Symmetries in Physics

Winter Semester 2026/2027
Universität Bielefeld
Neil Manibo
Tutor: Patricia Päßler

Organisation

- Master in mathematical and theoretical physics
- Master in (theoretical) physics

Lecture:

- Mo: 12-14, U5-133 (First session: **October 12**)
- Wed: 12-14, U5-133

Tutorials:

- Mo: 14-16, S0-115 (Tutor: Patricia Päßler)
- Postbox in room E5-108
- First session: **October 19**

Guidelines for the tutorials and exam:

- To obtain credit points, tutorials must be attended. There will be exercises in person (Präsenzübungen).
- 50% of the points are required (submitted solutions).
- Students must be able to present their solutions at the blackboard.
- Every student should participate in the discussions in the tutorials at least **seven** times. Presentations of solutions for in-person exercises, homeworks, and discussion with the tutor will count into this number.
- Course materials will be posted on the course website. The lecture notes will be regularly updated. The exercise sheets will be posted on Wednesdays at 12:00.
- The solutions to the exercise sheets should be submitted to the tutor's mail box or electronically to the tutor via email, one week after the posting of the sheet, until Wednesday 12:00.
- **AI Exercises**: more conceptual questions, should serve as practice in consolidating and processing AI-generated results. AI-conversations (prompts), as well as a one-paragraph summary, will form part of the submission.

  Why this component? The goal is three-fold.

  - Practice in generating better prompts and result consolidation (what is interesting? what sounds incorrect/misleading?)
  - Complement computation and proving skills expected to be gained from other exercises.
  - Review for the oral exam, in particular in identifying connections.

- **Examination type:** oral exam, 30 minutes, with focus on **connections** between themes, objects, and results discussed. One of the AI exercises will be asked in the exam. The students will be asked to discuss their answers at the board.

Course overview

Course plan

- Chapter 1: Groups, morphisms, and group actions
- Chapter 2: Groups acting on $\mathbb{R}^n$
- Chapter 3: Group representations
- Chapter 4: Applications in physics (I)
- Chapter 5: Lie groups and Lie algebras
- Chapter 6: Special topics, applications in physics (II)

References

- Main references
  - H.F. Jones, *Groups, Representations and Physics*, IOP Publishing Ltd., Bristol, 1990.
  - J.F. Cornwell, *Group Theory in Physics*, Vol. I and II, Academic Press, London, 1984.
  - J.F. Cornwell, *Group Theory in Physics: An Introduction*, Academic Press, London, 1997.
  - Vorlesungsskript: Symmetries in Physics (Trebin): translated to English and consolidated by F. Gähler
- Secondary references
  - G. Lugo, *Differential Geometry in Physics*, University of North Carolina Press, Wilmington, 2021.
  - V. Guillemin and S. Sternberg, *Symplectic Techniques in Physics*, Cambridge University Press, Cambrige, 1984.
  - E. Hewitt and K.A. Ross, *Abstract Harmonic Analysis Vol. 1: Structure of Topological Groups, Integration Theory, Group Representations*, Springer, New York NY, 1979.
  - M. Hall, *The Theory of Groups*, AMS Press, Providence RI, 1979.
  - G. James and M. Liebeck, *Representations and Characters of Groups*, Cambridge University Press, 2nd ed., 2001.

Main vignettes and (mathematical) themes

- Focus more on connections rather than definitions, i.e., less of "what is a group?" and more of "which groups appear in which areas of physics?" (e.g., quantum mechanics, optics, general relativity, classical mechanics, solid state physics, quantum electrodynamics, quantum chromodynamics). The list of applications that will be covered is of course not exhaustive.

- Parallelism and analogues for various mathematical areas; in *analysis (and topology)*, the concepts of continuity and convergence are central (e.g., when is a function f continuous? what do we gain from continuity? when is a sequence convergent?). In group theory, one deals with *algebraic* structures (homomorphisms, subgroups, quotients, cosets, stabilisers, group actions, operations on groups). There are objects with both analytic and algebraic structures: Lie groups!

- Learning through counter-examples! (not a group, not isomorphic, not conjugate, not a homomorphism, not a normal subgroup, not irreducible, etc.)

- Identifying deeper intepretations and consequences of *equivalence* and *invariance*!

  - Let d_1 and d_2 be two metrics in $\mathbb{R}^n$. What does is mean for them to be equivalent?
  - Let M and M' be two $n \times n$-matrices, and suppose that they are similar, i.e., there exists an invertible matrix S such that $M = SMS^{-1}$. This implies that M and M' share the same (i) eigenvalues, (ii) trace, (iii) determinant, (iv) characteristic polynomial.
  - For group elements: conjugacy, for groups: isomorphism, for representations: unitary equivalence
  - Invariance is defined with respect to a *process* or an underlying *action*!

- Representation theory = Group theory + Linear algebra, just as :

  - ergodic theory = probability theory + dynamical systems
  - algebraic topology = algebra + topology
  - analytic number theory = analysis + number theory, etc.

  This allows us to use objects and results in linear algebra (e.g., bases, matrices (in general, linear operators), the concept of orthogonality) to study groups and group actions!

- Decompositions of functions and spaces (needed to understand structures of solutions of physical problems)

Motivation

What are symmetries?

