SYMMETRIES

SAMUEL MIMRAM
École Polytechnique

This is a small survey on the use of symmetry in:

- algebra: Galois theory
- geometry: deck transformations

CLASSICAL GALOIS THEORY

Starting point

We want to find the roots of the following polynomial in $\mathbb{Q}[X]$:

$$X^4 - 4X^2 - 5 \quad = \quad (X^2 + 1)(X^2 - 5)$$

Starting point

We want to find the roots of the following polynomial in $\mathbb{Q}[X]$:

$$X^4 - 4X^2 - 5 \quad = \quad (X^2 + 1)(X^2 - 5)$$

Its four roots are

$$a = i \qquad b = -i \qquad c = \sqrt{5} \qquad d = -\sqrt{5}$$

Starting point

We want to find the roots of the following polynomial in $\mathbb{Q}[X]$:

$$X^4 - 4X^2 - 5 \quad = \quad (X^2 + 1)(X^2 - 5)$$

Its four roots are

$$a = i \qquad b = -i \qquad c = \sqrt{5} \qquad d = -\sqrt{5}$$

Any equation involving those, with coefficients in $\mathbb{Q}$, is still valid if we permute a with b, or c with d:

$$a^2 + 1 = 0 \qquad a + b = 0 \qquad ac = bd \qquad \ldots$$

Starting point

We want to find the roots of the following polynomial in $\mathbb{Q}[X]$:

$$X^4 - 4X^2 - 5 \quad = \quad (X^2+1)(X^2-5)$$

Its four roots are

$$a = i \qquad b = -i \qquad c = \sqrt{5} \qquad d = -\sqrt{5}$$

Any equation involving those, with coefficients in $\mathbb{Q}$, is still valid if we permute a with b, or c with d:

$$a^2 + 1 = 0 \qquad a + b = 0 \qquad ac = bd \qquad \dots$$

Otherwise said, we have two automorphisms of $\mathbb{Q}(i, \sqrt{5})$ fixing $\mathbb{Q}$:

$$\begin{array}{rcl} i & \mapsto & -i \\ \sqrt{5} & \mapsto & \sqrt{5} \end{array} \qquad\qquad \begin{array}{rcl} i & \mapsto & i \\ \sqrt{5} & \mapsto & -\sqrt{5} \end{array}$$

Intermediate fields

A **field extension** L/K consist of a field L and a subfield $K \subseteq L$ (or more generally a mono $K \hookrightarrow L$).

Intermediate fields

A **field extension** L/K consist of a field L and a subfield $K \subseteq L$
(or more generally a mono $K \hookrightarrow L$).

Note: in the category **Field** every morphism is mono and
morphisms are between fields of same characteristic
(we will be mostly interested in characteristic 0).

Intermediate fields

A **field extension** L/K consist of a field L and a subfield $K \subseteq L$
(or more generally a mono $K \hookrightarrow L$).

Note: in the category **Field** every morphism is mono and
morphisms are between fields of same characteristic
(we will be mostly interested in characteristic 0).

Given a field extension L/K, we write

$$L /\!\!/ K$$

for the poset of **intermediate extensions** $K \subseteq M \subseteq L$, the order being $\subseteq$.

Classical Galois theory

Given a field K, $\mathsf{Aut}(K)$ is the group of **automorphisms** of K.

Classical Galois theory

Given a field K, $\mathsf{Aut}(K)$ is the group of **automorphisms** of K.

Given a field extension L/K, i.e. $K \subseteq L$, the **Galois group**

$$\mathsf{Aut}(L/K)$$

is the subgroup of $\mathsf{Aut}(L)$ of automorphisms f fixing K, i.e.

$$\forall x \in K, \qquad f(x) = x$$

Classical Galois theory

Given a field K, $\mathrm{Aut}(K)$ is the group of **automorphisms** of K.

Given a field extension L/K, i.e. $K \subseteq L$, the **Galois group**

$$\mathrm{Aut}(L/K)$$

is the subgroup of $\mathrm{Aut}(L)$ of automorphisms f fixing K, i.e.

$$\forall x \in K, \qquad f(x) = x$$

Example: $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ (i sent to either i or $-i$).

Classical Galois theory

Given a field K, $\mathrm{Aut}(K)$ is the group of **automorphisms** of K.

Given a field extension L/K, i.e. $K \subseteq L$, the **Galois group**

$$\mathrm{Aut}(L/K)$$

is the subgroup of $\mathrm{Aut}(L)$ of automorphisms f fixing K, i.e.

$$\forall x \in K, \qquad f(x) = x$$

Example: $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ (i sent to either i or $-i$).

We also have a poset

$$\mathrm{Aut}(L /\!\!/ K)$$

of subgroups of $\mathrm{Aut}(L/K)$ ordered by $\subseteq$.

The Galois correspondence

Theorem

Given a field extension L/K, there is an adjunction

$$\begin{tikzcd}
\mathrm{Aut}(L/\!\!/K) \arrow[r, bend left, "F"] \arrow[r, phantom, "\perp"] & (L/\!\!/K)^{\mathrm{op}} \arrow[l, bend left, "G"]
\end{tikzcd}$$

The Galois correspondence

Theorem

Given a field extension L/K, there is an adjunction

$$\begin{tikzcd}
\mathrm{Aut}(L/\!\!/K) \arrow[r, bend left, "F"] \arrow[r, phantom, "\perp"] & (L/\!\!/K)^{\mathrm{op}} \arrow[l, bend left, "G"]
\end{tikzcd}$$

- G takes $K \subseteq M \subseteq L$ to the subgroup of $\mathrm{Aut}(L/K)$:

$$GM \quad = \quad \{f : L \to L \mid f \text{ fixes } M\}$$

- F takes a subgroup $A \subseteq \mathrm{Aut}(L/K)$ to

$$FA \quad = \quad \{x \in K \mid A \text{ fixes } x\}$$

We can check that they are functors such that

$$\frac{FA \supseteq B}{A \subseteq GB}$$

Galois correspondences

An adjunction between two posets

$$\begin{tikzcd} P \arrow[r, bend left, "F"] \arrow[r, phantom, "\perp"] & Q \arrow[l, bend left, "G"] \end{tikzcd}$$

is called a **Galois correspondence**.

Galois correspondences

An adjunction between two posets

$$\begin{tikzcd}
P \arrow[r, bend left, "F"] \arrow[r, phantom, "\perp"] & Q \arrow[l, bend left, "G"]
\end{tikzcd}$$

is called a **Galois correspondence**.

In this case $T = G \circ F$ is a **closure operator**:

- *extensive*: $x \leq T(x)$
- *increasing*: $x \leq y$ implies $T(x) \leq T(y)$
- *idempotent*: $T(T(x)) = T(x)$

Galois correspondences

An adjunction between two posets

$$\begin{tikzcd} P \arrow[r, bend left, "F"] \arrow[r, phantom, "\perp"] & Q \arrow[l, bend left, "G"] \end{tikzcd}$$

is called a **Galois correspondence**.

We write $P^* \subseteq P$ for the set of its **fixpoints**:

$$P^* \quad = \quad \{x \in P \mid G \circ F(x) = x\}$$

and similarly for $Q^* \subseteq Q$.

Galois correspondences

An adjunction between two posets

$$\begin{tikzcd} P \arrow[rr, bend left, "F"] \arrow[rr, phantom, "\perp"] & & Q \arrow[ll, bend left, "G"] \end{tikzcd}$$

is called a **Galois correspondence**.

Proposition

We have an induced bijection

$$\begin{tikzcd} P^* \arrow[rr, bend left, "F"] & & Q^* \arrow[ll, bend left, "G"] \end{tikzcd}$$

Generality

Note that up to now, the fact that we consider fields was used nowhere: it would equally work with groups, rings, or whatever you like...

The fundamental theorem

In the case of

$$\begin{tikzcd}
\mathrm{Aut}(L /\!\!/ K) \arrow[rr, bend left, "F"] \arrow[rr, phantom, "\perp"] & & (L /\!\!/ K)^{\mathrm{op}} \arrow[ll, bend left, "G"]
\end{tikzcd}$$

the correspondence is a bijection if (and only if) L/K is an extension which is *finite*, *separable* and *normal*.

