Q}(i)$ is not.
- $\mathbb{Q}(\sqrt{2})$ contains all of the roots of $f(x) = x^2 - 2$. It is called the **splitting field** of $f(x)$. Similarly, $\mathbb{Q}(i)$ is the **splitting field** of $g(x) = x^2 + 1$.

3.4 $\mathbb{Q}(\sqrt{2}, i)$: Another extension field of $\mathbb{Q}$

Example 3.3 (Question)

What is the *smallest* extension field F of $\mathbb{Q}$ that contains $\sqrt{2}$ and $i = \sqrt{-1}$?

We can do this in two steps:

(i) Adjoin the roots of the polynomial $x^2 - 2$ to $\mathbb{Q}$, yielding $\mathbb{Q}(\sqrt{2})$;

(ii) Adjoin the roots of the polynomial $x^2 + 1$ to $\mathbb{Q}(\sqrt{2})$, yielding $\mathbb{Q}(\sqrt{2})(i)$;

An element in $\mathbb{Q}(\sqrt{2}, i) := \mathbb{Q}(\sqrt{2})(i)$ has the form

$$\begin{aligned} \alpha + \beta i &= (a + b\sqrt{2}) + (c + d\sqrt{2})i && \alpha, \beta \in \mathbb{Q}(\sqrt{2}) \\ &= a + b\sqrt{2} + ci + d\sqrt{2}i && a, b, c, d \in \mathbb{Q} \end{aligned}$$

We say that $\{1, \sqrt{2}, i, \sqrt{2}i\}$ is a **basis** for the extension $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$. Thus,

$$\mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + d\sqrt{2}i \mid a, b, c, d \in \mathbb{Q}\}$$

In summary, $\mathbb{Q}(\sqrt{2}, i)$ is constructed by starting with $\mathbb{Q}$, and adjoining all roots of $h(x) = (x^2 - 2)(x^2 + 1) = x^4 - x^2 - 2$. It is the **splitting field** of $h(x)$.

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$: Another extension field of $\mathbb{Q}$

Example 3.4 (Question)

What is the *smallest* extension field F of $\mathbb{Q}$ that contains $\sqrt{2}$ and $\sqrt{3}$?

This time, our field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, constructed by starting with $\mathbb{Q}$, and adjoining all roots of the polynomial $h(x) = (x^2 - 2)(x^2 - 3) = x^4 - 5x^2 + 6$.

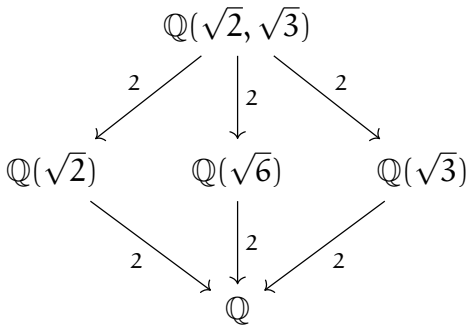
It is not difficult to show that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a **basis** for this field, i.e.,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.$$

Like with did with a group and its subgroups, we can arrange the **subfields** of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ in a lattice.

I've labeled each extension with the **degree** of the polynomial whose roots I need to adjoin.

Just for fun: What **group** has a subgroup lattice that looks like this?



3.5 Field automorphisms

Recall that an automorphism of a group G was an isomorphism $\phi : G \to G$.

Definition 3.3

Let F be a field. A **field automorphism** of F is a bijection $\phi : F \to F$ such that for all $a, b \in F$,

$$\phi(a + b) = \phi(a) + \phi(b) \qquad \text{and} \qquad \phi(ab) = \phi(a)\phi(b).$$

In other words, ϕ must *preserve the structure* of the field.

For example, let $F = \mathbb{Q}(\sqrt{2})$. Verify (HW) that the function

$$\phi : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2}), \qquad \phi : a + b\sqrt{2} \longmapsto a - b\sqrt{2}.$$

is an automorphism. That is, show that

- $\phi((a + b\sqrt{2}) + (c + d\sqrt{2})) = \cdots = \phi(a + b\sqrt{2}) + \phi(c + d\sqrt{2})$
- $\phi((a + b\sqrt{2})(c + d\sqrt{2})) = \cdots = \phi(a + b\sqrt{2})\phi(c + d\sqrt{2})$.

3.6 The Galois group of a field extension

The set of all automorphisms of a field form a group under composition.

Definition 3.4

Let F be an extension field of $\mathbb{Q}$. The **Galois group** of F is the group of **automorphisms** of F, denoted $\mathrm{Gal}(F)$.

Here are some examples (without proof):

- The Galois group of $\mathbb{Q}(\sqrt{2})$ is C_2:

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})) = \langle f \rangle \cong C_2, \qquad \text{where } f : \sqrt{2} \longmapsto -\sqrt{2}$$

- An automorphism of $F = \mathbb{Q}(\sqrt{2}, i)$ is completely determined by where it sends $\sqrt{2}$ and i. There are four possibilities: the identity map e, and

$$\begin{cases} h(\sqrt{2}) = -\sqrt{2} \\ h(i) = i \end{cases} \qquad \begin{cases} v(\sqrt{2}) = \sqrt{2} \\ v(i) = -i \end{cases} \qquad \begin{cases} r(\sqrt{2}) = -\sqrt{2} \\ r(i) = -i \end{cases}$$

Thus, the Galois group of F is $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)) = \langle h, v \rangle \cong V_4$.