- Euclidean motion leaving a figure, pattern, point set in Euclidean space ($\mathbb{R}^3$) invariant
  These can be **composed**, have **inverses**, etc. $\rightsquigarrow$ they form a **group**!
- Permutation of identical particles leaves physics invariant
- Symmetries of equations of motions: in Lagrangian mechanics, if the Lagrangian L does not depend on the coordinate q_α, then $\partial L/\partial \dot{q}_\alpha$ is conserved:

$$\frac{\mathrm{d}}{\mathrm{d}t}\frac{\partial L}{\partial \dot{q}_\alpha} - \frac{\partial L}{\partial q_\alpha} = 0$$

  - symmetries $\longleftrightarrow$ conserved quantities
  - rotational invariance $\longleftrightarrow$ angular momentum conserved
  - translational invariance $\longleftrightarrow$ momentum conserved
  - time invariance $\longleftrightarrow$ energy conservation

  In classical mechanics, certain conserved quantities are moment maps of Lie group actions on manifolds.
- Sometimes not so obvious: Runge–Lenz vector for the Coloumb-Potential $\frac{1}{r}$
  - For the $\frac{1}{r}$-potential, orbits are ellipses, vector to perihelion is constant.
  - For the $\frac{1}{r^\alpha}$-potential, $\alpha \neq 1$, orbits are rosettes, perihelion procession
  - General relativity gives correction; for planet Mercury, 43" perihelion precession per century
  - Correspondingly, for the hydrogen atom ($1/r$-potential!), the energy levels $E_{n,\ell,m}$ are independent not only of m, but also of $\ell \longrightarrow$ same symmetry!
- Often, a symmetry operation in physical space induces a transformation in a more abstract space, e.g.,
  - Vibrations of atoms in a molecule: symmetries of molecule act of the space of deviations from equilibrium position
  - in quantum mechanics, transformations of physical (ambient) space correspond to unitary operators in a Hilbert space

  In both cases, we have to deal with a representation of the symmetry group G, i.e., a homomorphism from G to a group of linear operators in some vector space. Depending on the context, G can act with different representations of various dimensions.

Understanding the symmetries of a problem are essential to understand the structure of the problem and its solutions. Moreover, it is also helpful for computations! It allows to chose, e.g., a symmetry adapted basis or coordinates, which can simplify things enormously. In perturbation theory, symmetry often gives relations between matrix elements so that only one (!) of them (or very few) needs to be computed. $\rightsquigarrow$ Wigner–Eckart theorem!

1 Groups, morphisms, and group actions

1.1 Groups: axioms and examples

Definition 1.1. A *group* is a pair $(G, \cdot)$ consisting of a set G and a map

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto g \cdot h \end{aligned}$$

with the following properties.

(i) Associativity: For all $g, h, k \in G$: $g \cdot (h \cdot k) = (g \cdot h) \cdot k$

(ii) Existence of a left-neutral element: $\exists\, e \in G$ such that $eg = g$, for all $g \in G$

(iii) Existence of left-inverses: For every $g \in G$, $\exists\, g' \in G$ with $g' \cdot g = e$
Notation: $g^{-1} := g'$.

A group $(G, \cdot)$ is called *Abelian* (or commutative) if, for all $g, h \in G$, $g \cdot h = h \cdot g$.

Remark 1.2.

(1) The group operation $\cdot$ can also be written as $\circ$ (for composition of maps) or $+$ for addition in Abelian groups.

(2) The left-neutral element e is also right-neutral ($e \cdot g = g \cdot e = g$, $\forall g \in G$) and this neutral element is unique!

(3) The left inverse g^{-1} of g is also a right-inverse, and there is a unique inverse with $g^{-1} \cdot g = g \cdot g^{-1} = e$.

Example 1.3.

(1) $(\mathbb{Z}, +), (\mathbb{R}, +), \ldots$ (additive groups)

(2) $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), \ldots$ (multiplicative groups)

(3) $(\mathbb{C}, +) \simeq (\mathbb{R}^2, +)$; this symbol signifies that these two groups are *isomorphic* (more later!)

(4) $S^1 = \{z \in \mathbb{C} \colon |z| = 1\} = \{z \in \mathbb{C} \colon z = \mathrm{e}^{2\pi \mathrm{i} \theta}, \theta \in [0, 1)\}$, with the multiplication operation

(5) Permutation groups: permutations of a finite set $X = \{1, \ldots, n\}$:

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}, \quad \text{where } f : X \to X \text{ is bijective}$$

e.g.,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} : \quad \text{in cycle notation: } (1\,2\,3)(4) = (1\,2\,3).$$

Example 1.4 (Matrix groups)**.** There are several matrix groups, all being composed of square matrices with $\det A \neq 0$.

1. $\mathrm{GL}(n,\mathbb{C}) = \{A \in \mathbb{C}^{n\times n} \colon \det(A) \neq 0\}$ (general linear group over $\mathbb{C}$)
2. $\mathrm{GL}(n,\mathbb{R}) = \{A \in \mathbb{R}^{n\times n} \colon \det(A) \neq 0\}$ (general linear group over $\mathbb{R}$)
3. $\mathrm{SL}(n,\mathbb{R}) = \{A \in \mathbb{R}^{n\times n} \colon \det(A) = 1\}$ (special linear group)
4. $\mathrm{SO}(n,\mathbb{R}) = \{A \in \mathbb{R}^{n\times n} \colon A^T A = I,\ \det(A) = 1\}$ (special orthogonal group)
5. $\mathrm{SU}(n,\mathbb{C}) = \{A \in \mathbb{C}^{n\times n} \colon A^\dagger A = I,\ \det(A) = 1\}$ (special unitary group). Here, the dagger operation corresponds to complex conjugate transpose.

Here, the group operation in matrix multiplication. In general, matrix groups are non-Abelian!

Example 1.5. Let T be a self-adjoint operator on a complex Hilbert space. Then the set $\{U(t) : t \in \mathbb{R}\} = \{\mathrm{e}^{-\mathrm{i}tT} \colon t \in \mathbb{R}\}$ (together with composition of operators as operation) forms a strongly continuous one-parameter *unitary group*. Its infinitesimal generator is $-\mathrm{i}T$. For every x in the domain $D(T)$ of T, $\psi(t) = \mathrm{e}^{-\mathrm{i}tT}x$ is the unique solution of the initial value problem (IVP)

$$\frac{\mathrm{d}}{\mathrm{d}t}\psi(t) = -\mathrm{i}S\psi(t), \quad \psi(0) = x \quad (t \in \mathbb{R}).$$

with $S = T$.

