# Mathematical Methods for Physics

October 20, 2023

## Contents



### Lecture 1

lun 02 ott 2023 08:30

## 1 Introduction

The course is about group theory and explaining where it appears in theoretical physics. Group theory is motivated by the fact that the current understanding of Nature is based on symmetries. Symmetries are properties that are invariant under some transformations. Utilizing Noether's theorem, one can link the conservation of charges to transformations and invariants. Symmetries play an important role in physics and are described by groups. There are several classes of symmetries.

**Continuous symmetries.** Symmetries can be parameterized by continuous variables. Some examples of continuous symmetries are:

- (space) translation, equivalent to the assumption that space is homogeneous: one can obtain the conservation of momentum;
- time translation, equivalent to the assumption that time is homogeneous: conservation of energy;
- space rotation, equivalent to the assumption of the isotropy of space: conservation of angular momentum;
- Lorentz and Poincaré transformations: conservation of the energy–momentum tensor.
- Local gauge symmetry: it is a symmetry of an internal degree of freedom (i.e. not related to temporal nor spacial degrees of freedom) and the transformation depends on the space-time coordinates

  $$V_{ab}(\vec{x}, t)\phi(\vec{x}, t)$$

  These kinds of symmetries describe the dynamics of quantum field theory and the properties of fundamental interactions.
- Internal, global symmetry, for example isospin: swapping the up and down quarks does not change the physics.

**Discrete symmetries.** A few examples of discrete symmetries are:

- parity $\vec{x} \to -\vec{x}$: parity is conserved in quantum electrodynamics and in quantum chromodynamics, but not in electroweak theory.
- Time reversal $t \to -t$;
- charge conjugation;
- discrete lattice: no more continuous translation symmetries, because there is only a subset of them. Lattices are used for the study of QCD in the non-perturbative regime.

This course will be dedicated to the classification and study of groups and their representations.

**Definition 1.1.** A group $G$ is a set endowed with a binary operation $\circ$ (called group multiplication) that has the following properties:

- closure: $\forall g_1, g_2 \in G$, $\exists! g_3 \in G$ such that $g_3 = g_1 \circ g_2$.
- associativity: $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$, $\forall g_1, g_2, g_3 \in G$.
- identity element: $\exists e \in G$ such that $g \circ e = e \circ g = g$, $\forall g \in G$.
- inverse element: $\forall g \in G$, $\exists g^{-1} \in G$ such that $g \circ g^{-1} = g^{-1} \circ g = e$.

**Example 1.2.** A few examples:

- The set $\mathbb{R}$ of the real numbers endowed with summation is a group $(\mathbb{R}, +)$ with identity element 0 and inverse $-g$.
- The whole numbers with summation $(\mathbb{Z}, +)$ is a group.
- The positive integers with summation $(\mathbb{N}, +)$ are not a group: there does not exist the inverse.
- The real numbers with multiplication $(\mathbb{R}, \cdot)$ has identity element 1, but is not a group because 0 does not have an inverse. To obtain a group, one can consider $\mathbb{R} \setminus \{0\}$.
- Consider the set of square matrices of size $n$ with either real entries $\mathrm{Mat}(n, \mathbb{R})$ or complex entries $\mathrm{Mat}(n, \mathbb{C})$. Taking the operation to be matrix multiplication, the identity to be $I = \mathrm{diag}(1, 1, 1, 1, \ldots)$, the set is not a group because the inverse element, inverse matrices, does not exist for matrices with null determinant.

**Definition 1.3.** The general linear group is defined as $\mathrm{GL}(n, \mathbb{R}) \equiv \{M \in \mathrm{Mat}(n, \mathbb{R}) \mid \det M \neq 0\}$ and is the largest and most general group of matrices. The definition is equivalent for matrices with complex entries.

**Definition 1.4.** The cyclic group $\mathbb{Z}_n$ is discrete and defined by

$$\mathbb{Z}_n \equiv \{e, a, a^2, a^3, \ldots, a^{n-1}\}, \quad a^n \equiv e$$

with generic operation $\circ$ where the notation implies $a^2 \equiv a \circ a$.

**Example 1.5.** Some examples are:

- $\mathbb{Z}_2 = \{0, 1\}$ with summation mod 2,
- the group $G = \{1, -1\}$ with multiplication,
- endowing the integers $\mathbb{Z}$ with summation mod $n$, one can split the set into equivalence classes that are the elements of the cyclic group. For example, if $n = 2$ then the sets

  $$\{0\} = \{0, 2, 4, \ldots\}, \quad \{1\} = \{1, 3, 5, \ldots\}$$

  are the elements of the cyclic group $\mathbb{Z}_2$. This group is important in particle physics.

**Definition 1.6.** The order of a group $G$, denoted by $|G|$, is given by the number of elements of the group.

**Definition 1.7.** A group $G$ is finite if its order is finite. Otherwise it is infinite.

**Definition 1.8.** A group $G$ is discrete if it is a countable set.

**Definition 1.9.** A group $G$ is abelian if its operation is commutative $g_1 \circ g_2 = g_2 \circ g_1$, $\forall g_1, g_2$.

**Example 1.10.** A few examples of abelian and non-abelian groups:

- Some abelian groups are $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$ which are also infinite. Though, the first is not countable, while the second is and as such it is a discrete group.
- All cyclic groups $\mathbb{Z}_n$ are abelian: $a^2 \circ a^3 = a^3 \circ a^2$.
- The general linear group $\mathrm{GL}(n, \mathbb{R})$ is not abelian: the order of matrix multiplication matters.

**Definition 1.11.** A ring $R$ is an abelian group with composition $+$, endowed with a second operation $\cdot : R \times R \to R$ with the properties:

- associativity $(r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3)$, $\forall r_1, r_2, r_3 \in R$;
- distributivity with respect to the first composition: $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3$ and equivalently for right multiplication.

**Remark 1.12.** The identity element of the relation $+$ is 0, while the inverse is $-r$. The second relation need not an identity nor an inverse.