In the general case, F is injective and G is surjective.

Dimension

Any extension L/K can be seen as a K-vector field.

Dimension

Any extension L/K can be seen as a K-vector field.

Its dimension is written $[L : K]$ and called the **degree** of L/K.

Dimension

Any extension L/K can be seen as a K-vector field.

Its dimension is written $[L : K]$ and called the **degree** of L/K.

L/K is **finite** when $[L : K]$ is.

Dimension

Any extension L/K can be seen as a K-vector field.

Its dimension is written $[L:K]$ and called the **degree** of L/K.

L/K is **finite** when $[L:K]$ is.

Given $K \subseteq L \subseteq M$,

$$[M:K] \quad = \quad [M:L] \times [L:K]$$

Dimension

Any extension L/K can be seen as a K-vector field.

Its dimension is written $[L : K]$ and called the **degree** of L/K.

L/K is **finite** when $[L : K]$ is.

Given $K \subseteq L \subseteq M$,

$$[M : K] \quad = \quad [M : L] \times [L : K]$$

Example

$$\begin{aligned}[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \times [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \\ &= 2 \times 2 = 4\end{aligned}$$

Galois extension

An extension L/K is

- **algebraic** when every element of L is *algebraic* over K,
  i.e. is the root of some $P \in K[X]$ with $P \neq 0$,

Galois extension

An extension L/K is

- **algebraic** when every element of L is *algebraic* over K, i.e. is the root of some $P \in K[X]$ with $P \neq 0$,
- **separable** when the minimal polynomial of every element in L over K is *separable*, i.e. has no repeated root in the algebraic closure over K,

Galois extension

An extension L/K is

- **algebraic** when every element of L is *algebraic* over K, i.e. is the root of some $P \in K[X]$ with $P \neq 0$,
- **separable** when the minimal polynomial of every element in L over K is *separable*, i.e. has no repeated root in the algebraic closure over K,
- **normal** when every irreducible polynomial P in $K[X]$ which has one root in L has all roots in L (it *splits* in L),

Galois extension

An extension L/K is

- **algebraic** when every element of L is *algebraic* over K, i.e. is the root of some $P \in K[X]$ with $P \neq 0$,
- **separable** when the minimal polynomial of every element in L over K is *separable*, i.e. has no repeated root in the algebraic closure over K,
- **normal** when every irreducible polynomial P in $K[X]$ which has one root in L has all roots in L (it *splits* in L),
- **Galois** when algebraic, normal and separable.

Why we need normal

Consider the intermediate field $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{R}/\mathbb{Q}$.

Why we need normal

Consider the intermediate field $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{R}/\mathbb{Q}$.

The minimal polynomial of $\sqrt[3]{2}$ is $X^3 - 2$ whose roots are

$$\sqrt[3]{2} \qquad j\sqrt[3]{2} \qquad -j\sqrt[3]{2}$$

Thus $\mathbb{Q}(\sqrt[3]{2})$ is not normal.

Why we need normal

Consider the intermediate field $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{R}/\mathbb{Q}$.

The minimal polynomial of $\sqrt[3]{2}$ is $X^3 - 2$ whose roots are

$$\sqrt[3]{2} \qquad j\sqrt[3]{2} \qquad -j\sqrt[3]{2}$$

Thus $\mathbb{Q}(\sqrt[3]{2})$ is not normal.

An element $f \in \mathbf{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ has to satisfy

$$f(\sqrt[3]{2})^3 = f((\sqrt[3]{2})^3) = f(2) = 2$$

and therefore $f(\sqrt[3]{2}) = \sqrt[3]{2}$.

Why we need normal

Consider the intermediate field $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{R}/\mathbb{Q}$.

The minimal polynomial of $\sqrt[3]{2}$ is $X^3 - 2$ whose roots are

$$\sqrt[3]{2} \qquad j\sqrt[3]{2} \qquad -j\sqrt[3]{2}$$

Thus $\mathbb{Q}(\sqrt[3]{2})$ is not normal.

An element $f \in \mathbf{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ has to satisfy

$$f(\sqrt[3]{2})^3 = f((\sqrt[3]{2})^3) = f(2) = 2$$

and therefore $f(\sqrt[3]{2}) = \sqrt[3]{2}$.

We have

$$G \circ F(\mathbb{Q}(\sqrt[3]{2})) \quad = \quad G \circ F(\mathbb{Q})$$

Let’s go through this slowly...

Generated extensions

Given an extension L/K and $A \subseteq L$ a subset, we write $K(A)$ for the **extension generated** by A, which can be described as

- the intersection of all extensions of K containing A,
- the subfield of L whose elements are of the form

  $$(P/Q)(a_1, \ldots, a_n)$$

  where P/Q is a rational fraction in $K(X_1, \ldots, X_n)$.

Simple extensions

A **simple extension** in L/K is one of the form $K(a)$ for $a \in L$.

Simple extensions

A **simple extension** in L/K is one of the form $K(a)$ for $a \in L$.

Ex: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ in $\mathbb{R}/\mathbb{Q}$.

Simple extensions

A **simple extension** in L/K is one of the form $K(a)$ for $a \in L$.

Ex: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ in $\mathbb{R}/\mathbb{Q}$.

Proposition

A simple extension $K(a)$ is either of the form

- $K(X)$ if a is transcendental over K,
- $K[X]/I$ if a is algebraic over K where I is the ideal

$$I \quad = \quad \{P \in K[X] \mid P(a) = 0\}$$

Simple extensions

A **simple extension** in L/K is one of the form $K(a)$ for $a \in L$.

Ex: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ in $\mathbb{R}/\mathbb{Q}$.

Proposition

A simple extension $K(a)$ is either of the form

- $K(X)$ if a is transcendental over K,
- $K[X]/I$ if a is algebraic over K where I is the ideal

$$I \quad = \quad \{P \in K[X] \mid P(a) = 0\}$$

Remark

I is the kernel of the evaluation at a (therefore an ideal) whose target is the field K, therefore it is a maximal ideal and $K[X]/I$ is a field.

Simple extensions

In fact, extensions are usually simple:

Theorem (Primitive element theorem)

If L/K is a separable extension of finite degree then it is simple.

Simple extensions

The ring $K[X]$ is always a PID, therefore

$$I \quad = \quad \{P \in K[X] \mid P(a) = 0\} \quad = \quad (\underline{P})$$

i.e. if a is a root of a polynomial over K then there is a **minimal polynomial** $\underline{P}$ with this property.

Simple extensions

The ring $K[X]$ is always a PID, therefore

$$I \quad = \quad \{P \in K[X] \mid P(a) = 0\} \quad = \quad (\underline{P})$$

i.e. if a is a root of a polynomial over K then there is a **minimal polynomial** $\underline{P}$ with this property.

Remark

$\underline{P}$ divides any polynomial Q such that $Q(a) = 0$.

Simple extensions

The ring $K[X]$ is always a PID, therefore

$$I \quad = \quad \{P \in K[X] \mid P(a) = 0\} \quad = \quad (\underline{P})$$

i.e. if a is a root of a polynomial over K then there is a **minimal polynomial** $\underline{P}$ with this property.

Remark

$\underline{P}$ is the only irreducible polynomial with a as root
(up to a non-zero multiplicative constant).

Simple extensions

The ring $K[X]$ is always a PID, therefore

$$I \quad = \quad \{P \in K[X] \mid P(a) = 0\} \quad = \quad (\underline{P})$$

i.e. if a is a root of a polynomial over K then there is a **minimal polynomial** $\underline{P}$ with this property.

Remark

This means that if we add a root of P to K,
we necessarily add all of them.

Simple extensions

The ring $K[X]$ is always a PID, therefore

$$I \quad = \quad \{P \in K[X] \mid P(a) = 0\} \quad = \quad (\underline{P})$$

i.e. if a is a root of a polynomial over K then there is a **minimal polynomial** $\underline{P}$ with this property.