3.7 $\mathbb{Q}(\zeta, \sqrt[3]{2})$: Another extension field of $\mathbb{Q}$

Example 3.5 (Question)

What is the *smallest* extension field F of $\mathbb{Q}$ that contains all roots of $g(x) = x^3 - 2$?

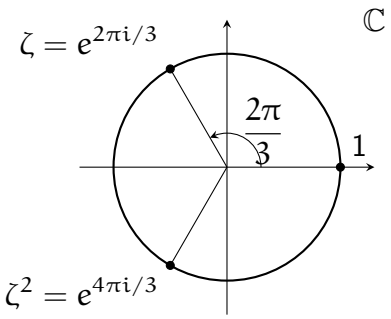
Let $\zeta = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. This is a **3rd root of unity**; the roots of $x^3 - 1 = (x-1)(x^2+x+1)$ are $1, \zeta, \zeta^2$.

Note that the roots of $g(x)$ are

$$z_1 = \sqrt[3]{2}, \qquad z_2 = \zeta\sqrt[3]{2}, \qquad z_3 = \zeta^2\sqrt[3]{2}.$$

Thus, the field we seek is $F = \mathbb{Q}(z_1, z_2, z_3)$.

I claim that $F = \mathbb{Q}(\zeta, \sqrt[3]{2})$. Note that this field contains z_1, z_2, and z_3. Conversely, we can construct ζ and $\sqrt[3]{2}$ from z_1 and z_2, using arithmetic.



A little algebra can show that

$$\mathbb{Q}(\zeta, \sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\zeta + e\zeta\sqrt[3]{2} + f\zeta\sqrt[3]{4} \mid a, b, c, d, e, f \in \mathbb{Q}\}.$$

Since $\zeta = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ lies in $\mathbb{Q}(\zeta, \sqrt[3]{2})$, so does $2(\zeta + \frac{1}{2}) = \sqrt{3}i = \sqrt{-3}$. Thus,

$$\mathbb{Q}(\zeta, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{3}i, \sqrt[3]{2}).$$

3.8 Subfields of $\mathbb{Q}(\zeta, \sqrt[3]{2})$

What are the subfields of

$$\mathbb{Q}(\zeta, \sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\zeta + e\zeta\sqrt[3]{2} + f\zeta\sqrt[3]{4} \mid a, b, c, d, e, f \in \mathbb{Q}\}?$$

Note that $(\zeta^2)^2 = \zeta^4 = \zeta$, and so $\mathbb{Q}(\zeta^2) = \mathbb{Q}(\zeta) = \{a + b\zeta \mid a, b \in \mathbb{Q}\}$.

Similarly, $(\sqrt[3]{4})^2 = 2\sqrt[3]{2}$, and so $\mathbb{Q}(\sqrt[3]{4}) = \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$.

There are two more subfields. As we did before, we can arrange them in a lattice.

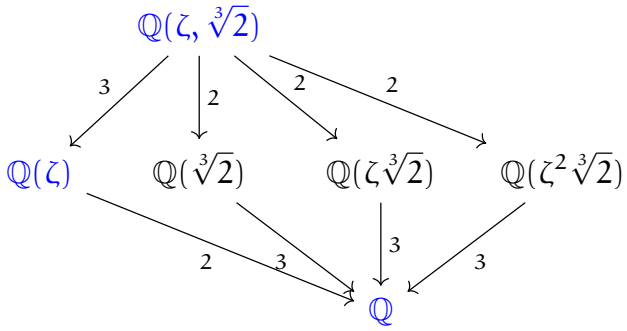


Fig. 3.1 . Look familiar? Lattice of subfields.

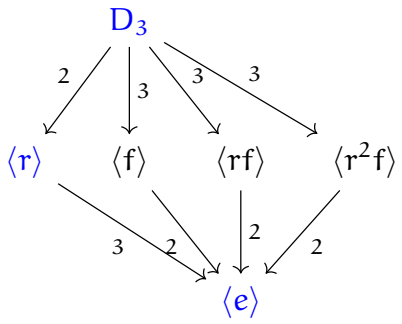


Fig. 3.2 . Compare this to the **subgroup lattice** of D_3.

3.9 Summary so far

Roughly speaking, a **field** is a group under both addition and multiplication (if we exclude 0), with the distributive law connecting these two operations.

We are mostly interested in the field $\mathbb{Q}$, and certain extension fields: $F \supseteq \mathbb{Q}$. Some of the extension fields we've encountered:

$$\mathbb{Q}(\sqrt{2}), \qquad \mathbb{Q}(i), \qquad \mathbb{Q}(\sqrt{2}, i), \qquad \mathbb{Q}(\sqrt{2}, \sqrt{3}), \qquad \mathbb{Q}(\zeta, \sqrt[3]{2}).$$

Remark 3.3

- An **automorphism** of a field $F \supseteq \mathbb{Q}$ is a structure-preserving map that **fixes** $\mathbb{Q}$.
- The set of all automorphisms of $F \supseteq \mathbb{Q}$ forms a group, called the **Galois group** of F, denoted $\mathrm{Gal}(F)$.

There is an intriguing but mysterious connection between subfields of F and subgroups of $\mathrm{Gal}(F)$. This is at the heart of Galois theory!

3.10 Polynomials

Definition 3.5

Let x be an unknown variable. A **polynomial** is a function

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0.$$

The highest non-zero power of n is called the **degree** of f.

We can assume that all of our coefficients a_i lie in a field F.