**Definition 1.13.** A field $\mathbb{F}$ is a ring such that $\mathbb{F} \setminus \{0\}$ is an abelian group with respect to the ring's second operation.

**Example 1.14.** Some examples and counterexamples of fields are the following.

- Consider the integers with summation $(\mathbb{Z}, +)$: it is an abelian group. It is also a ring with the multiplication $n_1 \cdot n_2 \in \mathbb{Z}$. However, $(\mathbb{Z}, \cdot)$ is not a group because $n^{-1} \notin \mathbb{Z}$, therefore the set of integers is not a field.
- The real numbers with summation and multiplication is a field.
- The complex numbers are also a field.
- The cyclic group $\mathbb{Z}_n$ with summation is an abelian group. Adding the multiplication $\{n_1\} \cdot \{n_2\} \equiv \{n_1 \cdot n_2\}$, the cyclic group is a field only for $n$ prime. See the following theorem.

The fact that real numbers and complex numbers are fields implies one can define sets of matrices with entries from those fields.

**Theorem 1.15.** If $n$ is prime, then the cyclic group $\mathbb{Z}_n$ is a field (and vice versa).

**Example 1.16.** Some more examples:

- Consider the cyclic group $\mathbb{Z}_5$. It is an abelian group with respect to summation. One can study if $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ is an abelian group:

  $$\{2\} \cdot \{3\} = \{6\} = \{1\}$$

  This means that $\{3\}$ is the inverse of $\{2\}$. Continuing, one gets

  $$\{4\} \cdot \{4\} = \{1 + 5 \cdot 3\} = \{1\}$$

  So $\{4\}$ is its own inverse. Since the remaining elements are the additive identity $\{0\}$ and multiplicative identity $\{1\}$, the set $\mathbb{Z}_5$ is a field.

- The group $(\mathbb{Z}_4 \setminus \{0\}, \cdot)$ is not abelian because

$$\{2\} \cdot \{2\} = \{4\} = \{0\}$$

the set is not closed under multiplication. Therefore $\mathbb{Z}_4$ is not a field.

**Definition 1.17.** A module $M$ with respect to a ring $R$ is an abelian group endowed with an action $\cdot : R \times M \to M$ such that the following properties hold for every $r \in R$ and $m \in M$:

- associativity $(r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$
- distributivity $r_1 \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$ and $(r_1 \cdot r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$

Pay attention to whom the operations apply: operations in different sets have the same notation.

**Definition 1.18.** A vector space $V$ with respect to a field $\mathbb{F}$ is a module over $\mathbb{F}$ such that the multiplicative identity of $\mathbb{F}$ acts as the identity on $V$: $1 \cdot v = v \cdot 1 = v$, $\forall v \in V$.

**Definition 1.19.** An associative algebra $A$ over a ring $R$ is a ring and also a module with respect to $R$ such that the action of $R$ on $A$ is bilinear

$$r \cdot (a_1 \cdot a_2) = (r \cdot a_1) \cdot a_2 = a_1 \cdot (r \cdot a_2)$$

Again, pay attention to whom the operations apply.

[r] image of recap

**Example 1.20.** The set of square matrices of size $n$, $\mathrm{Mat}(n, \mathbb{F})$, with summation, matrix multiplication and scalar product forms an algebra over the field $\mathbb{F}$.

## Lecture 2

mar 03 ott 2023 08:30

**Definition 1.21.** The set of vectors $\{|e_i\rangle\}$ is a basis of a vector space $V$ if and only if $|v\rangle = v^i |e_i\rangle$, $v^i \in \mathbb{F}$ for all $|v\rangle \in V$.

**Definition 1.22.** The action of an inner product on a basis defines a metric $g^i{}_j = \langle e^i | e_j \rangle$. The metric $g$ is hermitian and if $g^i{}_j = \delta^i{}_j$ then the basis is orthonormal.

**Lemma 1.23.** Linear operators over $V$ form an algebra called $\mathrm{End}(V)$:

$$A : |v\rangle \mapsto |Av\rangle \in V\,, \quad A : |w\rangle = \alpha |v_1\rangle + \beta |v_2\rangle \mapsto |Aw\rangle = \alpha |Av_1\rangle + \beta |Av_2\rangle$$

**Proposition 1.24.** Linear operators follow these properties:

- composition: $(A \circ B) |v\rangle = A |Bv\rangle = |ABv\rangle$;
- given a basis $\{|e_i\rangle\}$, the operator $A$ is a matrix $n \times n$ over a field $\mathbb{F}$;
- a basis rotation $S$ is a linear operator which is invertible ($\det S \neq 0$):

$$|e'_i\rangle = S^j{}_i |e_j\rangle \implies \langle e'^i | e'_j \rangle = (S^\dagger)^i{}_k \langle e^k | e_l \rangle S^l{}_j \implies g' = S^\dagger g S$$

**Definition 1.25.** A linear operator $A$ is idempotent if $A^2 = A$ (and $A \neq I$). Given a basis $\{|e_i\rangle\}$, an example of idempotent linear operator the projector $A = |e_i\rangle\langle e^i|$:

$$A |v\rangle = |e_i\rangle\langle e^i| v^k |e_k\rangle = v^i |e_i\rangle$$

**Definition 1.26.** A linear operator $A$ is nilpotent if $\exists n \in \mathbb{N}$ such that $A^n = 0$ where 0 is the null operator. For example

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

One wants to categorize type of transformations to be able to study symmetries.

## 1.1 Classical groups of matrices

**Linear group.** The general linear group $\mathrm{GL}(n,\mathbb{C})$ is the largest group in the endomorphism algebra $\mathrm{End}(V)$. The group is parametrized by $2n^2$ real elements. The dimension of the group is given by the number of free parameters.