Remark

Every element has a representative as $P(a)$
for some $P \in K[X]$ with $\mathbf{deg}(P) < \mathbf{deg}(\underline{P})$.

Simple extensions

The ring $K[X]$ is always a PID, therefore

$$I \quad = \quad \{P \in K[X] \mid P(a) = 0\} \quad = \quad (\underline{P})$$

i.e. if a is a root of a polynomial over K then there is a **minimal polynomial** $\underline{P}$ with this property.

Remark

Every element has a representative as $P(a)$
for some $P \in K[X]$ with $\deg(P) < \deg(\underline{P})$.

Proposition

Given $K(a)/K$ a simple extension one has

- $[K(a) : K] = \infty$ if a is transcendental,
- $[K(a) : K] = \deg(P)$ where P is the minimal polynomial of a otherwise.

In fact, a basis of $K(a)/K$ consists of the a^i with $0 \leq i < \deg(P)$.

Finite extensions

Lemma

An extension L/K is finite (i.e. $[L : K]$ finite) if and only if L is algebraic over K and $L = L(a_1, \dots, a_n)$.

Finite extensions

Lemma

An extension L/K is finite (i.e. $[L:K]$ finite) if and only if L is algebraic over K and $L = L(a_1, \ldots, a_n)$.

Remark

Every finite extension is algebraic, but an algebraic extension can be infinite. For instance, the set $\mathbb{A}$ of **algebraic numbers**, i.e. those which are algebraic over $\mathbb{Q}$:

$$\mathbb{A} \quad = \quad \{x \in \mathbb{C} \mid P(x) = 0 \text{ for some } P \in \mathbb{Q}[X]\}$$

Ruler and compass

Consider the points you can construct in $\mathbb{R}^2$, starting from two points, by

1. drawing a straight line through two points,
2. drawing circles centered at a point and going through another point,

and taking points at intersections of those.

We write $p_i = (x_i, y_i)$ for the sequence of constructed points, $K_0 = \mathbb{R}$ and $K_{i+1} = K_i(x_i, y_i)$.

Ruler and compass

Consider the points you can construct in $\mathbb{R}^2$, starting from two points, by

1. drawing a straight line through two points,
2. drawing circles centered at a point and going through another point,

and taking points at intersections of those.

We write $p_i = (x_i, y_i)$ for the sequence of constructed points, $K_0 = \mathbb{R}$ and $K_{i+1} = K_i(x_i, y_i)$.

Proposition

The elements x_{i+1} and y_{i+1} are zeros of polynomials of degree one or two in K_i. Therefore, $[K_i : K]$ is a power of two.

Trisecting the angle

Can we trisect an angle with ruler and compass?

Trisecting the angle

Can we trisect an angle with ruler and compass?

- We begin with $p_0 = (0, 0)$ and $p_1 = (1, 0)$.

Trisecting the angle

Can we trisect an angle with ruler and compass?

- We begin with $p_0 = (0, 0)$ and $p_1 = (1, 0)$.
- Trisecting is equivalent to constructing $(\cos(\pi/9), 0)$, and therefore $(a, 0)$ with $a = 2\cos(\pi/9)$.

Trisecting the angle

Can we trisect an angle with ruler and compass?

- We begin with $p_0 = (0, 0)$ and $p_1 = (1, 0)$.
- Trisecting is equivalent to constructing $(\cos(\pi/9), 0)$, and therefore $(a, 0)$ with $a = 2\cos(\pi/9)$.
- Setting $\theta = \pi/9$ in $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$ we have

$$a^3 - 3a - 1 \quad = \quad 0$$

Trisecting the angle

Can we trisect an angle with ruler and compass?

- We begin with $p_0 = (0, 0)$ and $p_1 = (1, 0)$.
- Trisecting is equivalent to constructing $(\cos(\pi/9), 0)$, and therefore $(a, 0)$ with $a = 2\cos(\pi/9)$.
- Setting $\theta = \pi/9$ in $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$ we have

$$a^3 - 3a - 1 \quad = \quad 0$$

- The polynomial is irreducible over $\mathbb{Q}$, i.e. $[\mathbb{Q}(a) : \mathbb{Q}] = 3$.

Trisecting the angle

Can we trisect an angle with ruler and compass?

- We begin with $p_0 = (0, 0)$ and $p_1 = (1, 0)$.
- Trisecting is equivalent to constructing $(\cos(\pi/9), 0)$, and therefore $(a, 0)$ with $a = 2\cos(\pi/9)$.
- Setting $\theta = \pi/9$ in $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$ we have

$$a^3 - 3a - 1 \quad = \quad 0$$

- The polynomial is irreducible over $\mathbb{Q}$, i.e. $[\mathbb{Q}(a) : \mathbb{Q}] = 3$.
- Contradiction.

Squaring the circle

Can we square the circle?

Squaring the circle

Can we square the circle?

- We begin with $p_0 = (0, 0)$ and $p_1 = (1, 0)$.
- We should be able to construct $(\sqrt{\pi}, 0)$ and therefore $(\pi, 0)$.
- This would imply that $[\mathbb{Q}(\pi) : \mathbb{Q}]$ is a power of two, but we know that π is not algebraic over $\mathbb{Q}$.
- Contradiction.

For the rest, we should rely on subtler invariants than size...

We should take *symmetries* in account!

General idea

Suppose that we want to make a simple algebraic extension $K(a)/K$, where P is the minimal polynomial of a.

We may not be able to distinguish between a and another root of P: more precisely, there will be an action of the Galois group.

Splitting fields

A polynomial P **splits** over K when $P = a(X - a_1)\dots(X - a_n)$.

Splitting fields

A polynomial P **splits** over K when $P = a(X - a_1)\dots(X - a_n)$.

The **splitting field** L of P over K is the smallest extension L/K such that P splits over L.

Splitting fields

A polynomial P **splits** over K when $P = a(X - a_1)\dots(X - a_n)$.

The **splitting field** L of P over K is the smallest extension L/K such that P splits over L.

Lemma

For any $P \in K[X]$, the splitting field exists and is unique up to isomorphism.

Proof.

Iteratively formally add roots of irreducible factors Q of P to K, i.e. take $K[x]/(Q)$, until P splits. □

Separable extensions

An irreducible polynomial is **separable** over K if it has only simple roots in a splitting field.

Separable extensions

An irreducible polynomial is **separable** over K if it has only simple roots in a splitting field.

A polynomial is separable when all its irreducible factors are.
An algebraic extension is separable when the minimal polynomial over every element is.

Separable extensions

An irreducible polynomial is **separable** over K if it has only simple roots in a splitting field.

A polynomial is separable when all its irreducible factors are.
An algebraic extension is separable when the minimal polynomial over every element is.

Lemma

a is a multiple root of $P \neq 0$ if and only if $P(a) = 0$ and $P'(a) = 0$.

Separable extensions

An irreducible polynomial is **separable** over K if it has only simple roots in a splitting field.

A polynomial is separable when all its irreducible factors are.
An algebraic extension is separable when the minimal polynomial over every element is.

Lemma

a is a multiple root of $P \neq 0$ if and only if $P(a) = 0$ and $P'(a) = 0$.

Lemma

In characteristic 0, every irreducible polynomial is separable.

Normal extensions

An extension L/K is **normal** if every irreducible polynomial with at least one zero in L splits over L.

Normal extensions

An extension L/K is **normal** if every irreducible polynomial with at least one zero in L splits over L.

The **normal closure** of an algebraic extension L/K is the smallest normal algebraic extension of L.

Normal extensions

An extension L/K is **normal** if every irreducible polynomial with at least one zero in L splits over L.

The **normal closure** of an algebraic extension L/K is the smallest normal algebraic extension of L.

Two elements are **conjugate** if they are roots of the same minimal polynomial.

Normal extensions

An extension L/K is **normal** if every irreducible polynomial with at least one zero in L splits over L.

The **normal closure** of an algebraic extension L/K is the smallest normal algebraic extension of L.

Two elements are **conjugate** if they are roots of the same minimal polynomial.