Here, the *infinitesimal generator* A of the one-parameter unitary group $\{U(t) \colon t \in \mathbb{R}\}$ is defined via

$$Ax = \lim_{t\to 0} \frac{1}{t}\Big(U(t) - I\Big)x,$$

which holds for all $x \in D(U(t))$. In the example above $D(U(t)) = D(T)$, for all $t \in \mathbb{R}$ (consequence of the spectral theorem!)
One can compare this with the role of x in the expansion

$$\mathrm{e}^{tx} = 1 + tx + \frac{(tx)^2}{2!} + \frac{(tx)^3}{3!}\cdots$$

and so on. Note that

$$\lim_{t\to 0} \frac{1}{t}\Big(e^{tx} - 1\Big) = \frac{1}{t}\left(tx + \frac{(tx)^2}{2} + \cdots\right) = x.$$

(more later, when we discuss Lie groups and Lie algebras!) 12.10.26

1.2 Subgroups, morphisms, and actions

Definition 1.6. A *subgroup* H of G ($H < G$) is a non-empty subset of G, which is closed under group operations (products, inverses). In particular, $e \in H$ since $g \in H$ implies $g^{-1} \in H$ and $g \cdot g^{-1} \in H$.

Theorem 1.7. *A non-empty subset $H < G$ is a subgroup of G if, and only if,*

$$g, h \in H \implies g \cdot h^{-1} \in H.$$

Example 1.8.

(1) $(\{e\}, \cdot) < G$ (trivial subgroup), $G < G$. Proper subgroups are bigger than the trivial subgroup, but smaller than G.

(2) $(2\mathbb{Z}, +) < (\mathbb{Z}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$. On the contrary, $(2\mathbb{Z} + 1, +) \not< (\mathbb{Z}, +)$.

(3) $\mathrm{SL}(n, \mathbb{R}) < \mathrm{SL}(n, \mathbb{C}) < \mathrm{GL}(n, \mathbb{C})$ (why?)

(4) $\mathrm{SL}(n, \mathbb{R}) < \mathrm{GL}(n, \mathbb{R}) < \mathrm{GL}(n, \mathbb{C})$

Definition 1.9. Suppose $(G, \cdot)$ and $(G', \circ)$ are two groups. A map $f\colon G \to G'$ is called a (group) *homomorphism* from G to G', if, for all $g_1, g_2 \in G$

$$f(g_1 \cdot g_2) = f(g_1) \circ f(g_2).$$

In the additive case, one also writes $f(x + y) = f(x) + f(y)$.

Definition 1.10. The *kernel* of the homomorphism f is the pre-image of the neutral element $e' \in G'$, that is,

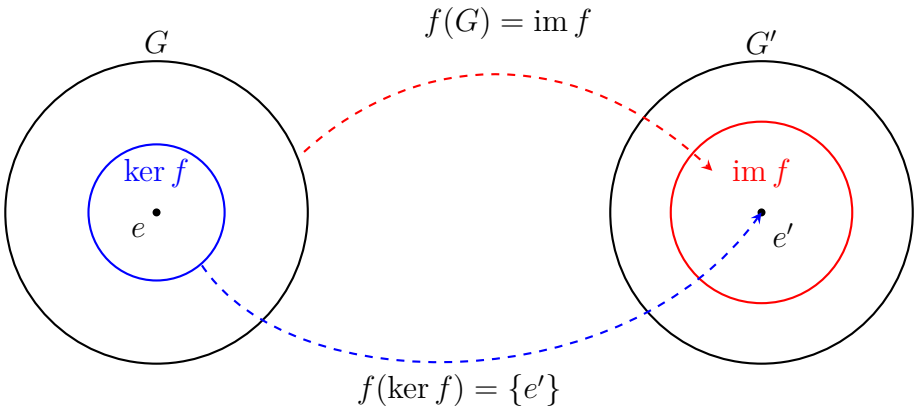
$$\ker f := \{g \in G\colon f(g) = e'\} = f^{-1}(\{e'\}) \subset G.$$

The *image* of f consists of all elements of G' that have a pre-image in G.

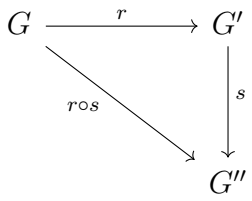
$$\operatorname{im} f := \{f(g)\colon g \in G\} \subset G'.$$

Consequences:

- $f(e) = e' \implies e \in \ker f$
- $f(g^{-1}) = f(g)^{-1}$, for all $g \in G$
- $\ker f \in G$ and $\operatorname{im} f \in G'$



- Let $r\colon G \to G'$, $s\colon G' \to G''$ be homomorphisms. Their composition $r \circ s$ is also a homomorphism.



- A homomorphism is *injective* if, and only if, its kernel is trivial. (Note: injective means $g \neq h \implies f(g) \neq f(h)$)
- Suppose G is finite. Then every $g' \in \operatorname{im} f$ has the same number of pre-images in G, namely $n = |\ker f|$.

$$f^{-1}(f(g)) = g \cdot \ker f = \{g.k : \ k \in \ker f\}.$$

Definition 1.11. A homomorphism $f\colon G \to G'$ is called

- an *epimorphism*, if f is surjective ($\operatorname{im} f = G'$)
- a *monomorphism*, if f is injective
- an *isomorphism*, if it is bijective (1-to-1 and onto)
- an *endomorphism*, if $G = G'$
- an *automorphism*, if $G = G'$ and f is an isomorphism

If two groups are isomorphic, one writes $G \simeq G'$.

Example 1.12.

(1) Let $(\mathbb{Z}_2, +) = (\mathbb{Z}/2\mathbb{Z}, +)$: integers with addition modulo 2 and let

$$S_3 = \{\text{permutations of } \{1,2,3\}\} = \{(1), (1\,2\,3), (1\,3\,2), (1\,2), (1\,3), (2\,3)\}.$$

There is a homomorphism $\phi\colon S_3 \to \mathbb{Z}_2$ given by

$$(1), (123), (132) \mapsto 0$$
$$(12), (13), (23) \mapsto 1$$

ϕ is surjective ($\operatorname{im}\phi = \mathbb{Z}_2$) with kernel $\ker\phi = \{(1), (123), (132)\}$.
What is this homomorphism counting?