The special linear group is defined by

$$\mathrm{SL}(n,\mathbb{C}) \equiv \{M \in \mathrm{GL}(n,\mathbb{C}) \mid \det M = 1\} \subset \mathrm{GL}(n,\mathbb{C})$$

This set is also a group, not just a subset of matrices. The number of free parameters is $2n^2-1$ because of the condition on the determinant. The definition is analogous for $\mathrm{SL}(n,\mathbb{R})$. The set $\mathrm{SL}(n,\mathbb{Z})$ is also a group.

Consider a change of coordinates from $x^i$ to $\overline{x}^j = S^j{}_i x^i$ with the intention to perform an integral over space-time. The measures of the two coordinate systems are related by the Jacobian

$$\mathrm{d}^n\overline{x} = |\partial_x \overline{x}|\,\mathrm{d}^n x = \det S\,\mathrm{d}^n x$$

Matrices in the special linear group preserve the volume.

**Unitary group.** Consider the groups that preserve the metric of $V$ over $\mathbb{C}$:

$$|\overline{e}_i\rangle = U^j{}_i\,|e_j\rangle \implies \delta^i{}_j = \langle\overline{e}^i|\overline{e}_j\rangle = \left\langle e^k\right|(U^\dagger)^i{}_k U^l{}_j\,|e_l\rangle = (U^\dagger)^i{}_k U^l{}_j\,\delta^k{}_l \implies U^\dagger U = I$$

Unitary matrices belong to the unitary group $\mathrm{U}(n,\mathbb{C})$ which is defined as

$$\mathrm{U}(n,\mathbb{C}) \equiv \{M \in \mathrm{GL}(n,\mathbb{C}) \mid M^\dagger M = MM^\dagger = I\}$$

The number of free parameters is $2n^2 - n - n(n-1) = n^2$:

- the unitary condition $U^\dagger U$ imposes $n$ conditions corresponding to the elements on the diagonal, $[U^\dagger U]^i{}_i = 1$ (no sum);
- the upper and lower triangular parts of the matrix provide $\frac{n(n-1)}{2}$ conditions each.

The unitary group U(1) describes quantum electrodynamics. The determinant of a unitary matrix is

$$\det\left(U^\dagger U\right) = |\det U|^2 = 1 \implies \det U = \mathrm{e}^{\mathrm{i}\varphi}, \quad \varphi \in \mathbb{R}$$

One can define the special unitary group as

$$\mathrm{SU}(n,\mathbb{C}) \equiv \{M \in \mathrm{U}(n,\mathbb{C}) \mid \det M = 1\}$$

The number of free parameters is $n^2-1$. The strong and weak interactions are described by special unitary groups.

**Orthogonal group.** Consider the groups that preserve the metric of $V$ over $\mathbb{R}$. The orthogonal group is

$$\mathrm{O}(n,\mathbb{R}) \equiv \{M \in \mathrm{GL}(n,\mathbb{R}) \mid M^\top M = MM^\top = I\}$$

The number of free parameters is $n^2 - n - \frac{n(n-1)}{2} = \frac{n(n-1)}{2}$. The determinant of the orthogonal matrices is

$$\det\left(O^\top O\right) = (\det O)^2 = 1 \implies \det O = \pm 1$$

The special orthogonal group is

$$\mathrm{SO}(n,\mathbb{R}) \equiv \{M \in \mathrm{O}(n,\mathbb{R}) \mid \det M = 1\}$$

The number of free parameters is the same as above. For the unitary group and orthogonal group, the field is not usually specified, but rather understood to be $\mathbb{C}$ and $\mathbb{R}$ respectively.

**Indefinite orthogonal group.** Consider the groups that preserve the metrics of $V$ over $\mathbb{R}$ with signature $(p, q)$. Consider the metric to be

$$g^i{}_j = \eta^i{}_j = \mathrm{diag}(\underbrace{1, \dots, 1}_{p}, \underbrace{-1, \dots, -1}_{q})$$

Then

$$|\overline{e}'_i\rangle = R^j{}_i \, |e_j\rangle \implies \overline{\eta} = R^\top \eta R$$

The indefinite orthogonal group is

$$\mathrm{O}(p, q, \mathbb{R}) \equiv \{R \in \mathrm{GL}(n, \mathbb{R}) \mid \eta = R^\top \eta R\}$$

The indefinite special orthogonal group is

$$\mathrm{SO}(p, q, \mathbb{R}) \equiv \{R \in \mathrm{O}(p, q, \mathbb{R}) \mid \det R = 1\}$$

The number of free parameters is the same as the orthogonal group. The Lorentz group is $\mathrm{SO}(1, 3)$. The group $\mathrm{SO}(p, q)$ contains both ordinary rotations $\mathrm{SO}(p)$ and $\mathrm{SO}(q)$ subgroups.

### 1.1.1 Symplectic forms

**Definition 1.27.** A symplectic vector space $V$ is a vector space over a field $\mathbb{F}$ equipped with a bilinear form $\Omega : V \times V \to \mathbb{F}$. The bilinear form is:

- anti-symmetric: $\Omega(\vec{v}, \vec{w}) = -\Omega(\vec{w}, \vec{v})$;
- non-singular: $\Omega(\vec{v}, \vec{w}) = 0, \, \forall \vec{w} \implies \vec{v} = \vec{0}$,

**Theorem 1.28.** Given a square matrix $A$ of size $n$ and a constant $c$, then

$$\det(cA) = c^n \det A$$

*Proof.* From the hypotheses, it follows

$$\det(cA) = \det(cI) \, \det A = c^n \det A$$

□

Given a vector space $V$ over $\mathbb{R}$, one of its bases $\{|e_i\rangle\}$ and a bilinear form $\Omega_{ij} = \Omega(|e_i\rangle, |e_j\rangle)$, the aim is to represent the form $\Omega$ as a linear operator acting on the basis of $V$. Using anti-symmetry and the theorem above, it follows

$$\det \Omega = \det\left(-\Omega^\top\right) = (-1)^n \det \Omega$$

Because of non-singularity, the dimension $n$ can only be even. Using anti-symmetry and setting $\vec{w} = \vec{v}$ then

$$\Omega(\vec{v}, \vec{v}) = -\Omega(\vec{v}, \vec{v}) \implies \Omega_{ii} = 0 \,, \quad \Omega_{ij} = -\Omega_{ji}$$