Proposition

With K separable, the normal closure of $K(a_1, \ldots, a_n)$, a finite extension of K, can be obtained by adding all conjugate of the a_i.

Normal extensions

An extension L/K is **normal** if every irreducible polynomial with at least one zero in L splits over L.

The **normal closure** of an algebraic extension L/K is the smallest normal algebraic extension of L.

Two elements are **conjugate** if they are roots of the same minimal polynomial.

Proposition

With K separable, the normal closure of $K(a_1, \dots, a_n)$, a finite extension of K, can be obtained by adding all conjugate of the a_i.

Proposition

When K is separable, a finite extension L/K is normal if and only if L is the splitting field for some polynomial over K.

Normal extensions

An extension L/K is **normal** if every irreducible polynomial with at least one zero in L splits over L.

The **normal closure** of an algebraic extension L/K is the smallest normal algebraic extension of L.

Two elements are **conjugate** if they are roots of the same minimal polynomial.

Proposition

With K separable, the normal closure of $K(a_1, \dots, a_n)$, a finite extension of K, can be obtained by adding all conjugate of the a_i.

Proposition

A finite extension L/K is normal iff the action of $\mathrm{Aut}(L/K)$ on the conjuguates of an element of K is transitive.

Normal extensions

An extension L/K is **normal** if every irreducible polynomial with at least one zero in L splits over L.

The **normal closure** of an algebraic extension L/K is the smallest normal algebraic extension of L.

Two elements are **conjugate** if they are roots of the same minimal polynomial.

Proposition

With K separable, the normal closure of $K(a_1, \dots, a_n)$, a finite extension of K, can be obtained by adding all conjugate of the a_i.

Proposition (???)

A finite extension L/K is separated iff the action of $\mathrm{Aut}(L/K)$ on the conjuguates of an element of K is faithful.

The fundamental theorem

Theorem (Galois)

When L/K is a finite, separable and normal extension, we have an isomorphism

$$\begin{tikzcd}
\mathrm{Aut}(L /\!\!/ K) \arrow[rr, bend left, "F"] \arrow[rr, phantom, "\perp"] & & (L /\!\!/ K)^{\mathrm{op}} \arrow[ll, bend left, "G"]
\end{tikzcd}$$

Back to Galois

Given a polynomial P over K with splitting field L, its **Galois group** is $\mathrm{Aut}(L/K)$.

Back to Galois

Given a polynomial P over K with splitting field L, its **Galois group** is $\mathrm{Aut}(L/K)$.

Given $f \in \mathrm{Aut}(L/K)$, and a such that $P(a) = 0$, we have

$$f(P(a)) = P(f(a)) = 0$$

so that f permutes the zeros of P: i.e. *exchanges conjugate elements*. Conversely, since L is generated by roots of P such a permutation determines an element of $\mathrm{Aut}(L/K)$.

Back to Galois

Given a polynomial P over K with splitting field L, its **Galois group** is $\mathrm{Aut}(L/K)$.

Given $f \in \mathrm{Aut}(L/K)$, and a such that $P(a) = 0$, we have

$$f(P(a)) = P(f(a)) = 0$$

so that f permutes the zeros of P: i.e. *exchanges conjugate elements*. Conversely, since L is generated by roots of P such a permutation determines an element of $\mathrm{Aut}(L/K)$.

The group $\mathrm{Aut}(L/K)$ can thus be seen as a group of permutation of roots of P (this was Galois' original definition).

An example

Consider $P = X^4 - 2$ over $\mathbb{Q}$, and consider its splitting field $K/\mathbb{Q}$.

An example

Consider $P = X^4 - 2$ over $\mathbb{Q}$, and consider its splitting field $K/\mathbb{Q}$.

In $\mathbb{C}$, we have

$$P \quad = \quad (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2})$$

Therefore

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

Since we are in characteristic 0, K is separable.
This is a splitting field, thus a normal extension.

An example

Consider $P = X^4 - 2$ over $\mathbb{Q}$, and consider its splitting field $K/\mathbb{Q}$.

In $\mathbb{C}$, we have

$$P \quad = \quad (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2})$$

Therefore

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

Since we are in characteristic 0, K is separable.
This is a splitting field, thus a normal extension.

Its degree is

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \times 4 = 8$$

(minimal polynomials are respectively, $X^2 - 1$ and $X^4 - 2$).

An example

The elements $f \in \mathsf{Aut}(K/\mathbb{Q})$ have to satisfy

$$f(i) \in \{i, -i\} \qquad\qquad f(\sqrt[4]{2}) \in \left\{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\right\}$$

and all possible combinations are suitable.

An example

The elements $f \in \mathrm{Aut}(K/\mathbb{Q})$ have to satisfy

$$f(i) \in \{i, -i\} \qquad\qquad f(\sqrt[4]{2}) \in \left\{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\right\}$$

and all possible combinations are suitable.

We can even work out a presentation with generators r, s

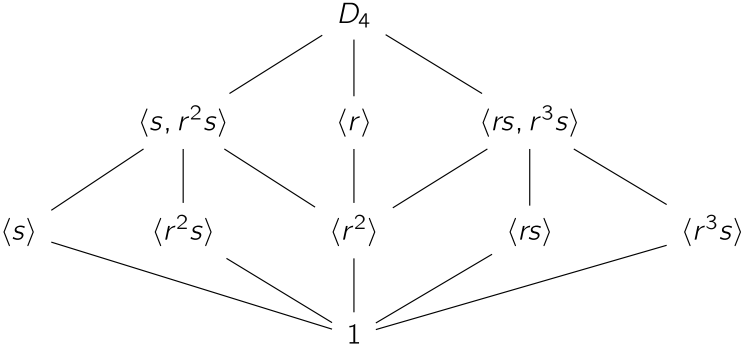
$$r(i) = i \qquad r(\sqrt[4]{2}) = i\sqrt[4]{2} \qquad\qquad s(i) = -i \qquad s(\sqrt[4]{2}) = \sqrt[4]{2}$$

namely

$$\mathrm{Aut}(K/\mathbb{Q}) \quad = \quad \langle r, s \mid r^4 = 1, s^2 = 1, srsr = 1 \rangle \quad = \quad D_4$$

An example

The subgroups of $\mathrm{Aut}(K/Q) = D_4$ are



An example

The intermediate extensions of K/Q are

$$\begin{tikzcd}
 & & \mathbb{Q}(i, \sqrt[4]{2}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & \\
 & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(i\sqrt{2}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt[4]{2}) \arrow[drr, dash] & \mathbb{Q}(i\sqrt[4]{2}) \arrow[dr, dash] & \mathbb{Q}(i, \sqrt{2}) \arrow[d, dash] & \mathbb{Q}(...) \arrow[dl, dash] & \mathbb{Q}(...) \arrow[dll, dash] \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

Radical extensions

An extension L/K is **radical** when $L = K(a_1, \ldots, a_k)$ with

$$a_i^{n_i} \quad \in \quad K(a_1, \ldots, a_{i-1})$$

for some $n_i \in \mathbb{N}$, i.e. L can be obtained from K by adjoining a sequence of n_i-th roots.

Radical extensions

An extension L/K is **radical** when $L = K(a_1, \ldots, a_k)$ with

$$a_i^{n_i} \quad \in \quad K(a_1, \ldots, a_{i-1})$$

for some $n_i \in \mathbb{N}$, i.e. L can be obtained from K by adjoining a sequence of n_i-th roots.

[Characteristic 0 from now on.]

Radical extensions

An extension L/K is **radical** when $L = K(a_1, \dots, a_k)$ with

$$a_i^{n_i} \quad \in \quad K(a_1, \dots, a_{i-1})$$

for some $n_i \in \mathbb{N}$, i.e. L can be obtained from K by adjoining a sequence of n_i-th roots.

[Characteristic 0 from now on.]

A polynomial $P \in K[X]$ is **solvable by radicals** when its splitting field is an intermediate field of a radical extension L/K.