(2) $\{1, -1\}$ form a group under multiplication: $G = (\{1, -1\}, \cdot)$. The map $f\colon G \to \mathbb{Z}_2$ given by

$$1 \mapsto 0, \ -1 \mapsto 1$$

is an isomorphism ($\operatorname{im} f = \mathbb{Z}_2$, $\ker f = G$).

(3) $f\colon (\mathbb{R}, +) \to (\mathbb{R}_+, \cdot)$ given by $f\colon x \to \mathrm{e}^x$ is an isomorphism, even though $\mathbb{R}$ seems "bigger" than $\mathbb{R}_+$.

(4) The circle group S^1 in Example 1.3 is isomorphic to the group $\mathbb{T} = [0, 1)$, with addition modulo 1. What is a possible isomorphism map?

The concept of "homomorphism" for groups is a special case of "maps" between mathematical objects that preserve the underlying structure. These maps figure prominently in the study of abstract spaces (category theory) and are called *morphisms*.

Definition 1.13. Let $\mathcal{O}, \mathcal{O}'$ be two sets with the same kind of structure (algebraic, topological, differentiable,...), e.g., two groups, two vector spaces, two differentiable manifolds, etc.. A map $f\colon \mathcal{O} \to \mathcal{O}'$ is called a *morphism* if f preserves that structure.
If a morphism f is bijective, it is called an isomorphism. If further $\mathcal{O} =, \mathcal{O}'$, f is called an automorphism. The set of automorphisms always form a group!

Remark 1.14.

(1) Morphisms of algebraic structures are called homomorphisms: (applicable to groups, rings, fields, vector spaces, Hilbert spaces, etc.)

(2) isomorphisms preserving differentiable structures are called *diffeomorphisms* (f, f^{-1} smooth)

(3) isomorphisms preserving topological structures are called *homeomorphisms* (f, f^{-1} continuous)

(4) Further examples: symplectomorphisms, Lie algebra isomorphisms, graph isomorphisms, etc.

Example 1.15.

(1) Let $\mathcal{O} = \{1, \dots, n\}$ (without further structure).

$$\begin{aligned}\mathrm{Aut}(\mathcal{O}) &= \{\text{bijective maps } \mathcal{O} \to \mathcal{O}\} = \{\text{permutations of } \mathcal{O}\} \\ &= S_n : \text{symmetric group!}\end{aligned}$$

(2) Let $\mathcal{O} = \mathbb{R}^3$ (vector space) $\rightsquigarrow \mathrm{Aut}(\mathcal{O}) = \mathrm{GL}(3, \mathbb{R})$.

(3) Let $\mathcal{O} = (\mathbb{R}^3, \langle \cdot, \cdot \rangle)$ (vector space with scalar product)
$\rightsquigarrow \mathrm{Aut}(\mathcal{O}) = \mathrm{O}(3, \mathbb{R}) < \mathrm{GL}(3, \mathbb{R})$.

(4) Let $\mathcal{O} = (\mathbb{R}^4, \text{with the Minkowski metric})$
$\rightsquigarrow \mathrm{Aut}(\mathcal{O}) = \mathrm{O}(1, 3)$ (Lorentz group).

(5) Let $\mathcal{O} = \mathbb{R}^n$ as affine Euclidean space
$\rightsquigarrow \mathrm{Aut}(\mathcal{O}) = E_n = \mathbb{R}^n \rtimes \mathrm{O}(n)$: group of all Euclidean motions
(group of isometries=distance preserving transformations!)

The concept of automorphisms is necessary to define the idea of a group action.

Definition 1.16. An *action* of a group G on an object $\mathcal{O}$ is a group homomorphism $h\colon G \to \mathrm{Aut}(\mathcal{O})$, $g \to h(g)$, where the map $h(g)$ is given by

$$h(g)\colon \mathcal{O} \to \mathcal{O}, \quad x \mapsto h(g)x.$$

In physics, groups are usually connected with a group action! Group actions can be seen as *dynamical* interpretations of a group as a *group of transformations*.

Example 1.17.

- $G = \mathrm{O}(3) = \mathrm{Aut}(\mathbb{R}^3, \langle\cdot,\cdot\rangle)$ and let $\mathcal{O} = C(\mathbb{R}^3)$ be the space of continuous functions on $\mathbb{R}^3$. An action of G on $\mathcal{O}$ is given by $h\colon \mathrm{O}(3) \to \mathrm{Aut}(C(\mathbb{R}^3))$, $g \mapsto h(g)$ with

$$\begin{aligned} h(g)\colon C(R^3) &\to C(\mathbb{R}^3) \\ \psi &\mapsto h(g)\psi, \qquad \text{with } (h(g)\psi)(x) := \psi(g^{-1}x). \end{aligned}$$

  It is clear that the new function $\widetilde{\psi} = (h(g))\psi = \psi \circ g^{-1}$ is continuous (why?).

- Let $P(M)$ be the sets of subsets of M (power set of M). $\mathrm{Aut}(M)$ acts naturally on $P(M)$ via

$$\begin{aligned} h\colon \mathrm{Aut}(M) &\to \mathrm{Aut}(P(M)) \\ g &\mapsto h(g) \end{aligned}$$

  with

$$\begin{aligned} h(g)\colon P(M) &\to P(M) \\ N &\mapsto h(g)N := \{ga \in M :\ a \in N\} \end{aligned}$$

14.10.26

The previous example motivates the following definition.

Definition 1.18. Let a group G act on the set $\mathcal{O}$ and let $a \in G$. The subgroup

$$H = \{h \in G\colon ha = a\}$$

is called the symmetry group/fixed-point group of a. This is also called the *stabiliser* subgroup of a (denote by $\mathrm{Stab}_G(a)$).

Note: elements of $\mathcal{O}$ and thus fixed-points can be **sets**!

Example 1.19.