For example, if each $a_i \in \mathbb{Z}$ (not a field), we could alternatively say that $a_i \in \mathbb{Q}$.

Let $F[x]$ denote the set of polynomials with coefficients in F. We call this the set of **polynomials over** F.

Remark 3.4

Even though $\mathbb{Z}$ is not a field, we can still write $\mathbb{Z}[x]$ to be the set of polynomials with integer coefficients. Most polynomials we encounter have integer coefficients anyways.

3.11 Radicals

The roots of low-degree polynomials can be expressed using **arithmetic** and **radicals**.

For example, the roots of the polynomial $f(x) = 5x^4 - 18x^2 - 27$ are

$$x_{1,2} = \pm\sqrt{\frac{6\sqrt{6}+9}{5}}, \qquad x_{3,4} = \pm\sqrt{\frac{9-6\sqrt{6}}{5}}.$$

Remark 3.5

The operations of **arithmetic**, and **radicals**, are really the "only way" we have to write down generic complex numbers.

Thus, if there is some number that cannot be expressed using radicals, we have no way to

express it, unless we invent a special symbol for it (e.g., π or e).

Even weirder, since a computer program is just a string of 0s and 1s, there are only countably infinite many possible programs.

Since $\mathbb{R}$ is an uncountable set, there are numbers (in fact, "almost all" numbers) that can *never* be expressed algorithmically by a computer program! Such numbers are called **uncomputable**.

Hasse diagrams

The relationship between the natural numbers $\mathbb{N}$, and the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{A}$, and $\mathbb{C}$, is shown in the following Hasse diagrams.

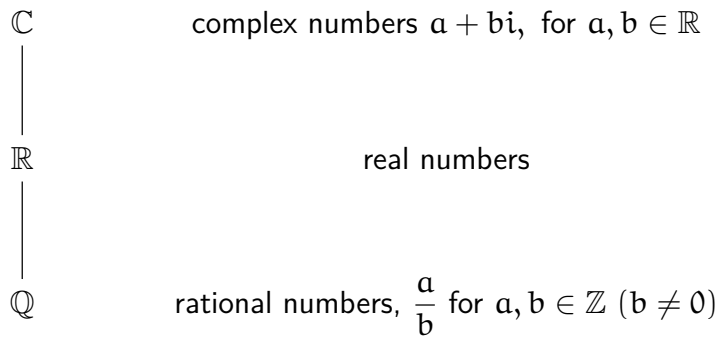


Fig. 3.3 . Standard inclusion lattice of foundational number fields.

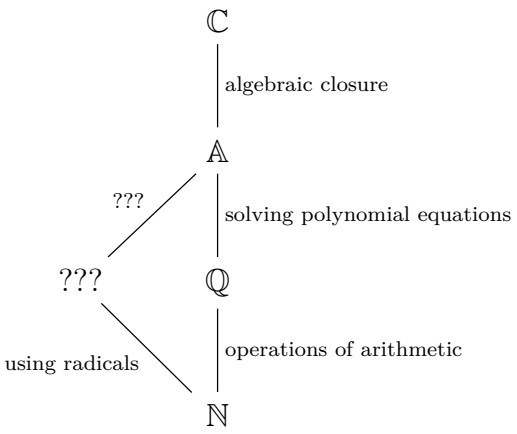


Fig. 3.4 . Hasse diagram mapping algebraic properties and transitions between extensions.

3.12 Some basic facts about the complex numbers

Definition 3.6

A field F is **algebraically closed** if for any polynomial $f(x) \in F[x]$, all of the roots of $f(x)$ lie in F.

Non-examples

- $\mathbb{Q}$ is not algebraically closed because $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ has a root $\sqrt{2} \notin \mathbb{Q}$.
- $\mathbb{R}$ is not algebraically closed because $f(x) = x^2 + 1 \in \mathbb{R}[x]$ has a root $\sqrt{-1} \notin \mathbb{R}$.

Theorem 3.1 (Fundamental theorem of algebra)

The field $\mathbb{C}$ is algebraically closed.

Thus, every polynomial $f(x) \in \mathbb{Z}[x]$ completely factors, or **splits** over $\mathbb{C}$:

$$f(x) = (x - r_1)(x - r_2)\dots(x - r_n), \qquad r_i \in \mathbb{C}.$$

Conversely, if F is *not* algebraically closed, then there are polynomials $f(x) \in F[x]$ that do *not* split into linear factors over F.

3.13 Complex conjugates

Remark 3.6

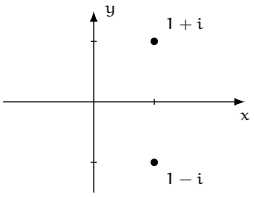
Recall that complex roots of $f(x) \in \mathbb{C}[x]$ come in **conjugate pairs**: If $r = a + bi$ is a root, then so is $\bar{r} := a - bi$.

Example 3.6

For example, here are the roots of some polynomials (degrees 2 through 5) plotted in the complex plane. All of them exhibit symmetry across the x-axis.

