Mathematical Methods for Physics

Maso*

November 11, 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.

*https://github.com/M-a-s-o/notes

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
$$V_{ab}(\mathbf{x}, t)\phi(\mathbf{x}, t)$$
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 $\mathbf{x} \to -\mathbf{x}$: 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

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

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

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

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

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 Ω 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 $\mathbf{w} = \mathbf{v}$ then

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

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 ϕ 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 ρ 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 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 $e^{i\frac{\pi}{2}}$ and four reflections, two along the diagonals, two splitting the sides. The presentation is

$$D_4 = \{\{\sigma, r\}, \sigma^2 = e, r^4 = e, (\sigma r)^2 = e\}$$

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

$$D_n = \{\{\sigma, r\}, r^n = e, \sigma^2 = e, (\sigma r)^2 = e\}$$

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 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 2×2 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 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 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 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 S_n has the following generators

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

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 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 φ_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 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 $hg_1h^{-1} = g_2$. 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 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 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 S_3 and one of its subgroup

$$H_1 = A_3 = \{e, (123), (132)\}$$

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

$$ph_i qh_j = p(qq^{-1})h_i qh_j = (pq)h_k$$

where $q^{-1}h_i q \in H$ 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 S_3 has three elements as it does A_3. The quotient has only two elements. Since the only group of order two is $\mathbb{Z}_2$ then

$${}^{S_3}/_{A_3} \simeq \mathbb{Z}_2$$

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

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

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

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

[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

- $h_1 h_2 = h_2 h_1$ 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 $g = h_1 h_2$.

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]

Lecture 6

lun 23 ott 2023 08:30

Example 4.23. Consider

$$\mathbb{Z}_6 = \{e, a, a^2, a^3, a^4, a^5\}$$

Two subgroups are

$$H_1 = \{e, a^3\} \simeq \mathbb{Z}_2\,, \quad H_2 = \{e, a^2, a^4\} \simeq \mathbb{Z}_3$$

The subgroups are abelian because the group is. They are also invariant $ghg^{-1} = hgg^{-1} = h$. Therefore one can write

$$\mathbb{Z}_6 = \mathbb{Z}_2 \otimes \mathbb{Z}_3 \implies {}^{\mathbb{Z}_6}/_{\mathbb{Z}_3} \simeq \mathbb{Z}_2$$

One may think that one can factor a cyclic group in terms of smaller cyclic groups by using factorization.

Theorem 4.24 (Chinese remainder)**.** Let p and q be coprime integers. Then

$$\mathbb{Z}_{pq} \simeq \mathbb{Z}_p \otimes \mathbb{Z}_q$$

Theorem 4.25. Let $\phi : G \to G'$ be a homomorphism. The kernel of ϕ

$$\operatorname{Ker}\phi = \{g \in G \mid \phi(g) = e'\} \equiv K$$

is an invariant subgroup of G. The quotient $G/\operatorname{Ker}\phi$ is isomorphic to G'.

Example 4.26. Consider again $\mathbb{Z}_6$ and assume not knowing its structure. Then

$$H_1 = \{e, a^3\}, \quad aH_1 = \{a, a^4\}, \quad a^2H_1 = \{a^2, a^5\}$$

There is a natural mapping ϕ using this structure. One can map every coset to the elements that multiply H_1:

$$\{e', b, b^2\}$$

The set $H_1 \simeq \mathbb{Z}_2$ is the kernel of ϕ. Therefore

$$G/H_1 \simeq G' = \mathbb{Z}_3$$

The direct product is restrictive because it requires subgroups to be invariant. One may want a more loose definition of product.