(1) Let $\triangle = \{x_1, x_2, x_3\} \in P(\mathbb{R}^2, \langle\cdot,\cdot\rangle)$ be an equilateral triangle. Its symmetry group relative to $\mathrm{SO}(2)$ consists only of **rotations** is given by

$$C_3 = \{I, c_3 = R_{120^\circ}, c_3^2\}.$$

On the other hand, relative to $\mathrm{O}(2)$ the symmetry group is given by

$$C_{3v} = \{I, c_3, c_3^2, \sigma_1, \sigma_2, \sigma_3\}$$

where σ_i is the reflection with respect to the perpendicular bisector passing through x_i (that is, the line passing through x_i and the center of the triangle). Compare with the exercise in the tutorials!

(2) Define $\Gamma = \{x_{n,m} = p + ne_1 + me_2 :\ m, n \in \mathbb{Z}\} \in P(\mathbb{R}^2, \text{affine space})$. Γ is a *lattice*! Its symmetry group is a *space group*, i.e., $H < E(2)$, $H\Gamma = \Gamma$. Here, Γ is a fixed point of H.

Remark 1.20. A *linear representation* of a group G is an action

$$\begin{aligned} G &\to \mathrm{Aut}(\mathbb{R}^n) = \mathrm{GL}(n,\mathbb{R}), \text{or} \\ G &\to \mathrm{Aut}(\mathbb{C}^n) = \mathrm{GL}(n,\mathbb{C}), \text{or} \\ G &\to \mathrm{Aut}(V), \quad \text{where } V \text{ is a vector space.} \end{aligned}$$

$\rightsquigarrow$ Group elements are mapped into linear operators! Examples 1.5 and 1.19.1 provide representations (of $\mathbb{R}$ and cyclic group C_3, respectively). More in Chapter 4!

1.3 Cosets, orbits

We have seen in Example 1.8.2 that $(2\mathbb{Z}, +)$ is a subgroup of the integers, but the set $2\mathbb{Z}+1$ of odd numbers is not. In this section, we will make sense of this set with respect to $2\mathbb{Z}$ seen as a subgroup of $\mathbb{Z}$.

Definition 1.21. A *relation* between pairs of elements of a set $\mathcal{O}$ is a subset R of $\mathcal{O}\times\mathcal{O}$. Two elements g, h are related (notation: $g \sim h$) if $(g,h) \in R$. A relation $\sim$ is called an *equivalence relation* if

(i) it is reflexive: $g \sim g$

(ii) it is symmetric: $g \sim h \implies h \sim g$

(iii) it is transitive: $g \sim h$ and $h \sim g \implies g \sim k$.

The *equivalence class* $[g] \subset \mathcal{O}$ consists of all $h \in \mathcal{O}$ related to g, that is,

$$[g] = \{h \in \mathcal{O} \colon h \sim g\}$$

g is a representative of the class $[g]$.

Example 1.22. Let us consider examples in ancestral genetics.

- The relation "parent of" is neither reflexive, nor symmetric, nor transitive. The same holds for "child of"
- "parent or child" is symmetric, but not reflexive, nor transitive
- "ancestor or descendant" is symmetric and transitive, but not reflexive

Theorem 1.23. *An equivalence relation on a set $\mathcal{O}$ splits $\mathcal{O}$ into a disjoint union of equivalence classes:*

$$\mathcal{O} = \bigcup_{g\in I} [g], \quad \underset{g\neq h}{g,h \in I} \implies [g]\cap[h] = \varnothing \quad (\iff g \not\sim h).$$

Proof.

- $g \in [g] \implies [g] \neq \varnothing$. Each element is in some class $\implies \mathcal{O} = \cup_g [g]$
- if $x \in [g]\cap[h]$, then $g \sim x$ and $h \sim x$, and by transitivity, $g \sim h$. Hence, $[g] = [h]$. We have either $[g] = [h]$ or $[g]\cap[h] = \varnothing$. □

Example 1.24.

- "Being isomorphic" is an equivalence relation for a collection of groups.
- Rational numbers can be regarded as an equivalence class of pairs of integers:

$$r_1 = \frac{z_1}{n_1} \sim r_2 = \frac{z_2}{n_2} \iff z_1 n_2 = z_2 n_1.$$

We now present an equivalence relation that depends on a subgroup $H < G$ of a group G.

Theorem 1.25. *Let $H < G$ and $g, k \in G$. The relation "equivalent modulo H", written as $\underset{mod\, H}{\sim}$, with*

$$g \underset{mod\, H}{\sim} k \iff g^{-1}k \in H, \text{ i.e., } k \in gH \equiv \{gh \colon h \in H\}$$

is an equivalence relation.

Proof.

- reflexive: $a^{-1}a = e \in H$
- symmetric: $a^{-1}b \in H \implies$ its inverse must also be in $H \implies (a^{-1}b)^{-1} = b^{-1}a \in H$
- transitive: $a^{-1}b \in H$, $b^{-1}c \in H \implies (a^{-1}b)(b^{-1}c) = a^{-1}c \in H$. □

Definition 1.26. The equivalence class $[g] = gH$ is called the *right coset* of g relative to H. (In german: *Restklasse, Nebenklasse*).

Definition 1.27. The set of all right cosets relative to H is called the *factor set* G/H, and the map

$$\begin{aligned} \pi : G &\to G/H \\ g &\mapsto [g] = gH \end{aligned}$$

is called a *projection*.

Notation: $\mathcal{O}$ is a set, $\mathcal{O}/\sim$ is a factor set:= set of all equivalence classes, $\mathcal{O} \to \mathcal{O}/\sim$ is the projection

Example 1.28.