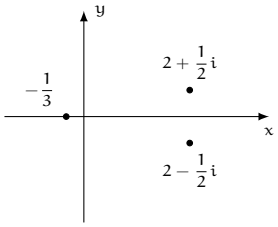
$$f(x) = x^2 - 2x + 2$$

Roots: $1 \pm i$



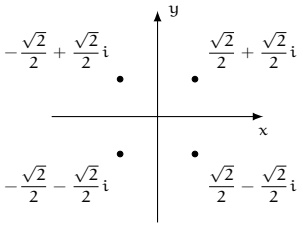
$$f(x) = 12x^3 - 44x^2 + 35x + 17$$

Roots: $-\frac{1}{3}, 2 \pm \frac{1}{2}i$



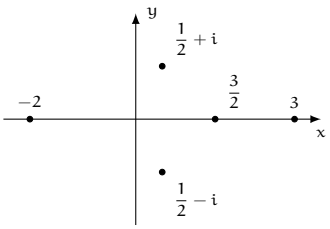
$$f(x) = x^4 + 1$$

Roots: $\pm\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2}i$



$$f(x) = 8x^5 - 28x^4 - 6x^3 + 83x^2 - 117x + 90$$

Roots: $-2, \frac{3}{2}, 3, \frac{1}{2} \pm i$



3.14 Irreducibility

Definition 3.7

A polynomial $f(x) \in F[x]$ is reducible over F if we can factor it as $f(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$ of strictly lower degree. If $f(x)$ is not reducible, we say it is irreducible over F.

Example 3.7

- $x^2 - x - 6 = (x + 2)(x - 3)$ is reducible over $\mathbb{Q}$.
- $x^4 + 5x^2 + 4 = (x^2 + 1)(x^2 + 4)$ is reducible over $\mathbb{Q}$, but it has no roots in $\mathbb{Q}$.
- $x^3 - 2$ is irreducible over $\mathbb{Q}$. If we could factor it, then one of the factors would have degree 1. But $x^3 - 2$ has no roots in $\mathbb{Q}$.

Remark 3.7

- If $\deg(f) > 1$ and has a root in F, then it is reducible over F.
- Every polynomial in $\mathbb{Z}[x]$ is reducible over $\mathbb{C}$.
- If $f(x) \in F[x]$ is a degree-2 or 3 polynomial, then $f(x)$ is reducible over F if and only if $f(x)$ has a root in F.

3.15 Eisenstein's criterion for irreducibility

Lemma 3.1

Let $f \in \mathbb{Z}[x]$ be irreducible. Then f is also irreducible over $\mathbb{Q}$.

Equivalently, if $f \in \mathbb{Z}[x]$ factors over $\mathbb{Q}$, then it factors over $\mathbb{Z}$.

Theorem 3.2 (Eisenstein's criterion)

A polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is irreducible if for some prime p, the following all hold:

1. $p \nmid a_n$;
2. $p \mid a_k$ for $k = 0, \ldots, n-1$;
3. $p^2 \nmid a_0$.

For example, Eisenstein's criterion tells us that $x^{10} + 4x^7 + 18x + 14$ is irreducible.

Remark 3.8

If Eisenstein's criterion fails for all primes p, that does not necessarily imply that f is reducible. For example, $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{Q}$, but Eisenstein cannot detect this.

3.16 Extension fields as vector spaces

Recall that a vector space over $\mathbb{Q}$ is a set of vectors V such that

- If $u, v \in V$, then $u + v \in V$ (closed under addition)
- If $v \in V$, then $cv \in V$ for all $c \in \mathbb{Q}$ (closed under scalar multiplication).

The field $\mathbb{Q}(\sqrt{2})$ is a 2-dimensional vector space over $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

This is why we say that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

Notice that the other field extensions we've seen are also vector spaces over $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + d\sqrt{2}i : a, b, c, d \in \mathbb{Q}\},$$
$$\mathbb{Q}(\zeta, \sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\zeta + e\zeta\sqrt[3]{2} + f\zeta\sqrt[3]{4} : a, b, c, d, e, f \in \mathbb{Q}\}.$$

As $\mathbb{Q}$-vector spaces, $\mathbb{Q}(\sqrt{2}, i)$ has dimension 4, and $\mathbb{Q}(\zeta, \sqrt[3]{2})$ has dimension 6.

Definition 3.8

If $F \subseteq E$ are fields, then the degree of the extension, denoted $[E : F]$, is the dimension of E as a vector space over F.

Equivalently, this is the number of terms in the expression for a general element for E using coefficients from F.

3.17 The Galois group of a polynomial

Definition 3.9

Let $f \in \mathbb{Z}[x]$ be a polynomial, with roots $r_1, \ldots, r_n$. The splitting field of f is the field

$$\mathbb{Q}(r_1, \ldots, r_n).$$

The splitting field F of $f(x)$ has several equivalent characterizations:

- the smallest field that contains all of the roots of $f(x)$;
- the smallest field in which $f(x)$ splits into linear factors:

$$f(x) = (x - r_1)(x - r_2)\dots(x - r_n) \in F[x].$$

Recall that the Galois group of an extension $F \supseteq \mathbb{Q}$ is the group of automorphisms of F, denoted $\mathrm{Gal}(F)$.

Definition 3.10

The Galois group of a polynomial $f(x)$ is the Galois group of its splitting field, denoted $\mathrm{Gal}(f(x))$.