Definition 4.27. Given two groups G and K with different operations $g_i \cdot g_j$, $k_i \circ k_j$, assuming G acts as a group of transformations over K

$$\forall g \in G, \quad g : K \to K, \quad k_i \mapsto g(k_i) = k_j$$

the semi-direct product, $G \ltimes K$, is the group given by the direct product endowed with the composition law

$$(g_1, k_1)(g_2, k_2) = (g_1 \cdot g_2, k_1 \circ g_1(k_2))$$

Proposition 4.28. A few properties of this definition:

- the definition is the composition law of Poincaré transformations,
- the inverse element of (g, k) is

$$(e, e) = (g, k)^{-1}(g, k) \implies (g, k)^{-1} = (g^{-1}, [g^{-1}(k)]^{-1})$$

- the order is

$$|G \ltimes K| = |G||K|$$

- the set K is an invariant subgroup of $G \ltimes K$ but not of G

$$(e, k) \in K \subset G \ltimes K \implies (g, h)^{-1}(e, k)(g, h) = (g^{-1}eg, \cdots) \in K$$

- if G acts trivially on K

$$g(k) = k, \forall g \in G, \forall k \in K$$

then

$$G \ltimes K = G \otimes K$$

Proposition 4.29. Given the subgroups K and H of G, then $G = K \ltimes H$ if

- H is invariant,
- the intersection is $K \cap H = \{e\}$,

- given $g \in G$, there exists $k \in K$ and $h \in H$ such that

$$g = (k, e)(e, h)$$

If only one subgroup is invariant, then one uses a semi-direct product. If both subgroups are invariant, one uses the direct product.

Example 4.30. In the dihedral groups, one can identify two subgroups: $\mathbb{Z}_k$ and $\mathbb{Z}_2$. Only the first is invariant. Therefore

$$\mathrm{D}_k/\mathbb{Z}_k \simeq \mathbb{Z}_2 \implies \mathrm{D}_k \simeq \mathbb{Z}_2 \ltimes \mathbb{Z}_k$$

Example 4.31. Consider

$$\mathbb{Z}_4/\mathbb{Z}_2 \simeq \mathbb{Z}_2\,, \quad \mathbb{Z}_4 \not\simeq \mathbb{Z}_2 \ltimes \mathbb{Z}_2$$

Because one cannot identify a second $\mathbb{Z}_2$ subgroup inside $\mathbb{Z}_4$.

5 Classification of finite simple groups

From simple groups one can build any other group.

There are 18 infinite series of finite simple groups:

- $\mathbb{Z}_p$ with p prime,
- the alternating subgroup A_n subgroup with the permutation group with $n \geq 5$,
- classical groups of matrices over finite fields.

There are also 26 exceptional groups (simple and finite):

- the smallest such group is Mathieu group M_{11} of order $7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$.
- the biggest such group is the monster group F_1, it contains 20 out of the 26 exceptional groups. Its order is about 8.08×10^{53}. This group is associated with Galois Theory.

6 Groups of space-time symmetries

Definition 6.1. The Euclidean group $\mathrm{ISO}(n)$ (inhomogeneous special orthogonal group?) consists of all continuous linear transformations of the n-dimensional Euclidean space $\mathbb{R}^n$ which leave the norm of all vectors invariant. The norm is defined as

$$\|x\|^2 = \sum_{i=0}^{n-1} (x^i)^2$$

A generic element of the Euclidean group $\mathrm{ISO}(n)$ maps

$$x^i \mapsto x'^i = R^i{}_j x^j + b^i$$

where R is a rotation and b is a translation.

6.1 Two dimensions

Rotations. An active transformation rotates a point P and keeps the axes fixed, while a passive rotation is the opposite, the axes are rotated. The latter will be used. The rotation is then

$$\begin{bmatrix} x'_p \\ y'_p \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x_p \\ y_p \end{bmatrix} = R(\theta) \begin{bmatrix} x_p \\ y_p \end{bmatrix}$$

All rotation matrices $R(\theta)$ form a group. In fact

$$R(\theta_1)R(\theta_2) = R(\theta_1 + \theta_2)\,, \quad RR^\top = I$$

The matrices are orthogonal and have determinant equal to $\det R = 1$. In two dimensions, rotations form the special orthogonal group $\mathrm{SO}(2)$. It is abelian, its identity is $R(\theta = 0) = I$, the inverse is $R^{-1}(\theta) = R(-\theta)$.