(1) Let $H = (5\mathbb{Z}, +) = \{0, \pm 5, \pm 10, \pm 15, \ldots\}$ be the subgroup of $\mathbb{Z}$ consisting of all multiples of 5. $\mathbb{Z}$ splits into 5 cosets

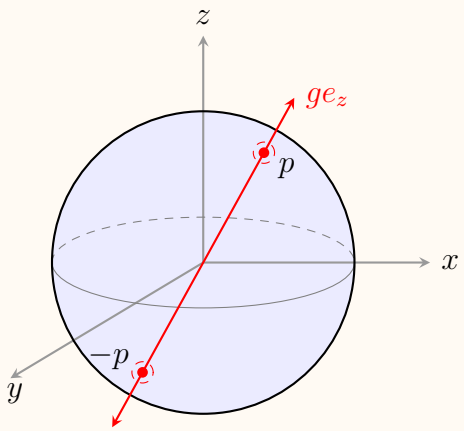
$$\mathbb{Z} = (0 + 5\mathbb{Z}) \sqcup (1 + 5\mathbb{Z}) \sqcup (2 + 5\mathbb{Z}) \sqcup (3 + 5\mathbb{Z}) \sqcup (4 + 5\mathbb{Z})$$

The symbol $\sqcup$ here is used (in place of $\cup$ to emphasise that this is a *disjoint* union. For additive (Abelian) groups, one can write $g + H$ instrad of $g \cdot H$. The factor set contains 5 cosets $\{5\mathbb{Z}, 1 + 5\mathbb{Z}, \cdots, 4 + 5\mathbb{Z}\}$.

(2) Let $\mathrm{SO}(2) < \mathrm{SO}(3)$ consist of all rotations around the z-axis e_z. Given $g \in \mathrm{SO}(3)$, the coset $g \cdot \mathrm{SO}(2)$ consists of all rotations around ge_z. The set $\{ge_z\}$ can be parametrised by a 2-sphere S^2, with antipodal points (p and $-p$ in the figure below) identified, and so

$$\begin{aligned} \pi : \mathrm{SO}(3) &\to \mathrm{SO}(3)/\mathrm{SO}(2) \simeq S^2/\mathbb{Z}_2 = \mathbb{R}P^2, \\ g &\mapsto ge_z = gH \end{aligned}$$

where $\mathbb{R}P^2$ is the *real projective space of dimension 2* (set of all lines in $\mathbb{R}^3$ passing through the origin). In general, $\mathrm{SO}(n)$ acts on $\mathbb{R}P^{d-1}$.



This also fits the following description of matrices in SO(3): every matrix M in SO(3) is similar to a rotation matrix around the z-axis, that is

$$M = PR_\theta P^T, \quad \text{with } R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where P is an orthogonal matrix, and $\theta \in [0, 2\pi)$. This also makes the statement $\mathrm{SO}(2) < \mathrm{SO}(3)$ transparent (the set $\{R_\theta\}$ forms a subgroup isomorphic to SO(2))!

Note: The relation $\mathrm{SO}(3)/\mathrm{SO}(2) \simeq S^2/\mathbb{Z}_2$ here pertains to "identification as sets". We have not shown yet that either of them is a group. In fact, in this case SO(3)/SO(2) is **not** a group, and hence this relation cannot be a group isomorphism!

Proposition 1.29. *If H is finite, every coset gH contains as many elements as H.*

Proof. T.S.: the map $\psi\colon H \to gH, h \mapsto gh$ is bijective. By definition, ψ is surjective. ψ is also injective: $\psi(k) = \psi(\ell) \implies gk = g\ell \implies k = \ell$. □

As a direct consequence, we get that a finite group splits into disjoint subsets gH of the *same size*:

$$\begin{aligned} G &= \bigcup_g gH = \bigcup_g \{gh :\ h \in H, g \in G\} \\ &= \bigcup_g Hg = \bigcup_g \{hg :\ h \in H, g \in G\} \end{aligned}$$

Recall that, for finite groups, the *order of* G (written as $|G|$) is the number of elements of G.

Definition 1.30. If $H < G$ is a subgroup of G, then the number of cosets relative to H is called the index of H in G, written as $[G : H]$ (or $\mathrm{ind}(H)$).

Theorem 1.31 (Lagrange)**.** *If G is a finite group, and $H < G$ is a subgroup, then $|H|$ divides G and*

$$|G| = [G : H] \cdot |H|.$$

Proof. Each g is in exactly one H-coset. These are disjoint and have the same number of elements $\implies$ G must be a multiple of $|H|$. □

As a corollary, if $|G|$ is prime, then G has no non-trivial proper subgroups.

We now present an equivalence relation that is induced by a group action. This relation can be interepreted as a notion of *"reachability"*.

Definition 1.32. Let a group G act on a set $\mathcal{O}$ (say via the homomorphism $h\colon G \to \mathrm{Aut}(\mathcal{O})$). An element $x \in \mathcal{O}$ is called *G-equivalent* to $y \in \mathcal{O}$ ($x \overset{G}{\sim} y$) if there exists $g \in G$ with $y = g \cdot x := h(g)x$. An equivalence class $[x]_G$ of the relation $\overset{G}{\sim}$ is called the *orbit* (in german: Bahn) of the element $x \in \mathcal{O}$:

$$[x]_G = G \cdot x = \{g \cdot x\colon g \in G\} = \{h(g)x\colon g \in G\}.$$

If there is only one orbit in $\mathcal{O}$, the action of G is called *transitive*.

Remark 1.33.

- $\overset{G}{\sim}$ is indeed an equivalence relation (easy to see via reachability)
- The set of orbits is written as $\mathcal{O}/G$.

There are also other notions associated to actions such as faithfulness and freeness

- An action of G on $\mathcal{O}$ is *faithful*, if $g \cdot x = x$, for all $x \in \mathcal{O}$, $\implies$ $g = e$ (the only element of G that fixes ALL elements x is the identity). This is equivalent to the homomorphism h being injective.
- An action of G on $\mathcal{O}$ is *free* if, $g \cdot x = x$ *for some* $x \in \mathcal{O} \implies g = e$. 19.10.26

Example 1.34.

(1) Orbits of SO(3) acting on $\mathbb{R}^3$ are spherical shells, one for each radius: $\mathcal{O}/G = \mathbb{R}^3/\mathrm{SO}(3) = [0, \infty)$. The action is not transitive, but it is faithful (free even).