3.17.1 A few examples of Galois groups

- The polynomial $x^2 - 2$ splits in $\mathbb{Q}(\sqrt{2})$, so

$$\mathrm{Gal}(x^2 - 2) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2})) \cong C_2.$$

- The polynomial $x^2 + 1$ splits in $\mathbb{Q}(i)$, so

$$\mathrm{Gal}(x^2 + 1) = \mathrm{Gal}(\mathbb{Q}(i)) \cong C_2.$$

- The polynomial $x^2 + x + 1$ splits in $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/3}$, so

$$\mathrm{Gal}(x^2 + x + 1) = \mathrm{Gal}(\mathbb{Q}(\zeta)) \cong C_2.$$

- The polynomial $x^3 - 1 = (x - 1)(x^2 + x + 1)$ also splits in $\mathbb{Q}(\zeta)$, so

$$\mathrm{Gal}(x^3 - 1) = \mathrm{Gal}(\mathbb{Q}(\zeta)) \cong C_2.$$

- The polynomial $x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$ splits in $\mathbb{Q}(\sqrt{2}, i)$, so

$$\mathrm{Gal}(x^4 - x^2 - 2) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)) \cong V_4.$$

- The polynomial $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ splits in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, so

$$\mathrm{Gal}(x^4 - 5x^2 + 6) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) \cong V_4.$$

- The polynomial $x^3 - 2$ splits in $\mathbb{Q}(\zeta, \sqrt[3]{2})$, so

$$\mathrm{Gal}(x^3 - 2) = \mathrm{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2})) \cong D_3 \text{ ???}$$

3.18 The tower law of field extensions

Recall that if we had a chain of subgroups $K \leqslant H \leqslant G$, then the index satisfies a tower law: $[G : K] = [G : H][H : K]$.

Not surprisingly, the degree of field extensions obeys a similar tower law:

Theorem 3.3 (Tower law)

For any chain of field extensions $F \subset E \subset K$,

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

We have already observed this in our subfield lattices:

$$\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right] = \underbrace{\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right]}_{\text{min. poly: } x^2-3} \underbrace{\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right]}_{\text{min. poly: } x^2-2} = 2 \cdot 2 = 4.$$

3.19 Primitive elements

Theorem 3.4 (Primitive element theorem)

If F is an extension of $\mathbb{Q}$ with $[F:\mathbb{Q}] < \infty$, then F has a primitive element: some $\alpha \notin \mathbb{Q}$ for which $F = \mathbb{Q}(\alpha)$.

How do we find a primitive element α of $F = \mathbb{Q}(\zeta, \sqrt[3]{2}) = \mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$?

Let's try $\alpha = i\sqrt{3}\sqrt[3]{2} \in F$. Clearly, $[\mathbb{Q}(\alpha):\mathbb{Q}] \leqslant 6$. Observe that

$$\alpha^2 = -3\sqrt[3]{4}, \quad \alpha^3 = -6i\sqrt{3}, \quad \alpha^4 = -18\sqrt[3]{2}, \quad \alpha^5 = 18i\sqrt[3]{4}\sqrt{3}, \quad \alpha^6 = -108.$$

Thus, α is a root of $x^6 + 108$. The following are equivalent (why?):

(i) α is a primitive element of F;

(ii) $[\mathbb{Q}(\alpha):\mathbb{Q}] = 6$;

(iii) the minimal polynomial $m(x)$ of α has degree 6;

(iv) $x^6 + 108$ is irreducible (and hence must be $m(x)$).

In fact, $[\mathbb{Q}(\alpha):\mathbb{Q}] = 6$ holds because both 2 and 3 divide $[\mathbb{Q}(\alpha):\mathbb{Q}]$:

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = \left[\mathbb{Q}(\alpha):\mathbb{Q}\left(i\sqrt{3}\right)\right] \underbrace{\left[\mathbb{Q}\left(i\sqrt{3}\right):\mathbb{Q}\right]}_{=2}, \qquad [\mathbb{Q}(\alpha):\mathbb{Q}] = \left[\mathbb{Q}(\alpha):\mathbb{Q}\left(\sqrt[3]{2}\right)\right] \underbrace{\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]}_{=3}.$$

Example 3.8 (The Galois group of $x^4 - 5x^2 + 6$)

The polynomial $f(x) = (x^2-2)(x^2-3) = x^4 - 5x^2 + 6$ has splitting field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

We already know that its Galois group should be V_4. Let's compute it explicitly; this will help us understand it better.

We need to determine all automorphisms ϕ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. We know:

- ϕ is determined by where it sends the basis elements $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.
- ϕ must fix 1.
- If we know where ϕ sends two of $\{\sqrt{2}, \sqrt{3}, \sqrt{6}\}$, then we know where it sends the third, because

$$\phi(\sqrt{6}) = \phi(\sqrt{2}\sqrt{3}) = \phi(\sqrt{2})\phi(\sqrt{3}).$$

In addition to the identity automorphism e, we have

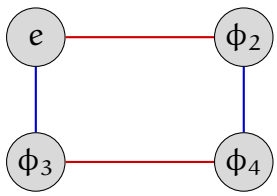
$$\begin{cases} \phi_2(\sqrt{2}) = -\sqrt{2} \\ \phi_2(\sqrt{3}) = \sqrt{3} \end{cases} \qquad \begin{cases} \phi_3(\sqrt{2}) = \sqrt{2} \\ \phi_3(\sqrt{3}) = -\sqrt{3} \end{cases} \qquad \begin{cases} \phi_4(\sqrt{2}) = -\sqrt{2} \\ \phi_4(\sqrt{3}) = -\sqrt{3} \end{cases}$$