Radical extensions

An extension L/K is **radical** when $L = K(a_1, \ldots, a_k)$ with

$$a_i^{n_i} \quad \in \quad K(a_1, \ldots, a_{i-1})$$

for some $n_i \in \mathbb{N}$, i.e. L can be obtained from K by adjoining a sequence of n_i-th roots.

[Characteristic 0 from now on.]

A polynomial $P \in K[X]$ is **solvable by radicals** when its splitting field is an intermediate field of a radical extension L/K.

Theorem

An separable extension L/K is radical if and only if $\mathrm{Aut}(L/K)$ *is solvable.*

Solvable groups

A group G is **solvable** if there exists subgroups

$$1 = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n = G$$

such that

- G_i is a normal subgroup of G_{i+1},
- G_{i+1}/G_i is abelian

Solvable groups

A group G is **solvable** if there exists subgroups

$$1 \quad = \quad G_0 \quad \subseteq \quad G_1 \quad \subseteq \quad \ldots \quad \subseteq \quad G_n \quad = \quad G$$

such that

- G_i is a normal subgroup of G_{i+1},
- G_{i+1}/G_i is abelian

(when G is finite G_{i+1}/G_i simple abelian iff cyclic of prime order).

Solvable groups

A group G is **solvable** if there exists subgroups

$$1 = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$$

such that

- G_i is a normal subgroup of G_{i+1},
- G_{i+1}/G_i is abelian

(when G is finite G_{i+1}/G_i simple abelian iff cyclic of prime order).

Remark

The relation "being a normal subgroup" is not transitive.

Solvable groups

A group G is **solvable** if there exists subgroups

$$1 = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n = G$$

such that

- G_i is a normal subgroup of G_{i+1},
- G_{i+1}/G_i is abelian

(when G is finite G_{i+1}/G_i simple abelian iff cyclic of prime order).

Remark

The relation "being a normal subgroup" is not transitive.

Proposition

The symmetric groups S_n are solvable only for $n < 5$.

Idea of the proof

Lemma

Write L for the splitting field of $P = X^p - 1$ with p prime.
The Galois group $\mathrm{Aut}(L/K)$ is abelian.

Proof.

- Since $P' = pX^{p-1}$, P and P' have not zeros in common, therefore P has only simple zeros.
- Thus the group of roots of P is cyclic of order p.
- Writing a for a root, $L = K(a)$ and $f \in \mathrm{Aut}(L/K)$ is determined by $f(a)$ which should be in $\{a^i\}$.
- Writing f_i for the automorphism such that $f_i(a) = a^i$, we have $f_j \circ f_i(a) = f_i \circ f_j(a) = a^{ij}$ and therefore any two elements of $\mathrm{Aut}(L/K)$ commute. □

Idea of the proof

Lemma

Given a field K in which $X^n - 1$ splits, $a \in K$, and L the splitting field for $X^n - a$ over K, then $\mathrm{Aut}(L/K)$ is abelian.

Proof.

- Given b such that $b^n = a$, the roots of $X^n - a$ are of the form $u^i b$ with u a root of $X^n - 1$.
- Automorphisms are of the form f_i with $f_i(b) = u^i b$ and

  $$f_j \circ f_i(b) = u^{i+j} b$$

  they thus commute. ☐

Idea of the proof

Theorem

If a separable extension L/K is radical then $\mathrm{Aut}(L/K)$ is solvable.

Proof.

Given a radical extension L/K:

- we can suppose that we only take roots of prime powers,
- we take the normal closure of L,
- the splitting field of $X^n - a$ splits $X^n - 1$,
- we apply previous lemmas. ☐

An insoluble polynomial

Consider $P = X^5 - 6X + 3$ over $\mathbb{Q}$.

An insoluble polynomial

Consider $P = X^5 - 6X + 3$ over $\mathbb{Q}$.

Its Galois group is S_5, which is not solvable.

An insoluble polynomial

Consider $P = X^5 - 6X + 3$ over $\mathbb{Q}$.

Its Galois group is S_5, which is not solvable.

Therefore, P is not solvable by radicals.

Primitives

Note that this result is really due to the fact that our primitive for computing are **radicals**, i.e. roots of

$$X^n - a$$

Primitives

Note that this result is really due to the fact that our primitive for computing are **radicals**, i.e. roots of

$$X^n - a$$

For instance, an **ultraradical** is the real solution of

$$X^5 + X - a$$

Every quintic is solvable with radicals and ultraradicals.

Can we use symmetry to show that
some tasks cannot be implemented?

The Galois task

A **task** is a polynomial P for which we want to find a root.

The Galois task

A **task** is a polynomial P for which we want to find a root.

A **process** is a program consisting of a loop which iteratively

- computes some new values from previously computed ones using $+$ and $\times$,
- calls an external procedure which computes a y such that $y^n = x$,

and outputs a value after a number of iterations.

The Galois task

A **task** is a polynomial P for which we want to find a root.

A **process** is a program consisting of a loop which iteratively

- computes some new values from previously computed ones using $+$ and $\times$,
- calls an external procedure which computes a y such that $y^n = x$,

and outputs a value after a number of iterations.

Can every task be solved by a process?

Where can we find symmetries?

Sources of symmetry:

- high-level programming languages can manipulate memory locations, but the implementation guarantees that the behavior will not depend on the chosen locations:

  invariance under action of the symmetric group on memory!

Where can we find symmetries?

Sources of symmetry:

- high-level programming languages can manipulate memory locations, but the implementation guarantees that the behavior will not depend on the chosen locations:

  invariance under action of the symmetric group on memory!

- there can be a symmetry between the various inputs of a programs.

COVERING SPACES

Covering maps

A continuous map $p : E \to B$ between topological spaces is **covering** when every point $x \in B$ has an neighborhood U such that

$$p^{-1}(U) \quad \cong \quad \coprod_{i \in I} U$$

for some set I.

Covering maps

A continuous map $p : E \to B$ between topological spaces is **covering** when every point $x \in B$ has an neighborhood U such that

$$p^{-1}(U) \quad \cong \quad \coprod_{i \in I} U$$

for some set I.

The set $p^{-1}(x)$ is called the **fiber** over x.

Pointed covers

A *pointed space* (X, x) is a space X together with $x \in X$.

A *pointed morphism* $f : (X, x) \to (Y, y)$ is a morphism $f : X \to Y$ such that $f(x) = y$.

We write $\mathbf{Top}_\bullet$ for the resulting category.

A *pointed covering* is a pointed morphism which is also covering.

The universal cover

Given a pointed space (B, b), consider the full subcategory of

$$\mathbf{Top}_\bullet/(B, b)$$

whose objects are pointed covering $p : (E, e) \to (B, b)$.

The universal cover

Given a pointed space (B, b), consider the full subcategory of

$$\mathbf{Top}_\bullet/(B, b)$$

whose objects are pointed covering $p : (E, e) \to (B, b)$.

A **universal cover** is an initial object in this category.

The universal cover

Given a pointed space (B, b), consider the full subcategory of

$$\mathbf{Top}_\bullet/(B, b)$$

whose objects are pointed covering $p : (E, e) \to (B, b)$.

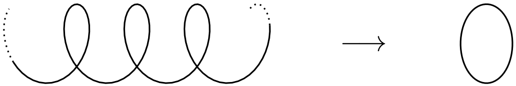
A **universal cover** is an initial object in this category.

Remark

It is not hard to show that morphisms of the above category are covering.

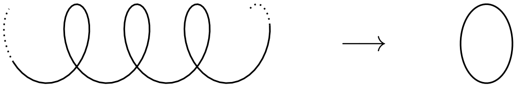
The universal cover

When B is "reasonable" (connected, locally path-connected and semilocally simply connected) the universal cover exists and can be described as the space whose points are homotopy classes of paths in B originating in b.



The universal cover

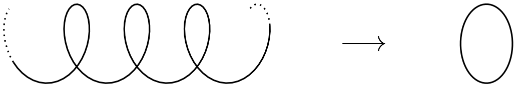
When B is “reasonable” (connected, locally path-connected and semilocally simply connected) the universal cover exists and can be described as the space whose points are homotopy classes of paths in B originating in b.



This construction does not depend on the choice of b in its connected component.