(2) Time evolution in quantum mechanics: $\mathrm{e}^{-itH/\hbar}|\psi\rangle$, $t \in \mathbb{R}$
(compare with Example 1.5)
$G = \mathbb{R}$, $\mathcal{O} =$ Hilbert space

(3) Cosets can be interpreted as orbits!
Let $H < G$ be a subgroup of G, acting on G via $\varphi\colon H \to \mathrm{Aut}(G), h \mapsto \varphi(h)$ with

$$\begin{aligned} \varphi(h)\colon\ & G \to G \\ & g \mapsto gh^{-1}. \end{aligned}$$

Right cosets of H are orbits under this action! One can check that φ is indeed a homomorphism!

Definition 1.35. A subset $N \subset \mathcal{O}$ is called *G-invariant*, if $g \cdot N \subset N$, for all $g \in G$. In this case, G is the symmetry group of N.

Theorem 1.36 (Orbit–Stabiliser theorem)**.** *Let G act on $\mathcal{O}$, $x \in \mathcal{O}$ and let $H < G$ be the stabiliser subgroup of x (i.e., $Hx = x$). Then*

(i) *The coset gH consists of elements that send x to $y = g \cdot x$.*

(ii) *The map $Gx \to G/H, y = gx \mapsto gH$ is bijective. If G is finite, the orbit $G \cdot x$ has $[G : H]$ elements.*

Proof of (i).
$(\implies)$: $k \in gh \implies k = gh$ for some $h \in H \implies k \cdot x = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = y$.
$(\impliedby)$: If $y = k \cdot x$, the $g \cdot x = k \cdot x$, and so $x = (g^{-1}k) \cdot x$. It follows that $g^{-1}k \in H \implies k \in gH$. □

Definition 1.37. Fix an element $k \in G$. The map $L(k)$ with

$$\begin{aligned} L(k)\colon\ & G \to G \\ & g \mapsto kg. \end{aligned}$$

is called the left translation on G. This defines a G-action of G onto itself.

Remark 1.38.

- $L(k)$ is an automorphism of G as a set, but not as a group! (why?)
- Since $L(k_1k_2) = L(k_1) \circ L(k_2)$, the map

$$\begin{aligned} L\colon\ & G \to \mathrm{Aut}(G) \\ & k \mapsto L(k). \end{aligned}$$

Since L is injective we have that $G \simeq \operatorname{im} L < \mathrm{Aut}(G)$.

Theorem 1.39 (Cayley)**.** *Every finite group G with $|G| = n \in \mathbb{N}$ is isomorphic to a subgroup of the symmetric group S_n.*

Proof. Recall that $\mathrm{Aut}(G) = S_n$ (G seen as a set)! It follows from the remarks above that

$$G \simeq \operatorname{im} L < \mathrm{Aut}(G) = S_n. \qquad \square$$

Theorem 1.40. *Let G act on $\mathcal{O}$, $H < G$ the stabiliser subgroup of $x \in \mathcal{O}$ and $y = g \cdot x$, $g \in G$. Then, the stabiliser subgroup of y is $gHg^{-1} = \{ghg^{-1} \colon h \in H\}$ and is called* conjugate *to H.*

Proof. Exercise! $\square$

The picture so far:

- Homomorphisms: maps between groups that preserve the group structure
- Action of $G \curvearrowright \mathcal{O}$: homomorphism from G to $\mathrm{Aut}(\mathcal{O})$
- Equivalence relation modulo a subgroup H gives rise to **cosets**!
- Equivalence relation induced by group actions gives rise to **orbits**!
- Partition of G via cosets of a subgroup $H < G$: $G = \bigcup_{[g]} gH$
- Cosets seen as uniform translations of the subgroup H
  $\rightsquigarrow$ (special case of orbits for $H \curvearrowright G$)
- So far G/H only has the structure of equivalence classes. We show that under a certain condition on H that this actually has a group structure!
  $\rightsquigarrow$ **normality**!

1.4 Normal subgroups, quotient groups, conjugacy classes

Question 1.41. *When does the factor set G/H admit a group structure?*

Definition 1.42. A subgroup $H < G$ is called a *normal subgroup* if, for all $g \in G$ one has

- $gH = Hg$, or
- $\{gh \colon h \in H\} = \{hg \colon h \in H\}$, or
- for all $h \in H$, $ghg^{-1} \in H$

Notation: $H \triangleleft G$: H is normal in G.

Remark 1.43. We do not require that $ghg^{-1} = h$ (this would imply that $gh = hg$, for all $h \in H$, which is too strong)! We only need for ghg^{-1} to *not leave* H.

Theorem 1.44. *Let G be a group, $H < G$, G/H the factor set. If H is normal in G, the product*

$$[g] \cdot [k] = [g \cdot k] \quad \textit{for } [g], [k] \in G/H, \quad g, k \in G,$$

or $gH \cdot kH = (gk)H$ is consistent and turns G/H into a group. In this case, G/H is called the quotient group.

Proof. We only show here that the product is consistent, i.e., if $g \sim g'$ and $k \sim k'$, then $[g] \cdot [h] = [g'] \cdot [k']$. Suppose H is normal in G. Consider the product $(gk)^{-1}(g'k')$. One has

$$(gk)^{-1}(g'k') = k^{-1}g^{-1}g'k \cdot k^{-1}k' = \underbrace{k^{-1}\underbrace{g^{-1}g'}_{\in H}k}_{\in H, \text{ since } H \triangleleft G} \cdot \underbrace{k^{-1}k'}_{\in H} \in H.$$

This implies that $gk \sim g'k'$, hence $[gk] = [g'k']$. One can check that the group axioms are satisfied! □

Example 1.45.

(1) C_3 is normal in C_{3v}, $C_{3v}/C_3 \simeq \mathbb{Z}_2$

(2) Every index-2 subgroup is normal:
if $[G : H] = 2$, there are only two cosets: $G = H \cup gH$, for some $g \notin H$. We also have $G = H \cup Hg$, and $H \cap gH = \varnothing = H \cap Hg \implies gH = Hg$.

(3) Every subgroup of an Abelian group is normal.