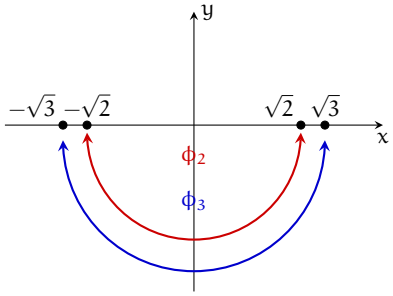
There are 4 automorphisms of $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, the splitting field of $x^4 - 5x^2 + 6$:

$$\begin{aligned} e&: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \\ \phi_2&: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\ \phi_3&: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\ \phi_4&: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6} \end{aligned}$$

They form the Galois group of $x^4 - 5x^2 + 6$. The multiplication table and Cayley diagram are shown below.

	e	ϕ_2	ϕ_3	ϕ_4
e	e	ϕ_2	ϕ_3	ϕ_4
ϕ_2	ϕ_2	e	ϕ_4	ϕ_3
ϕ_3	ϕ_3	ϕ_4	e	ϕ_2
ϕ_4	ϕ_4	ϕ_3	ϕ_2	e





3.19.1 The Galois group acts on the roots

Theorem 3.5

If $f \in \mathbb{Z}[x]$ is a polynomial with a root in a field extension F of $\mathbb{Q}$, then any automorphism of F permutes the roots of f.

Said differently, we have a group action of $\mathrm{Gal}(f(x))$ on the set $S = \{r_1, \ldots, r_n\}$ of roots of $f(x)$.

That is, we have a homomorphism

$$\psi \colon \mathrm{Gal}(f(x)) \longrightarrow \mathrm{Perm}(\{r_1, \ldots, r_n\}).$$

If $\phi \in \mathrm{Gal}(f(x))$, then $\psi(\phi)$ is a permutation of the roots of $f(x)$.

This permutation is what results by "pressing the ϕ-button" – it permutes the roots of $f(x)$ via the automorphism ϕ of the splitting field of $f(x)$.

Corollary 3.1

If the degree of $f \in \mathbb{Z}[x]$ is n, then the Galois group of f is a subgroup of S_n.

The next result says that "$\mathbb{Q}$ can't tell apart the roots of an irreducible polynomial."

Theorem 3.6 (The "One orbit theorem")

Let r_1 and r_2 be roots of an irreducible polynomial over $\mathbb{Q}$. Then

(a) There is an isomorphism $\phi : \mathbb{Q}(r_1) \longrightarrow \mathbb{Q}(r_2)$ that fixes $\mathbb{Q}$ and with $\phi(r_1) = r_2$.

(b) This remains true when $\mathbb{Q}$ is replaced with any extension field F, where $\mathbb{Q} \subset F \subset \mathbb{C}$.

Corollary 3.2

If $f(x)$ is irreducible over $\mathbb{Q}$, then for any two roots r_1 and r_2 of $f(x)$, the Galois group $\mathrm{Gal}(f(x))$ contains an automorphism $\phi : r_1 \longmapsto r_2$.

In other words, if $f(x)$ is irreducible, then the action of $\mathrm{Gal}(f(x))$ on the set $S = \{r_1, \ldots, r_n\}$ of roots has only one orbit.

3.20 Normal field extensions

Definition 3.11

An extension field E of F is normal if it is the splitting field of some polynomial $f(x)$.

If E is a normal extension over F, then every irreducible polynomial in $F[x]$ that has a root in E splits over F.

Thus, if you can find an irreducible polynomial that has one root, but not all of its roots in E, then E is *not* a normal extension.

Theorem 3.7 (Normal extension theorem)

The degree of a normal extension is the order of its Galois group.

Corollary 3.3

The order of the Galois group of a polynomial $f(x)$ is the degree of the extension of its splitting field over $\mathbb{Q}$.

3.21 The Galois group of $x^3 - 2$

We can now conclusively determine the Galois group of $x^3 - 2$.

By definition, the Galois group of a polynomial is the Galois group of its splitting field, so $\mathrm{Gal}(x^3 - 2) = \mathrm{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2}))$.

By the normal extension theorem, the order of the Galois group of $f(x)$ is the degree of the extension of its splitting field:

$$|\mathrm{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2}))| = [\mathbb{Q}(\zeta, \sqrt[3]{2}) : \mathbb{Q}] = 6.$$

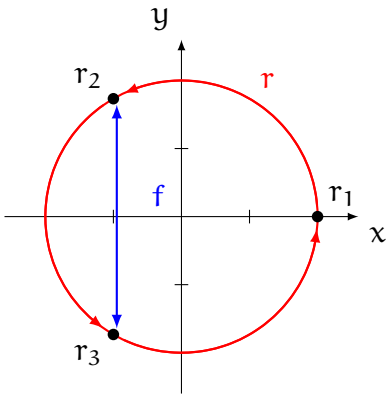
Since the Galois group acts on the roots of $x^3 - 2$, it must be a subgroup of $S_3 \cong D_3$.

There is only one subgroup of S_3 of order 6, so $\mathrm{Gal}(x^3 - 2) \cong S_3$. Here is the action diagram

of $\mathrm{Gal}(x^3-2)$ acting on the set $S=\{r_1,r_2,r_3\}$ of roots of x^3-2:

$$\begin{cases} r:\sqrt[3]{2}\longmapsto \zeta\sqrt[3]{2} \\ r:\zeta\longmapsto\zeta \end{cases}$$

$$\begin{cases} f:\sqrt[3]{2}\longmapsto \sqrt[3]{2} \\ f:\zeta\longmapsto\zeta^2 \end{cases}$$



3.22 Paris, May 31, 1832

The night before a duel that Évariste Galois knew he would lose, the 20-year-old stayed up late preparing his mathematical findings in a letter to Auguste Chevalier.