Fixing $i$, if $\Omega_{ij} = 0$ for all $j$ then $|e_i\rangle = 0$. Negating this statement means if all basis' vectors are non-zero (which must hold for a vector to be part of a basis) then, for at least one $j$, it must be true that $\Omega_{ij} \neq 0$. One can choose $\Omega_{ij} = 0$ for all $j \neq i + 1$ and $\Omega_{i,i+1} = \lambda_i$. With this choice, one can obtain the canonical form

$$\Omega = \begin{pmatrix} 0 & 1 & & & \\ -1 & 0 & 1 & & \\ & -1 & 0 & 1 & \\ & & -1 & 0 & 1 \end{pmatrix}$$

Another canonical form obtained by change of basis from the previous is

$$\Omega = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$$

given by the conditions

$$\Omega_{i,\frac{n}{2}+i} = 1\,, \quad \Omega_{ij} = 0\,, \quad \forall j \neq \frac{n}{2} + i\,, \quad i < \frac{n}{2}$$

These two forms amount to a decomposition of the vector space $V = V_1 \oplus V_1^*$ — where $V_1^*$ is the dual space of $V_1$ — such that a basis of $V$ can be written as

$$\{|e_1\rangle\,, \ldots, |e_m\rangle\,, |f_1\rangle\,, \ldots, |f_m\rangle\}\,, \quad |e_i\rangle \leftrightarrow V_1\,, \quad |f_i\rangle \leftrightarrow V_1^*$$

As such the dimension is always even

$$n = \dim V = \dim V_1 + \dim V_1^* = 2\dim V_1 = 2m$$

A generic transformation of a symplectic form

$$\Omega' = A\Omega B$$

needs to preserve the form's properties:

$$\begin{aligned}(\Omega')^\top &= B^\top \Omega^\top A^\top = -B^\top \Omega A^\top \\ &= -\Omega' = -A\Omega B \implies A = B^\top\end{aligned}$$

**Symplectic group.** The symplectic group is

$$\mathrm{Sp}(2n, \mathbb{F}) \equiv \{M \in \mathrm{Mat}(2n, \mathbb{F}) \mid M^\top \Omega M = \Omega\}\,, \quad (\det M)^2 = 1$$

This group also preserves the pfaffian

$$[\mathrm{Pf}(N)]^2 = \det N$$

## 1.2 Morphisms

**Definition 1.29.** A morphism $\phi$ is a map from a group $G$ to another group $G'$, $\phi : G \to G'$, $\phi(g) = g'$ with $g \in G$ and $g' \in G'$.

**Definition 1.30.** A homomorphism is a morphism that respects the composition law of $G$ and $G'$: $\forall g_1, g_2 \in G$, $\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$. The first composition is in $G$, the second is in $G'$.

**Definition 1.31.** An isomorphism is an invertible homomorphism. It is a bijective map: $\forall g \in G$, $\phi(g) = g' \in G'$ and $\exists \phi^{-1} : G' \to G$ such that $\phi^{-1}(g') = \phi^{-1}(\phi(g)) = g$.

**Definition 1.32.** An automorphism is an isomorphism with $G' = G$.

## Lecture 3

lun 09 ott 2023 08:30

**Definition 1.33.** A representation $\rho$ is a homomorphism where $G'$ is a group of matrices:

$$\rho : G \to \mathrm{GL}(n, \mathbb{C})$$

The number $n$ is the dimension of the representation.

**Example 1.34.** A few examples:

- the trivial homomorphism exists: it maps all elements into the identity, $\phi(g) = e'$, $\forall g \in G$, $e' \in G'$; this is used in the context of representations because, if it exists, there is always a group element $g$ mapped to the identity of the general linear group.
- Take a function between two cyclic groups $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2$. To create a homomorphism one can take $\phi(e) = \phi(a^2) = e'$ and $\phi(a) = \phi(a^3) = a'$. One then has

$$\phi(ea) = \phi(a) = a'\,, \quad \phi(ea) = \phi(e)\phi(a) = e'a' = a'$$

- It's possible to construct an isomorphism between the definitions of $\mathbb{Z}_n$: the set $\{e, a, \dots, a^{n-1}\}$ with multiplication and the set $\{\{0\}, \{1\}, \dots, \{n-1\}\}$ with addition.
- One can also construct an isomorphism between $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$. The following should hold $\phi(g_1 + g_2) = \phi(g_1)\phi(g_2)$. Such an isomorphism is the exponential function $\mathrm{e}^{g_1+g_2} = \mathrm{e}^{g_1}\mathrm{e}^{g_2}$. Its inverse is the natural logarithm.
- An example of non trivial automorphism considers $\mathbb{Z}_3$. One can define

  $$\phi(e) = e' \,, \quad \phi(a) = a'^2 \,, \quad \phi(a^2) = a'$$

  and one should check that the morphism respects the composition law

  $$\phi(a)\phi(a^2) = \phi(a^3) = e' \,, \quad \phi(a)\phi(a^2) = a'^2 a = e'$$

  However, this is not true for $\mathbb{Z}_4$. Consider the mapping

  $$\phi(e) = e' \,, \quad \phi(a) = a'^2 \,, \quad \phi(a^2) = a'$$

  The fourth element is given by

  $$\phi(a)\phi(a^3) = b^3$$

  but

  $$\phi(a)\phi(a^3) = \phi(a^4) = \phi(e) = e' \,, \quad \phi(a)\phi(a^3) = a'^2 e' = a'^2$$

**Definition 1.35.** Two elements $h_1$ and $h_2$ of a group $G$ are conjugate of one another if there exists a third element $g$ of the group such that $h_2 \equiv g^{-1} h_1 g$.