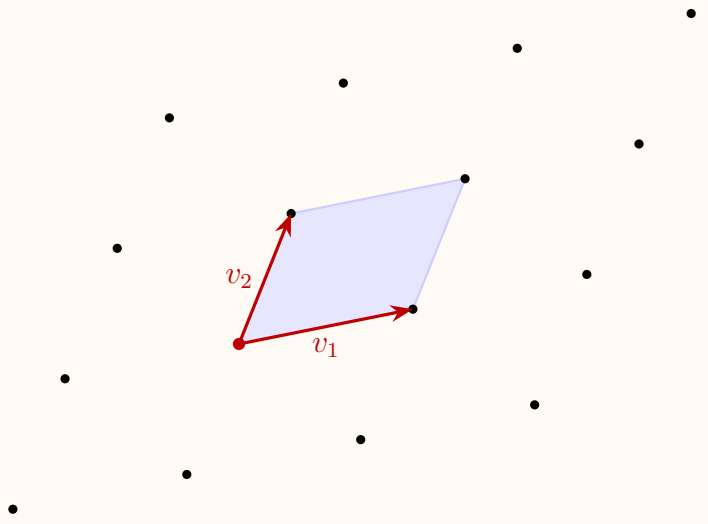
(4) $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} = (\{0, \ldots, n-1\})$ with addition mod n. One can compute with representatives $k \in k + n\mathbb{Z}$, e.g.,

$$(1+5\mathbb{Z})+(3+5\mathbb{Z}) = (-4+5\mathbb{Z})+(13+5\mathbb{Z}) = (-4+13)+5\mathbb{Z} = 9+5\mathbb{Z} = 4+5\mathbb{Z}$$

(5) From (3) $(\mathbb{Z}, +) \triangleleft (\mathbb{R}, +)$. The quotient group is the 1-torus:

$$\mathbb{R}/\mathbb{Z} = ([0, 1), + \bmod 1).$$

This represents the translations (up to symmetries) of the lattice $\mathbb{Z} \subset \mathbb{R}$. What is $\mathbb{R}^2/\Gamma$, for a general 2D-lattice Γ? What it the corresponding operation?



$\rightsquigarrow \mathbb{R}^2/\Gamma$ can be identified with the fundamental domain/primitive cell of Γ. Group operation is vector addition modulo Γ.

Proposition 1.46. *Let $f\colon G \to G'$ is a homomorphism, then* $\ker f$ *is normal in* G*.*

Proof. We know that $\ker f < G$. Let $g \in G, h \in \ker f$, i.e., $f(h) = e'$. We then get $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)e'f(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = e' \implies ghg^{-1} \in \ker f$. □

Proposition 1.47. *Let $H \triangleleft G$. The canonical projection*

$$\pi\colon G \to G/H, \quad g \mapsto gH$$

is an epimorphism with $\ker \pi = H$*.*

Theorem 1.48 (Homomorphism theorem)**.** *Let $f\colon G \to G'$ be a homomorphism. Then it induces a monomorphism*

$$\phi\colon G/\ker f \to G' \quad \textit{with } f = \phi \circ \pi.$$

Proof. Let $x \in G/\ker f, g \in G$ with $\pi(g) = x$, and set

$$\phi(x) := f(g).$$

We have to show the following the properties:

(i) $\phi(x)$ is independent of the choice of $g \in G$

(ii) ϕ is a homomorphism

(iii) ϕ is injective

(i): For all $g' \in \pi^{-1}(x) \subset G$: $\pi(g) = \pi(g')$
$\implies g\ker f = g'\ker f \implies$ there exists $h \in \ker f$ with $g = g'h$. From this it follows that,

$$f(g) = f(g'h) = f(g')\underbrace{f(h)}_{e} = f(g').$$

(ii): Let $x, y \in G/\ker f$. Choose $g, h \in G$ with $\pi(g) = x$ and $\pi(h) = y$.
$\implies \pi(gh) = \pi(g)\pi(h) = xy$. This implies

$$\phi(xy) = f(gh) = f(g)f(h) = \phi(x)\phi(y).$$

(iii): Let $x \in \ker\phi$, $g \in \pi^{-1}(x)$. Then

$$f(g) = \phi(x) = e' \in G' \implies g \in \ker f.$$

Hence, $x \in g\ker f = \ker f \implies x = e(G/\ker f)$. □

As an immediate corollary, we get the *first isomophism theorem.*

Corollary 1.49. *Let $f\colon G \to G'$ be a homomorphism. Then*

$$G/\ker f \simeq \operatorname{im} f,$$

where the isomorphism if the map ϕ above.

What does this abstract result give us?

- If we know that the subgroup H is a kernel of some homomorphism f, then it must be normal, and we know we can apply Corollary 1.49 to determine the group structure of G/H!
- Conversely, every normal subgroup is a kernel of some homomorphism (the canonical projection!) by Proposition 1.47.

Example 1.50.

(1) Consider Example 1.12 with $G = S_3$ and f being the homomorphism that counts the number of two-cycles in the cycle decomposition of a permutation. Here, $\ker f = \{(1), (123), (132)\} \simeq C_3$. It follows from, Corollary 1.49 that

$$S_3/C_3 \simeq \operatorname{im} f = \mathbb{Z}_2.$$

The two elements of S_3/C_3 are $\ker f$ and $(12)\ker f$.

(2) Let $G = (\mathbb{R}, +)$, $f\colon \mathbb{R} \to \mathbb{R}, x \mapsto x - \lfloor x \rfloor$, where $\lfloor x \rfloor = \text{floor}(x)$: largest integer $\leqslant x$. This is a homomorphism with kernel $\ker f = \mathbb{Z}$ and $\operatorname{im} f = [0, 1)$.

- What do the cosets look like?
  For a fixed $y \in [0, 1)$, we have

$$y \ker f = \{x \in \mathbb{R} : \ x - \lfloor x \rfloor = y\}$$

  Each coset if projected to an element of $G/\ker f = \mathbb{R}/\mathbb{Z}$.
- The group product is addition mod 1, and we have the isomorphism

$$\phi\colon \mathbb{R}/\mathbb{Z} = G/\ker f \to \operatorname{im} f = [0, 1), \quad \text{with } \overline{y} \mapsto y.$$

  This is consistent with Example 1.45.5 above.

21.10.26