Hermann Weyl (1885–1955) said "*This letter, if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind.*"

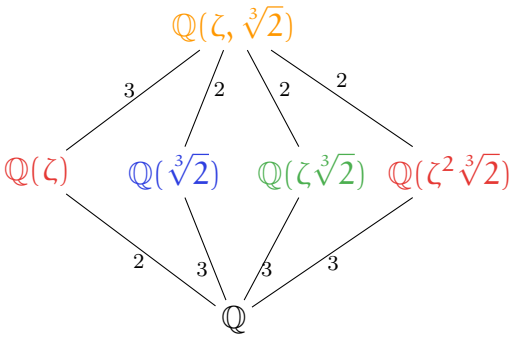
Theorem 3.8 (Fundamental theorem of Galois theory)

Given $f\in\mathbb{Z}[x]$, let F be the splitting field of f, and G the Galois group. Then the following hold:

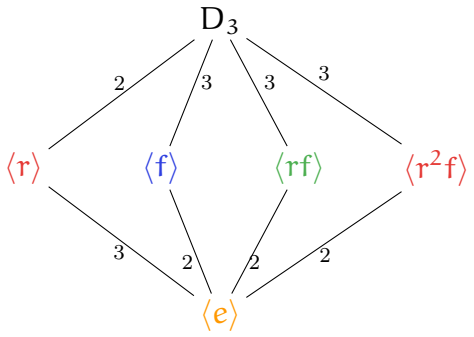
(a) The subgroup lattice of G is identical to the subfield lattice of F, but upside-down. Moreover, $H\triangleleft G$ if and only if the corresponding subfield is a normal extension of $\mathbb{Q}$.

(b) Given an intermediate field $\mathbb{Q}\subset K\subset F$, the corresponding subgroup $H<G$ contains precisely those automorphisms that fix K.

Example 3.9 (An example: the Galois correspondence for $f(x) = x^3 - 2$)



Subfield lattice of $\mathbb{Q}(\zeta, \sqrt[3]{2})$



Subgroup lattice of $\mathrm{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2})) \cong D_3$.

- The automorphisms that fix $\mathbb{Q}$ are precisely those in D_3.
- The automorphisms that fix $\mathbb{Q}(\zeta)$ are precisely those in $\langle r \rangle$.
- The automorphisms that fix $\mathbb{Q}(\sqrt[3]{2})$ are precisely those in $\langle f \rangle$.
- The automorphisms that fix $\mathbb{Q}(\zeta\sqrt[3]{2})$ are precisely those in $\langle rf \rangle$.
- The automorphisms that fix $\mathbb{Q}(\zeta^2\sqrt[3]{2})$ are precisely those in $\langle r^2 f \rangle$.
- The automorphisms that fix $\mathbb{Q}(\zeta, \sqrt[3]{2})$ are precisely those in $\langle e \rangle$.

The normal field extensions of $\mathbb{Q}$ are: $\mathbb{Q}$, $\mathbb{Q}(\zeta)$, and $\mathbb{Q}(\zeta, \sqrt[3]{2})$.

The normal subgroups of D_3 are: D_3, $\langle r \rangle$ and $\langle e \rangle$.

3.23 Solvability

Definition 3.12

A group G is solvable if it has a chain of subgroups:

$$\{e\} = N_0 \triangleleft N_1 \triangleleft N_2 \triangleleft \cdots \triangleleft N_{k-1} \triangleleft N_k = G.$$

such that each quotient N_i/N_{i-1} is abelian.

Remark 3.9

Each subgroup N_i need not be normal in G, just in N_{i+1}.

Example 3.10

- $D_4 = \langle r, f \rangle$ is solvable. There are many possible chains:

$$\langle e \rangle \triangleleft \langle f \rangle \triangleleft \langle r^2, f \rangle \triangleleft D_4, \qquad \langle e \rangle \triangleleft \langle r \rangle \triangleleft D_4, \qquad \langle e \rangle \triangleleft \langle r^2 \rangle \triangleleft D_4.$$

- Any abelian group A is solvable: take $N_0 = \{e\}$ and $N_1 = A$.
- For $n \geqslant 5$, the group A_n is simple and non-abelian. Thus, the only chain of normal subgroups is

$$N_0 = \{e\} \triangleleft A_n = N_1.$$

Since $N_1/N_0 \cong A_n$ is non-abelian, A_n is not solvable for $n \geqslant 5$.

3.24 The hunt for an unsolvable polynomial

The following lemma follows from the Correspondence Theorem. (Why?)

Lemma 3.2

If $N \triangleleft G$, then G is solvable if and only if both N and G/N are solvable.

Corollary 3.4

S_n is not solvable for all $n \geqslant 5$. (Since $A_n \triangleleft S_n$ is not solvable).

Theorem 3.9 (Galois' theorem)

A field extension $E \supseteq \mathbb{Q}$ contains only elements expressible by radicals if and only if its Galois group is solvable.

Corollary 3.5

$f(x)$ is solvable by radicals if and only if it has a solvable Galois group.

3.25 An unsolvable quintic!

To find a polynomial not solvable by radicals, we'll look for a polynomial $f(x)$ with $\mathrm{Gal}(f(x)) \cong S_5$.