One can then build equivalence classes.

**Definition 1.36.** An internal automorphism is the mapping given by conjugating every element of a group while fixing $g$:

$$\phi_g : G \to G \,, \quad \phi_g : h \mapsto g^{-1} h g$$

The inverse mapping is

$$\phi_g^{-1} : h \mapsto g h g^{-1}$$

**Lemma 1.37.** The set of automorphisms of a group is itself a group $\mathrm{Aut}(G)$ with the operation of composition of functions.

**Definition 1.38.** Given a set $S = \{s_1, \dots, s_k\}$ of $k$ elements, the set of all words $S'$ created by the concatenation of the elements of the set $S$, together with an equivalence relation, forms a free group. A word can be of any length, with as many repeated elements as one wants. The composition is given by concatenating words. The identity is the null word.

**Definition 1.39.** Given a subset of words $R \subset S'$, a presentation is a group whose elements are given by the equivalence classes in $S$ of the relation $r = e$ for all $r \in R$. The set $R$ is the set of relations.

**Remark 1.40.** In terms of groups, the set $S'$ is a group and one wants to identify the elements of $S$ that give all the elements of the group utilizing equivalence classes. The set $S$ is the set of generators: the minimal set that gives all the group elements.

**Definition 1.41.** The number of generators is called rank.

**Example 1.42.** The set of generators of the cyclic group $\mathbb{Z}_n$ has rank one because it only contains the element $a$ with relation $a^n = e$: all other elements can be generated from $a$.

**Theorem 1.43.** Every finite group $G$ admits an homomorphism of the form $\phi : G \to G'$ where $G'$ is a free group. Therefore, a presentation always exists.

**Example 1.44.** A presentation for $\mathbb{Z}_n$ is $\{a, a^n = e\}$.

# 2 Dihedral groups

**Definition 2.1.** A dihedral group $\mathrm{D}_k$ is a group of symmetries of a $k$-gon.

**Remark 2.2.** The course considers the Euclidean plane $\mathbb{R}^2$ and its isometries, transformations that keep invariant the distance between points. Such isometries are translation, rotation and reflection.

**Definition 2.3.** A figure is a subset of $\mathbb{R}^2$ delimited by a closed curve.

**Definition 2.4.** In $\mathbb{R}^2$, a $k$-gon is a regular polygon figure with $k$ side.

**Three points.** A 3-gon is a regular triangle. One wants to find all transformations that keep the triangle in the same situation as initially. Such transformations are the identity, rotations by $\mathrm{e}^{\mathrm{i}\frac{2}{3}\pi}$ or $\mathrm{e}^{\mathrm{i}\frac{4}{3}\pi}$, and reflections $R_i$ by each side's axis of the triangle. The number of elements of the dihedral group is 6. [r] image

One wants to find the minimal set of transformations as to find the generators. Let $r = \mathrm{e}^{\mathrm{i}\frac{2}{3}\pi}$ and $\sigma = R_1$. Combining some transformations one gets

$$\sigma r = R_3\,, \quad r\sigma = R_2\,, \quad r^2 = \mathrm{e}^{\mathrm{i}\frac{4}{3}\pi}\,, \quad r^2\sigma = R_3$$

Note that the order of operation is from right to left. The presentation of the dihedral group is

$$\mathrm{D}_3 = \{\{r, \sigma\}, r^3 = e, \sigma^2 = e, (\sigma r)^2 = e\}$$

The rank is then 2.

**Two points.** Since two sides are not enough for a planar figure, one can consider two points connected by two overlapping segments. The transformations include rotations by $r = \mathrm{e}^{i\pi}$ and reflections along the $x$ and $y$ axes. Let $\sigma = R_x$, then $\sigma r = R_y$. The presentation is

$$\mathrm{D}_2 = \{\{r, \sigma\}, \sigma^2 = e, r^2 = e, (\sigma r)^2 = e\}$$

This group is abelian.

**One point.** There is only one transformation to be made and that is a reflection about an arbitrary axis. Given $\sigma = R$ then the presentation is

$$\mathrm{D}_1 = \{\{\sigma\}, \sigma^2 = e\}$$

This group is abelian and it's isomorphic to the cyclic group: $\mathrm{D}_1 \simeq \mathbb{Z}_2$.

**Four points.** The transformations are rotations every $\mathrm{e}^{\mathrm{i}\frac{\pi}{2}}$ and four reflections, two along the diagonals, two splitting the sides. The presentation is

$$\mathrm{D}_4 = \{\{\sigma, r\}, \sigma^2 = e, r^4 = e, (\sigma r)^2 = e\}$$

**Arbitrary points.** The $n$ dihedral group has $n+n$ elements given by rotations and reflections. The rank is 2 for $n > 1$. The group is not abelian for $n > 2$. The presentation is

$$\mathrm{D}_n = \{\{\sigma, r\}, r^n = e, \sigma^2 = e, (\sigma r)^2 = e\}$$

**Subgroups.** The rotations are a subgroup $\mathbb{Z}_n = \{r, r^n = e\}$ and so is each reflection $\mathbb{Z}_2 = \{\sigma, \sigma^2 = e\}$ along some axes: there are $n$ copies of $\mathbb{Z}_2$.

**Definition 2.5.** A subgroup is a subset $H$ of a group $G$ which is a group itself under the same composition of $G$. It suffices to check

$$\forall h_1, h_2 \in H, h_1 \cdot h_2 \in H\,, \quad \forall h \in H, \exists h^{-1} \in H \mid hh^{-1} = h^{-1}h = e$$

**Example 2.6.** Some trivial examples are $H = G$ and $H = \{e\}$.

**Lecture 4**

lun 16 ott 2023 08:30

# 3 Finite groups of small order

Groups can be represented through a multiplication table, like the following

| | $e$ | $g_1$ | $g_2$ |
|---|---|---|---|
| $e$ | $g_1$ | $g_2$ | $g_2$ |
| $g_1$ | $g_1$ | $g_1^2$ | $g_1 g_2$ |

**Order one.** A group of order one contains only the identity.

**Order two.** For a group of order two, $G = \{e, a\}$, the table is

| | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | $a^2$ |

To be a group, then $a^2$ must be an element of $G$. If $a^2 = a$ then

$$a^{-1}a^2 = a\,, \quad a^{-1}a^2 = a^{-1}a = e$$

which is a contradiction. So if $a^2 = e$ then one has $\mathbb{Z}_2 = \{e, a\}$ with $a^2 = e$. It has rank one, it is abelian, it has no subgroups and it is the only group of order two.