The universal cover

When B is “reasonable” (connected, locally path-connected and semilocally simply connected) the universal cover exists and can be described as the space whose points are homotopy classes of paths in B originating in b.



This construction does not depend on the choice of b in its connected component.

It can be characterized as the *simply connected* pointed cover of (B, b).

The universal cover

When B is connected, the universal cover does not depend on the base point b.

We will be in this case in the following and forget about the base point (otherwise consider connected components).

The universal cover

When B is connected, the universal cover does not depend on the base point b.

We will be in this case in the following and forget about the base point (otherwise consider connected components).

We will also suppose that covering spaces we consider are connected.

Deck transformations

A **deck transformation** of a covering $p : E \to B$ is a homeomorphism $f : E \to E$ such that

$$p \circ f \quad = \quad p$$

Deck transformations

A **deck transformation** of a covering $p : E \to B$ is a homeomorphism $f : E \to E$ such that

$$p \circ f \quad = \quad p$$

This means that f permutes points within fibers.

Deck transformations

A **deck transformation** of a covering $p : E \to B$ is a homeomorphism $f : E \to E$ such that

$$p \circ f \quad = \quad p$$

This means that f permutes points within fibers.

We write $\mathrm{Aut}(p)$ for the **deck group**.

The fundamental theorem

Given an universal cover $p : (\tilde{X}, \tilde{x}) \to (X, x)$, there is an isomorphism

$$\pi_1(X, x) \quad \cong \quad \mathsf{Aut}(p)$$

The fundamental theorem

Given an universal cover $p : (\tilde{X}, \tilde{x}) \to (X, x)$, there is an isomorphism

$$\pi_1(X, x) \quad \cong \quad \mathrm{Aut}(p)$$

There is a bijective correspondence between

- subgroups of $\pi_1(X, x)$,
- coverings of (X, x).

$$\begin{tikzcd}
\mathrm{Aut}(p) \arrow[rr, bend left, "F"] & & (\mathbf{Cov}(X))^{\mathrm{op}} \arrow[ll, bend left, "G"]
\end{tikzcd}$$

Let’s detail this…

The fundamental groupoid

Given a space X, its **fundamental groupoid** $\Pi_1(X)$ is the category whose objects are points in X and morphisms

$$f \quad : \quad x \quad \twoheadrightarrow \quad y$$

are paths up to homotopy.

The fundamental groupoid

Given a space X, its **fundamental groupoid** $\Pi_1(X)$ is the category whose objects are points in X and morphisms

$$f \quad : \quad x \quad \twoheadrightarrow \quad y$$

are paths up to homotopy.

For every object x, the endomorphisms form a group

$$\pi_1(X, x) \quad = \quad \Pi_1(X)(x, x)$$

The fundamental groupoid

Given a space X, its **fundamental groupoid** $\Pi_1(X)$ is the category whose objects are points in X and morphisms

$$f \quad : \quad x \quad \twoheadrightarrow \quad y$$

are paths up to homotopy.

For every object x, the endomorphisms form a group

$$\pi_1(X, x) \quad = \quad \Pi_1(X)(x, x)$$

X being connected, for every points x, y, there exists a morphism $f : x \twoheadrightarrow y$. It induces a group isomorphism

$$\begin{array}{rcl} \pi_1(X, x) & \to & \pi_1(X, y) \\ g & \mapsto & f \circ g \circ f^{-1} \end{array}$$

The fundamental groupoid

This construction is functorial

$$\mathbf{Top} \quad \to \quad \mathbf{Gpd}$$

The fundamental groupoid

This construction is functorial

$$\mathbf{Top} \quad \to \quad \mathbf{Gpd}$$

A continuous function

$$f \quad : \quad X \quad \to \quad Y$$

induces a functor

$$f_* \quad : \quad \Pi_1(X) \quad \to \quad \Pi_1(Y)$$

The fundamental groupoid

This construction is functorial

$$\mathbf{Top} \quad \to \quad \mathbf{Gpd}$$

A continuous function

$$f \quad : \quad X \quad \to \quad Y$$

induces a functor

$$f_* \quad : \quad \Pi_1(X) \quad \to \quad \Pi_1(Y)$$

and thus a group morphism

$$f_* \quad : \quad \pi_1(X, x) \quad \to \quad \pi_1(Y, f(x))$$

The homotopy lifting property

Proposition

Given a covering $p : E \to B$, a homotopy $f : X \times I \to B$ and a lifting $\tilde{f}_0 : X \to E$, there exists a homotopy $\tilde{f} : X \times I \to E$ such that

$$\begin{tikzcd}
X \arrow[r, "\tilde{f}_0"] \arrow[d, "\mathrm{id} \times 0"'] & E \arrow[d, "p"] \\
X \times I \arrow[r, "f"'] \arrow[ur, dotted, "\tilde{f}"] & B
\end{tikzcd}$$

The homotopy lifting property

Proposition

Given a covering $p : E \to B$, a homotopy $f : X \times I \to B$ and a lifting $\tilde{f}_0 : X \to E$, there exists a homotopy $\tilde{f} : X \times I \to E$ such that

$$\begin{tikzcd}
X \arrow[r, "\tilde{f}_0"] \arrow[d, "\mathrm{id} \times 0"'] & E \arrow[d, "p"] \\
X \times I \arrow[r, "f"'] \arrow[ru, dotted, "\tilde{f}"] & B
\end{tikzcd}$$

For instance,

- with $X = \{*\}$, we get the **path lifting property**.
- with $X = I$, we can lift homotopies between paths,
- etc.

Faithfulness

The induced functor is always faithful:

$$p_* \quad : \quad \Pi_1(E) \quad \to \quad \Pi_1(B)$$

Faithfulness

The induced functor is always faithful:

$$p_* \quad : \quad \Pi_1(E) \quad \to \quad \Pi_1(B)$$

We can thus see $\pi_1(E, e)$ as a subgroup of $\pi_1(B, b)$.

The action of $\pi_1(X)$

By the path lifting property, every path

$$f \quad : \quad x \quad \twoheadrightarrow \quad y$$

induces a function

$$p^{-1}(x) \quad \to \quad p^{-1}(y)$$

sending $\tilde{x} \in p^{-1}(x)$ to the endpoint $\tilde{y}$ of the path

$$\tilde{f} \quad : \quad \tilde{x} \quad \twoheadrightarrow \quad \tilde{y}$$

lifting f from $\tilde{x}$.

The action of $\pi_1(X)$

By the path lifting property, every path

$$f \quad : \quad x \quad \twoheadrightarrow \quad y$$

induces a function

$$p^{-1}(x) \quad \to \quad p^{-1}(y)$$

sending $\tilde{x} \in p^{-1}(x)$ to the endpoint $\tilde{y}$ of the path

$$\tilde{f} \quad : \quad \tilde{x} \quad \twoheadrightarrow \quad \tilde{y}$$

lifting f from $\tilde{x}$.

By the homotopy lifting property, two homotopic paths give rise to the same function.

The action of $\pi_1(X)$

We thus get a functor

$$p^* \quad : \quad \Pi_1(X) \quad \to \quad \mathbf{Set}$$

such that

$$p^*(x) \quad = \quad p^{-1}(x)$$

and for $f : x \twoheadrightarrow y$ the function

$$p^*(f) \quad : \quad p^*(x) \quad \to \quad p^*(y)$$

is the previously described one.

The action of $\pi_1(X)$

We thus get a functor

$$p^* \quad : \quad \Pi_1(X) \quad \to \quad \mathbf{Set}$$

such that

$$p^*(x) \quad = \quad p^{-1}(x)$$

and for $f : x \twoheadrightarrow y$ the function

$$p^*(f) \quad : \quad p^*(x) \quad \to \quad p^*(y)$$

is the previously described one.

Since X is connected, we obtain for instance that any two fibers are isomorphic: their cardinal is called the **degree** of the cover.