We'll restrict our search to degree-5 polynomials, because $\mathrm{Gal}(f(x)) \leqslant S_5$ for any degree-5 polynomial $f(x)$.

Remark 3.10

Recall that for any 5-cycle σ and 2-cycle (=transposition) τ,

$$S_5 = \langle \sigma, \tau \rangle.$$

Moreover, the *only* elements in S_5 of order 5 are 5-cycles, e.g., $\sigma = (a\ b\ c\ d\ e)$.

Let $f(x) = x^5 + 10x^4 - 2$. It is irreducible by Eisenstein's criterion (use $p = 2$). Let $F = \mathbb{Q}(r_1, \ldots, r_5)$ be its splitting field.

Basic calculus tells us that f exactly has 3 real roots. Let $r_1, r_2 = a \pm bi$ be the complex roots, and r_3, r_4, and r_5 be the real roots.

Since f has distinct complex conjugate roots, complex conjugation is an automorphism $\tau : F \longrightarrow F$ that transposes r_1 with r_2, and fixes the three real roots. We just found our transposition $\tau = (r_1\ r_2)$. All that's left is to find an element (i.e., an automorphism) σ of order 5.

Take any root r_i of $f(x)$. Since $f(x)$ is irreducible, it is the minimal polynomial of r_i. By the Degree Theorem,

$$[\mathbb{Q}(r_i) : \mathbb{Q}] = \deg(\text{minimum polynomial of } r_i) = \deg f(x) = 5.$$

The splitting field of $f(x)$ is $F = \mathbb{Q}(r_1, \ldots, r_5)$, and by the normal extension theorem, the degree of this extension over $\mathbb{Q}$ is the order of the Galois group $\mathrm{Gal}(f(x))$.

Applying the tower law to this yields

$$|\mathrm{Gal}(f(x))| = [\mathbb{Q}(r_1, r_2, r_3, r_4, r_5) : \mathbb{Q}] = [\mathbb{Q}(r_1, r_2, r_3, r_4, r_5) : \mathbb{Q}(r_1)] \underbrace{[\mathbb{Q}(r_1) : \mathbb{Q}]}_{=5}$$

Thus, $|\mathrm{Gal}(f(x))|$ is a multiple of 5, so Cauchy's theorem guarantees that G has an element σ of order 5.

Since $\mathrm{Gal}(f(x))$ has a 2-cycle τ and a 5-cycle σ, it must be all of S_5.

$\mathrm{Gal}(f(x))$ is an unsolvable group, so $f(x) = x^5 + 10x^4 - 2$ is unsolvable by radicals!

3.26 Summary of Galois' work

Let $f(x)$ be a degree-n polynomial in $\mathbb{Z}[x]$ (or $\mathbb{Q}[x]$). The roots of $f(x)$ lie in some splitting field $F \supseteq \mathbb{Q}$.

The Galois group of $f(x)$ is the automorphism group of F. Every such automorphism fixes $\mathbb{Q}$ and permutes the roots of $f(x)$.

This is a group action of $\mathrm{Gal}(f(x))$ on the set of n roots! Thus, $\mathrm{Gal}(f(x)) \leqslant S_n$.

There is a 1–1 correspondence between subfields of F and subgroups of $\mathrm{Gal}(f(x))$.

A polynomial is solvable by radicals iff its Galois group is a solvable group.

The symmetric group S_5 is not a solvable group.

Since $S_5 = \langle \tau, \sigma \rangle$ for a 2-cycle τ and 5-cycle σ, all we need to do is find a degree-5 polynomial whose Galois group contains a 2-cycle and an element of order 5.

General Conclusion

In conclusion, this work demonstrates that symmetry is not merely a geometric property, but a structural tool for understanding algebraic frameworks through Galois Theory. Throughout our research, we traced the transition from geometric to algebraic symmetry, where geometric transformations (such as rotations and reflections) are encoded by numbering the vertices of a shape, thereby transforming its movements into permutations and elements within the symmetric group S_n. Through this framework, we showed how this algebraic symmetry is mirrored in the roots of polynomials within a field extension L/K, forming a distinct group structure denoted as $\mathrm{Gal}(L/K)$. Ultimately, we proved that the structural properties of this Galois group — specifically whether it is a solvable group — hold the definitive key to determining the solvability of equations by radicals, highlighting the profound impact of symmetry on modern algebra. Finally, we hope that this research opens new horizons for fellow students and researchers in the coming years."

Bibliography

[1] Ewing, J. H., Gehring, F. W., & Halmos, P. R. *Undergraduate Texts in Mathematics*.

[2] Gallian, J. (2021). *Contemporary Abstract Algebra*. Chapman and Hall/CRC.

[3] Goodman, F. (2014). *Algebra: Abstract and Concrete* (2.6th ed.). SemiSimple Press.

[4] Judson, T. W. (2020). *Abstract Algebra: Theory and Applications*.

[5] Matsuura, R. (2022). *A Friendly Introduction to Abstract Algebra* (Vol. 72). American Mathematical Society.

[6] Miller, W. (1973). *Symmetry Groups and Their Applications* (Vol. 50). Academic Press.

[7] Von Buhren, J. *Isométries d'un espace euclidien*. Cours de mathématiques, TSI 2, Lycée Blaise Pascal. Disponible sur : http://vonbuhren.free.fr.

[8] Macauley, M. (2016). *Visual Group Theory, Lecture 6.7: Ruler and compass constructions* [Vidéo YouTube].https://youtu.be/8k5AJoqHZJ4