**Order three.** For a group of order three, the table is

| | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $a^2$ | $ab$ |
| $b$ | $b$ | $ba$ | $b^2$ |

One can follow a branching logic as before. Setting $a^2 = a$ leads to $a = e$ which means that the group is no longer of order three.

So if $a^2 = e$ then $a^{-1} = a$. The product $ab$ must be an element of the group. Therefore

- if $ab = e$ then $b = a$;
- if $ab = b$ then $a = e$;
- if $ab = a$ then $b = e$.

These are not acceptable conditions since the order would no longer be three. So one must modify the previous condition to $a^2 = b$:

- if $ab = b$ then $a = e$, or if $ab = a$ then $b = e$, which are not acceptable;
- if $ab = e$ then $b^2$ must be an element of the group also:
  - ◇ if $b^2 = b$ then $b = e$, not acceptable;
  - ◇ if $b^2 = e$ then $b = a$, not acceptable;
  - ◇ if $b^2 = a$ then it is a valid condition.

The only such group is $\mathbb{Z}_3$:

| | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $b$ | $e$ |
| $b$ | $b$ | $e$ | $a$ |

When the multiplication table is symmetric, the group is abelian. From the multiplication table one can identify subgroups by looking at smaller multiplication tables already known (not necessarily with entries one next to each other). In this case, $\mathbb{Z}_3$ has rank one, it is the only group of order three and has no subgroups.

**Order four.** For a group of order four, the table is

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $a^2$ | $ab$ | $ac$ |
| $b$ | $b$ | $ba$ | $b^2$ | $bc$ |
| $c$ | $c$ | $ca$ | $cb$ | $c^2$ |

Repeating the same branching procedure gives two ways of filling the multiplication table. The first one leads to $\mathbb{Z}_4$. It is abelian and has rank 1 with $a^4 = e$:

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $b$ | $c$ | $e$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $e$ | $a$ | $b$ |

Looking at the table one can see the sub-table of $\mathbb{Z}_2 = \{e, a^2\} = \{e, b\}$ in the upper-left corner.

The second way of filling the multiplication table gives the dihedral group $\mathrm{D}_2$. It is abelian and has rank 2:

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

One can identify three subgroups $\mathbb{Z}_2$, two the corners and one at the center. There's also a fourth hidden $\mathbb{Z}_2$ subgroup that is found by combining the corners in $2 \times 2$ blocks.

These two groups constructed with the branching procedure are not isomorphic: one can look at the subgroups, in this case how many there are. Also by looking at their subgroups, it holds

$$\mathrm{D}_2 = \mathbb{Z}_2 \otimes \mathbb{Z}_2$$

where $\otimes$ is the Cartesian product later called direct product.

**Higher orders.** At order five there is only $\mathbb{Z}_5$. At order six there are $\mathbb{Z}_6$ and the group of permutations $\mathrm{S}_3$. At order seven there is $\mathbb{Z}_7$. One may notice that for prime-number orders, there are only cyclic groups.

## 3.1 Groups of permutations

**Definition 3.1.** The set of $n!$ permutations of $n$ objects forms a group $\mathrm{S}_n$ (also called the symmetric group).

**Remark 3.2.** A permutation is an automorphism over the set of $n$ objects. The group of permutations $\mathrm{S}_n$ is a group of automorphisms.

**Notation.** The permutation of $n$ elements is represented as

$$p = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ p_1 & p_2 & p_3 & \cdots & p_n \end{pmatrix}$$

In the product $PQ$ the permutation that acts first is $Q$ followed by $P$.

**Representation in matrix notation.** Given a permutation $p \in \mathrm{S}_n$, its $n \times n$ matrix representation is $[P]_{ij} = \delta_{jp_i}$. [r]

A representation is a homomorphism so it must preserve the group structure. In fact the matrix representation of a product of permutations must represent the product of the permutations:

$$[PQ]_{ij} = \sum_k P_{ik} Q_{kj} = \sum_k \delta_{ip_k} \delta_{kq_j} = \delta_{i,(pq)_j}$$

[r]

Permutations are used for rotations on the lattice.

**Cycle notation.** The cycle notation is compact way to write permutations. It has the properties

- the sum of all cycle lengths is equal to $n$,
- the order of the cycles is irrelevant,
- the cyclic order within a cycle is irrelevant.

For example

$$(134)(2)$$

means that 2 stays put, while 1 and 3 interchange then 3 and 4 interchange. The last property means $(134) = (341) = (413)$. It is possible rewrite a cycle of length $n$ in terms of two cycles that pivot around the same element: $(134) = (14)(13)$.

**Lemma 3.3.** Every cycle can be written as the product of two cycles with repeated elements. For convention, one always chooses 1 to be the pivotal, repeated number.

**Proposition 3.4.** It holds

$$(1\,2\,\cdots\,m) = (1\,m)(1\,m-1)\cdots(13)(12)$$

It follows that

$$(ij) = (1i)(1j)(1i)$$

From the cycle notation, one can represent the entire group. By combining two-cycles one can get arbitrary permutations. So, the symmetric group $\mathrm{S}_n$ has the following generators

$$\{(12), (13), \ldots, (1n)\}\,, \quad \operatorname{rank} \mathrm{S}_n = n - 1$$

The identity is given by $(12)^2(13)^2(14)^2$ but is not part of the generators.