Lifting morphisms

An automorphism $g \in \mathsf{Aut}(p)$ gives rise to an isomorphism on the set $p^{-1}(x)$, i.e. we have a group morphism

$$\mathsf{Aut}(p) \quad \to \quad \mathsf{Iso}(p^{-1}(x))$$

Lifting morphisms

An automorphism $g \in \mathsf{Aut}(p)$ gives rise to an isomorphism on the set $p^{-1}(x)$, i.e. we have a group morphism

$$\mathsf{Aut}(p) \quad \to \quad \mathsf{Iso}(p^{-1}(x))$$

Which isomorphisms come from such an automorphism?

Lifting morphisms

An automorphism $g \in \mathsf{Aut}(p)$ gives rise to an isomorphism on the set $p^{-1}(x)$, i.e. we have a group morphism

$$\mathsf{Aut}(p) \quad \to \quad \mathsf{Iso}(p^{-1}(x))$$

Which isomorphisms come from such an automorphism?

In fact, we will see that such an automorphism is determined by the image of one element of $p^{-1}(x)$.

Lifting morphisms

Theorem

Given a covering $p : E \to B$, a continuous $f : X \to B$, $x \in X$ and $e \in p^{-1}(f(x))$,

$$\begin{tikzcd} & E \arrow[d, "p"] \\ X \arrow[ur, dotted, "g"] \arrow[r, "f"'] & B \end{tikzcd}$$

there exists g such that $p \circ g = f$ and $g(x) = e$ if and only if

$$f_*(\pi_1(X, x)) \subseteq p_*(\pi_1(E, e))$$

and in this case g is unique.

Lifting morphisms

Theorem

Given a covering $p : E \to B$*, a continuous* $f : X \to B$*,* $x \in X$ *and* $e \in p^{-1}(f(x))$*,*

$$\begin{tikzcd}
& E \arrow[d, "p"] \\
X \arrow[ru, dotted, "g"] \arrow[r, "f"'] & B
\end{tikzcd}$$

there exists g *such that* $p \circ g = f$ *and* $g(x) = e$ *if and only if*

$$f_*(\pi_1(X, x)) \subseteq p_*(\pi_1(E, e))$$

and in this case g *is unique.*

Proof.

Given a path $x \twoheadrightarrow y$ in X, its image by f has a lifting $\tilde{x} \twoheadrightarrow \tilde{y}$ under p and we set $g(x) = \tilde{y}$. The condition ensure that this does not depend on the path. □

Lifting morphisms

Theorem

Given a covering $p : E \to B$, *a continuous* $f : X \to B$, $x \in X$ *and* $e \in p^{-1}(f(x))$,

$$\begin{tikzcd} & E \arrow[d, "p"] \\ X \arrow[ur, dotted, "g"] \arrow[r, "f"'] & B \end{tikzcd}$$

there exists g *such that* $p \circ g = f$ *and* $g(x) = e$ *if and only if*

$$f_*(\pi_1(X, x)) \subseteq p_*(\pi_1(E, e))$$

and in this case g *is unique.*

Remark

When X is simply connected, the condition is always satisfied!

Lifting morphisms

We can apply the theorem to

$$\begin{tikzcd}
 & E \arrow[d, "p"] \\
E \arrow[ur, dotted, "g"] \arrow[r, "p"'] & B
\end{tikzcd}$$

and deduce that, given $x \in E$, a p-automorphism g is uniquely determined by the image $g(x)$, and any $y \in E$ such that

$$p_*(\pi_1(E, x)) \quad = \quad p_*(\pi_1(E, y))$$

is possible as value for $g(x)$.

Automorphisms of the universal covering

In particular, if $p : E \to B$ is the universal covering,

Automorphisms of the universal covering

In particular, if $p : E \to B$ is the universal covering,

- a point $y \in E$ such that $p(y) = p(x)$ corresponds to an element of $\pi_1(X, x)$,

Automorphisms of the universal covering

In particular, if $p : E \to B$ is the universal covering,

- a point $y \in E$ such that $p(y) = p(x)$ corresponds to an element of $\pi_1(X, x)$,
- $\pi_1(E, y) = 0$.

Automorphisms of the universal covering

In particular, if $p : E \to B$ is the universal covering,

- a point $y \in E$ such that $p(y) = p(x)$ corresponds to an element of $\pi_1(X, x)$,
- $\pi_1(E, y) = 0$.

We thus have

$$\mathrm{Aut}(p) \quad \cong \quad \pi_1(X, x)$$

Galois theory

Theorem

There is a bijective correspondence between

- *subgroups of* $\pi_1(X, x)$,
- *coverings of* (X, x).

$$\mathrm{Aut}(p) \quad \cong \quad (\mathbf{Cov}(X))^{\mathrm{op}}$$

Proof.

To a subgroup of $G \subseteq \mathrm{Aut}(p)$, we associate the covering

$$p/G \quad : \quad \tilde{X}/G \to X$$

where $p : \tilde{X} \to X$ is the universal covering.

To a covering $q : Y \to X$, we associate $q_*(\pi_1(Y, y))$ for some $y \in p^{-1}(x)$. ☐

Degree and index

The **index** $|G : H|$ of a subgroup $H \subseteq G$ is the number of cosets gH of H in G:

Degree and index

The **index** $|G : H|$ of a subgroup $H \subseteq G$ is the number of cosets gH of H in G:

- when G is finite $|G : H| = |G|/|H|$,

Degree and index

The **index** $|G : H|$ of a subgroup $H \subseteq G$ is the number of cosets gH of H in G:

- when G is finite $|G : H| = |G|/|H|$,
- when H is normal $|G : H| = |G/H|$.

Degree and index

The **index** $|G : H|$ of a subgroup $H \subseteq G$ is the number of cosets gH of H in G:

- when G is finite $|G : H| = |G|/|H|$,
- when H is normal $|G : H| = |G/H|$.

Proposition

The degree of a covering is the index of the corresponding subgroup in $\pi_1(X, x)$.

Normal covering

A covering $p : (\tilde{X}, \tilde{x}) \to (X, x)$ is **normal** if its action on the fiber $p^{-1}(x)$ is **transitive**:

$$\forall y, z \in p^{-1}(x), \exists f \in \mathrm{Aut}(p), \quad y \cdot f = z$$

Normal covering

A covering $p : (\tilde{X}, \tilde{x}) \to (X, x)$ is **normal** if its action on the fiber $p^{-1}(x)$ is **transitive**:

$$\forall y, z \in p^{-1}(x), \exists f \in \mathrm{Aut}(p), \quad y \cdot f = z$$

Proposition

A normal covering p corresponds to a normal subgroup G of $\pi_1(X, x)$ and we have

$$\mathrm{Aut}(p) \quad \cong \quad \pi_1(X, x)/G$$

Normal covering

A covering $p : (\tilde{X}, \tilde{x}) \to (X, x)$ is **normal** if its action on the fiber $p^{-1}(x)$ is **transitive**:

$$\forall y, z \in p^{-1}(x), \exists f \in \mathrm{Aut}(p), \quad y \cdot f = z$$

Proposition

A normal covering p corresponds to a normal subgroup G of $\pi_1(X, x)$ and we have

$$\mathrm{Aut}(p) \quad \cong \quad \pi_1(X, x)/G$$

The intuition of a normal covering: a given loop gets unfolded a given number of time, uniformly.

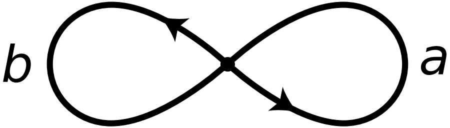
Separated covering

A covering is **separated** when the action is free...

...which is always the case (as we have seen).

An example

Consider the space $X = S_1 \vee S_1$:

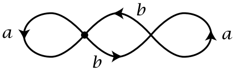


Its fundamental group is

$$\pi_1(X) \quad = \quad \langle a, b \mid \, \rangle$$

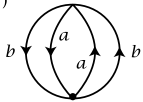
Some fundamental groups

(1)



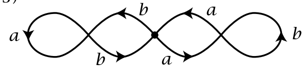
$\langle a,\ b^2, bab^{-1}\rangle$

(2)



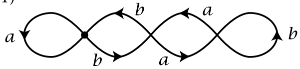
$\langle a^2, b^2, ab\rangle$

(3)



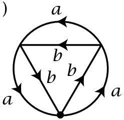
$\langle a^2, b^2, aba^{-1}, bab^{-1}\rangle$

(4)



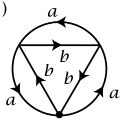
$\langle a, b^2, ba^2b^{-1}, baba^{-1}b^{-1}\rangle$

(5)



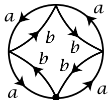
$\langle a^3, b^3, ab^{-1}, b^{-1}a\rangle$

(6)



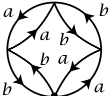
$\langle a^3, b^3, ab, ba\rangle$

(7)



$\langle a^4, b^4, ab, ba, a^2b^2\rangle$

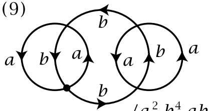
(8)



$\langle a^2, b^2, (ab)^2, (ba)^2, ab^2a\rangle$

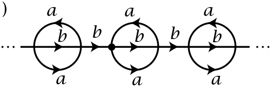
Some fundamental groups

(9)



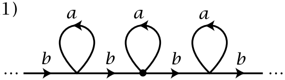
$\langle a^2, b^4, ab, ba^2b^{-1}, bab^{-2}\rangle$

(10)



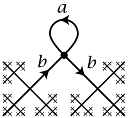
$\langle b^{2n}ab^{-2n-1}, b^{2n+1}ab^{-2n} \mid n \in \mathbb{Z}\rangle$

(11)



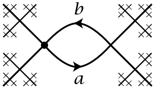
$\langle b^nab^{-n} \mid n \in \mathbb{Z}\rangle$

(12)



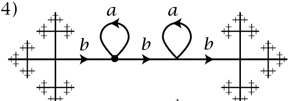
$\langle a\rangle$

(13)



$\langle ab\rangle$

(14)



$\langle a, bab^{-1}\rangle$

Let's try to drop
connectedness assumptions
(on E and on B)

Subgroups vs transitive actions

We have seen that

$$\begin{array}{c} \text{connected covering spaces} \\ \text{of } B \end{array} \quad \cong \quad \begin{array}{c} \text{subgroups} \\ \text{of } \pi_1(B) \end{array}$$

Subgroups vs transitive actions

We have seen that

$$\begin{array}{c}\text{connected covering spaces}\\ \text{of } B\end{array} \quad \cong \quad \begin{array}{c}\text{subgroups}\\ \text{of } \pi_1(B)\end{array}$$

This can be reformulated as

$$\begin{array}{c}\text{connected covering spaces}\\ \text{of } B \text{ with fiber } F\end{array} \quad \cong \quad \begin{array}{c}\text{transitive actions}\\ \text{of } \pi_1(B) \text{ on } F\end{array}$$

Subgroups vs transitive actions

The two points of view are the same on connected coverings:

- given $H \subseteq \pi_1(B)$, we define

$$F \quad = \quad \pi_1(B)/H$$

Subgroups vs transitive actions

The two points of view are the same on connected coverings:

- given $H \subseteq \pi_1(B)$, we define

$$F \quad = \quad \pi_1(B)/H$$

- given an action $\pi_1(B) \times F \to F$, we define

$$H \quad = \quad \mathsf{Stab}(x) \quad = \quad \{y \in \pi_1(B) \mid y \cdot x = x\}$$

  for some $x \in F$.

Non-connected covering spaces

We have seen that

connected covering spaces of B with fiber F	$\cong$	transitive actions of $\pi_1(B)$ on F

Non-connected covering spaces

We have seen that

connected covering spaces of B with fiber F	$\cong$	transitive actions of $\pi_1(B)$ on F

If we consider non-connected covers (but B still is), we get

covering spaces of B with fiber F	$\cong$	actions of $\pi_1(B)$ on F

Non-connected covering spaces

We have seen that

$$\begin{array}{c}\text{connected covering spaces}\\ \text{of } B \text{ with fiber } F\end{array} \quad \cong \quad \begin{array}{c}\text{transitive actions}\\ \text{of } \pi_1(B) \text{ on } F\end{array}$$

If we consider non-connected E and B, we get

$$\begin{array}{c}\text{covering spaces}\\ \text{of } B \text{ with fiber } F\end{array} \quad \cong \quad \begin{array}{c}\text{functors}\\ \Pi_1(B) \to \mathbf{Set}\end{array}$$

More categorically

In fact, this has mostly nothing to do with topology: everything can be done at the level of the fundamental groupoid $\pi_1(X)$.

More categorically

In fact, this has mostly nothing to do with topology: everything can be done at the level of the fundamental groupoid $\pi_1(X)$.

A functor $F : \mathcal{E} \to \mathcal{B}$ between groupoids is **covering**, or a **discrete opfibration**, when for every $f : x \to y$ in $\mathcal{B}$ and $\tilde{x} \in \mathcal{E}$ with $p(\tilde{x}) = x$, there exists a unique $\tilde{f} : \tilde{x} \to \tilde{y}$ such that $F(\tilde{f}) = f$.

$$\begin{tikzcd}
\tilde{x} \arrow[r, dotted, "\tilde{f}"] & \tilde{y} \\
x \arrow[r, "f"] & y
\end{tikzcd}$$

More categorically

In fact, this has mostly nothing to do with topology: everything can be done at the level of the fundamental groupoid $\pi_1(X)$.

A functor $F : \mathcal{E} \to \mathcal{B}$ between groupoids is **covering**, or a **discrete opfibration**, when for every $f : x \to y$ in $\mathcal{B}$ and $\tilde{x} \in \mathcal{E}$ with $p(\tilde{x}) = x$, there exists a unique $\tilde{f} : \tilde{x} \to \tilde{y}$ such that $F(\tilde{f}) = f$.

$$\begin{tikzcd}
\tilde{x} \arrow[r, dotted, "\tilde{f}"] & \tilde{y} \\
x \arrow[r, "f"] & y
\end{tikzcd}$$

Typical example: when $p : E \to B$ is a covering map,

$$p_* : \pi_1(E) \to \pi_1(B)$$

is a covering functor.

Covering functors

All previous theorem can be shown in this setting.

Covering functors

All previous theorem can be shown in this setting.

Theorem

There is an equivalence between the categories of

- *discrete opfibrations over* $\mathcal{B}$
- *covariant presheaves over* $\mathcal{B}$

This means that a covering functor

$$\mathcal{E} \to \mathcal{B}$$

is the same as a functor

$$\mathcal{B} \to \mathbf{Set}$$

Covering functors

All previous theorem can be shown in this setting.

Theorem

There is an equivalence between the categories of

- *discrete opfibrations over $\mathcal{B}$*
- *covariant presheaves over $\mathcal{B}$*

This means that a covering functor

$$\mathcal{E} \to \mathcal{B}$$

is the same as a functor

$$\mathcal{B} \to \mathbf{Set}$$

Bonus: this works even when $\mathcal{B}$ is a category (not a groupoid)!

RELATING THOSE

Duality between geometry and algebra

Fix a field K.

To any space X, one can associate the commutative algebra

$$\mathcal{O}(X) \quad = \quad X \Rightarrow K$$

For instance:

$$(f+g)(x) \quad = \quad f(x)+g(x)$$

Bibliography I

John Baez and Michael Shulman.
Lectures on n-categories and cohomology.
In *Towards higher categories*, pages 1–68. Springer, 2010.

Francis Borceux and George Janelidze.
Galois theories.
Cambridge University Press, 2001.

Régine Douday and Adrien Douady.
Algebre et théories galoisiennes.
Nouvelle Bibliotheque Mathématique. Cassini, 2005.

Allen Hatcher.
Algebraic topology.
2000.

Bibliography II

J Peter May.
A Concise Course in Algebraic Topology.
University of Chicago press, 1999.

Alice Medvedev, Ramin Takloo-Bighash, et al.
An invitation to model-theoretic galois theory.
Bulletin of Symbolic Logic, 16(2):261–269, 2010.

Ian Stewart.
Galois theory.
CRC Press, 2015.