**Definition 3.5.** The parity of an element $g \in \mathrm{S}_n$ is the number of two-cycles in any two-cycle decomposition.

**Definition 3.6.** Since the identity $e$ is even under parity, the set of even permutations forms a subgroup called alternating group $\mathrm{A}_n$. Its order is $2^{-1}n!$.

**Example 3.7.** Consider $\mathrm{S}_3 = \{e, (12), (13), (23), (123), (132)\}$. Let $g_1 = (12)$ and $g_2 = (23)$. It is not abelian

$$abc \xrightarrow{g_1} bac \xrightarrow{g_2} bca\,, \quad abc \xrightarrow{g_2} acb \xrightarrow{g_1} cab$$

The identity is given by $e = (12)^2(13)^2$. There are also three copies of $\mathbb{Z}_2$:

$$\{e, (12)\}\,, \quad \{e, (13)\}\,, \quad \{e, (23)\}$$

The alternating group is given by the even permutations

$$\mathrm{A}_3 = \{e, (123), (132)\}$$

At order three, there is only one group, so $\mathrm{A}_3 \simeq \mathbb{Z}_3$. At order six, one has $\mathrm{D}_3 \simeq \mathrm{S}_3$. For general groups, $\mathrm{S}_n \not\simeq \mathrm{D}_n$ because $|\mathrm{D}_n| = 2n$ and $|\mathrm{S}_n| = n!$. The dihedral group is a subset of the symmetric group: there are permutations that cannot be achieved from rotations and reflections.

**Lemma 3.8** (Rearrangement)**.** If $g, a, b$ are elements of a group $G$ and $g \circ a = g \circ b$, then $a = b$.

*Proof.* Multiplying $g \circ a = g \circ b$ by $g^{-1}$ on the left one finds the thesis. □

**Corollary 3.9.** Consider the group $G$ of $n$ elements. Multiplying every element by $h \in G$ gives a new group, mapping the group $G$ to itself. It is an automorphism.

**Definition 3.10.** A morphism $\varphi_h : G_n \to \mathrm{S}_{|G|}$, $h \mapsto p_h$ such the above gives the permutations of the set $G$. It is a homomorphism: $\varphi_{h_1}\varphi_{h_2} = \varphi_{h_1 h_2}$. The range of $\varphi_h$ is a subset of $\mathrm{S}_{|G|}$ and it is a subgroup $P_h$. [r]

**Theorem 3.11** (Cayley's)**.** Every group $G$ of order $n$ is isomorphic to a subgroup of $\mathrm{S}_n$ called Cayley's group.

### Lecture 5

mar 17 ott 2023 08:30

**Corollary 3.12.** Two consequences are

- given a permutation $P_h$ in Cayley's group, it cannot contain 1-cycles except for the identity $h = e$;
- a permutation $P_h$ in Cayley's group can be decomposed in cycles of equal length. If $n$ is prime, the corresponding permutations in Cayley's group can only contain non-factorized $n$-cycles. This means that one 1-cycle is the identity as it is one $n$-cycle: the entire Cayley's group is built from them and as such has rank one and order $n$. It is $\mathbb{Z}_n$.

**Remark 3.13.** Applying $n$ times a cycle of length $n$, one gets the identity.

**Theorem 3.14.** If the order $n$ of a group $G$ is prime, then it must be isomorphic to $\mathbb{Z}_n$.

# 4 Structural properties of groups

**Definition 4.1.** Two elements are said to be conjugate $g_1 \sim g_2$ if and only if $\exists h \in G$ such that $h g_1 h^{-1} = g_2$. The relation induces a partitioning of the group into equivalence classes.

**Definition 4.2.** If $H$ is a subgroup of $G$ and $a \in G$, then its conjugate group is

$$H' = \{aha^{-1}, \forall h \in H\} \equiv aHa^{-1}$$

which is also a subgroup.

**Lemma 4.3.** If $H$ and $H'$ are conjugate subgroups, then either $H \cap H' = \{e\}$ or $H = H'$.

**Definition 4.4.** An invariant subgroup $H$ of $G$ is identical to all its conjugate subgroups. It is also called normal. The set $H \subseteq G$ is invariant if and only if $gHg^{-1} = H$ for all $g \in G$.

**Example 4.5.** A few examples:

- Consider the group of permutations

  $$\mathrm{S}_3 = \{e, (12), (13), (23), (123), (132)\}$$

  It has three copies of $\mathbb{Z}_2$ given by the 2-cycles

  $$\{e, (12)\}, \quad \{e, (13)\}, \quad \{e, (23)\}$$

  The conjugate subgroup of the first $\mathbb{Z}_2$ is

  $$(23)^{-1} e (23) = e, \quad (23)^{-1}(12)(23) = (23)(12)(23) = (13)$$

  but this does not remain within the group. Remember that two-cycles are their own inverse. So $H' \neq H$ but only share the identity. Since the two sets do not coincide, by the lemma $\mathbb{Z}_2$ is not invariant. Consider instead the subgroup

  $$H_2 = \{e, (123), (132)\} \simeq \mathbb{Z}_3$$

  Its conjugate group is

  $$(12)H_2(12) = \{e, (132), (123)\} = H_2$$

  Therefore $\mathbb{Z}_3$ is invariant.

- Consider
$$\mathbb{Z}_4 = \{e, a, a^2, a^3\}$$
It has one subgroup
$$\mathbb{Z}_2 = \{e, a^2\}$$
Its conjugate is
$$a^{-1}\{e, a^2\}a = \{e, a^2\}, \quad (a^3)^{-1}\{e, a^2\}a^3 = \{e, a^2\}$$
Remember that $\mathbb{Z}_2$ is abelian. It is also abelian.
- Consider the dihedral group $\mathrm{D}_n$. The relations used $r^n = e$ and $\sigma^2 = e$ corresponding to a $\mathbb{Z}_n$ and $\mathbb{Z}_2$. In general, $\mathbb{Z}_n \subset \mathrm{D}_n$ is normal, while $\mathbb{Z}_2 \subset \mathrm{D}_n$ is not invariant. On the other hand, in general $\mathbb{Z}_n \subset \mathrm{S}_n$ is not invariant.

**Lemma 4.6.** All subgroups of abelian groups are invariant subgroups.

**Definition 4.7.** A group is simple if it does not contain any non-trivial invariant subgroup.

**Definition 4.8.** A group is semi-simple if it does not contain any abelian invariant subgroup.

**Example 4.9.** Some examples:

- The group $\mathbb{Z}_4$ has a $\mathbb{Z}_2$ subgroup which is invariant and abelian: the group $\mathbb{Z}_4$ is not simple nor semi-simple.
- The group $\mathrm{S}_3$ has a $\mathbb{Z}_3$ subgroup which is invariant and abelian.
- The cyclic group $\mathbb{Z}_n$ with $n$ prime is a simple group (because it does not admit subgroups).

**Remark 4.10.** The simple property describes whether a group is fundamental or has substructures.

**Definition 4.11.** Consider a set $H$ subgroup of $G$, an element $g \in G$ such that $g \notin H$. The set of elements
$$gH = \{gh_1, gh_2, \ldots\}$$
is a left coset. Similarly $Hg$ is a right coset.

**Remark 4.12.** Cosets have the same order of their parent group.

**Lemma 4.13.** Cosets are not subgroups.

*Proof.* Cosets do not have the identity element and $g$ can't be the identity if it is not part of the subgroup $H$. □

**Lemma 4.14.** Two cosets either coincide completely or have no common elements.

*Proof.* Consider two cosets $pH$ and $qH$. If $ph_i = qh_j$ then $q^{-1}p = h_j h_i^{-1} \in H$. If? it holds for all elements, then
$$q^{-1}pH = H \implies pH = qH$$
[r] □

**Theorem 4.15** (Lagrange)**.** The order of a finite group must be an integer multiple of the order of any of its subgroups.

**Example 4.16.** Consider the symmetric group $\mathrm{S}_3$ and one of its subgroup
$$H_1 = \mathrm{A}_3 = \{e, (123), (132)\}$$
The only coset that can be built is
$$(12)H_1 = (13)H_1 = (23)H_1 = \{(12), (13), (23)\}$$
Cosets induce a partitioning of the group. Consider one $\mathbb{Z}_2$ subgroup
$$\mathbb{Z}_2 \simeq H_2 = \{e, (12)\}$$
It has two cosets
$$(23)H_2 = (132)H_2 = \{(23), (132)\}, \quad (13)H_2 = (123)H_2 = \{(13), (123)\}$$

**Theorem 4.17.** If $H$ is an invariant subgroup of $G$, then its left and right cosets coincide. The set of cosets endowed with the composition

$$pH \cdot qH = (p \cdot q)H$$

forms a group called quotient group of $G$ denoted by ${}^{G}/_{H}$, [r] with order ${}^{|G|}/_{|H|}$.

*Proof.* It holds

$$gH = gH(g^{-1}g) = (gHg^{-1})g = Hg$$

Also

$$ph_iqh_j = p(qq^{-1})h_iqh_j = (pq)h_k$$

where $q^{-1}h_iq \in H$ and $h_j \in H$. □

**Example 4.18.** Two examples are:

- Consider the group $\mathbb{Z}_4$. It has an invariant subgroup

  $$\mathbb{Z}_2 \simeq H = \{e, a^2\}$$

  which has only one coset

  $$M = aH = \{a, a^3\} = a\mathbb{Z}_2 = a^3\mathbb{Z}_2$$

  In the sense of sets, that is multiplying all the elements together, one has

  $$HH = H\,, \quad HM = MH = M\,, \quad MM = H$$

  Therefore ${}^{\mathbb{Z}_4}/_{\mathbb{Z}_2} \simeq \mathbb{Z}_2$ the partitioning sets behave as elements of $\mathbb{Z}_2$.

- The set $\mathrm{S}_3$ has three elements as it does $\mathrm{A}_3$. The quotient has only two elements. Since the only group of order two is $\mathbb{Z}_2$ then

  $${}^{\mathrm{S}_3}/_{\mathrm{A}_3} \simeq \mathbb{Z}_2$$

## 4.1 Multiplication of groups

**Definition 4.19.** Given two groups $H_1$ and $H_2$, their direct product is the set of pairs

$$\{(h_1, h_2) \mid h_1 \in H_1, h_2 \in H_2\}$$

with the composition law

$$(h_1, h_2) \cdot (h_1', h_2') = (h_1h_1', h_2h_2') \in H_1 \otimes H_2$$

The order of the direct product is $|H_1 \otimes H_2| = |H_1||H_2|$. The sets $H_1$ and $H_2$ are invariant subgroups of $H_1 \otimes H_2$.

**Remark 4.20.** Consider

$$(h_1', h_2')^{-1}(e_1, h_2)(h_1', h_2') = (h_1'^{-1}, h_2'^{-1})(e_1, h_2)(h_1', h_2') = (h_1'^{-1}h_1', h_2'^{-1}h_2h_2') = (e_1, h_2'^{-1}h_2h_2')$$

[r]

**Definition 4.21.** Given a group $G = H_1 \otimes H_2$, it is the direct product group of the subgroups $H_1$ and $H_2$ if

- $h_1h_2 = h_2h_1$ for all $h_1 \in H_1$ and $h_2 \in H_2$;
- the intersection is $H_1 \cap H_2 = \{e\}$;
- for all $g \in G$, $\exists h_1 \in H_1, h_2 \in H_2$ such that $g = h_1h_2$.

**Remark 4.22.** If $G = H_1 \otimes H_2$ with $H_1$ and $H_2$ invariant subgroups then

$${}^{G}/_{H_1} \simeq H_2\,, \quad {}^{G}/_{H_2} \simeq H_1$$

[r]