Translations. A translation is a transformation such that

$$T(\mathbf{b}) : x^i \mapsto x'^i = T(\mathbf{b}_1 + \mathbf{b}_2)$$

It holds

$$T(\mathbf{b}_1)T(\mathbf{b}_2) = T(\mathbf{b}_1 + \mathbf{b}_2)\,, \quad T(\mathbf{0}) = e\,, \quad T^{-1}(\mathbf{b}) = T(-\mathbf{b})$$

The translations form an abelian group.

Euclidean group. An element of the Euclidean group ISO(2) is

$$g(\theta, \mathbf{b}) : \begin{bmatrix} x' \\ y' \end{bmatrix} = R \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} b_x \\ b_y \end{bmatrix}$$

One may want to understand if elements g with both compositions form a group. It holds

$$g(\theta_1, \mathbf{b}_1)g(\theta_2, \mathbf{b}_2) = g(\theta_1 + \theta_2, \mathbf{b}_1 + R(\theta_1) \cdot \mathbf{b}_2)$$

In fact, applying one element g after the other, one gets

$$R_1(R_2\mathbf{x} + \mathbf{b}_2) + \mathbf{b}_1$$

The inverse is

$$g^{-1}(\theta, \mathbf{b}) = g(-\theta, -[R(-\theta) \cdot \mathbf{b}])$$

The identity is

$$g(0, \mathbf{0}) = e$$

The Euclidean group ISO(2) is a group and it is a semi-direct product

$$\mathrm{ISO}(2) = \mathrm{SO}(2) \ltimes \mathrm{T}_2$$

Exercise. Prove that T_2 is invariant and SO(2) is not.

Reflections. Consider the reflection with respect to the x axis

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ -y \end{bmatrix}$$

One may want a reflection about an arbitrary line. If the line has an angle θ from the x axis, then the reflected point P'' forms an angle with the origin and P' of 2θ. So a reflection about an arbitrary axis is a reflection about the x axis and then a reflection:

$$I(\theta) = R(2\theta)I(0)$$

For a passive transformation one has

$$I(\theta) = I(0)R(-2\theta)$$

Since one should get the same result for both active and passive transformations then

$$R(2\theta)I(0) = I(0)R(-2\theta) \implies I^{-1}(0)R(2\theta)I(0) = R(-2\theta)$$

Since θ is arbitrary, so is $2\theta = \varphi$:

$$I^{-1}(0)R(\varphi)I(0) = R(-\varphi) = R^{-1}(\varphi)$$

Substituting this relation, one gets

$$I(\theta) = I(0)R(-2\theta) = I(0)[I^{-1}(0)R(\theta)I(0)]R(-\theta) = R(\theta)I(0)R(-\theta)$$

[r] A reflection through the origin is

$$\begin{bmatrix} x''' \\ y''' \end{bmatrix} = -I \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -x \\ -y \end{bmatrix}$$

Noting that $-I = R(\pi)$. A reflection about the y axis is

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = R(\pi)I(0)$$

Therefore

- all reflections are built from a single reflection $I(0)$ and reflections;
- it holds
$$\det[I(\theta)] = \det R \det I(0) = \det I(0) = -1$$
- it holds
$$I^2(0) = I\,, \quad I^{-1}(0) = I(0)$$
The element $I(0)$ represents a generator of $\mathbb{Z}_2$.
- the metric transforms as
$$g' = I(0)gI(0)$$
If $g = \delta$ then
$$g' = I^2(0) = I$$
The matrix $I(0)$ preservers the 2×2 metric and as such it is an element of the orthogonal group O(2).
- Elements M in the orthogonal group have $\det M = \pm 1$; this group has two disjoint sets
$$\mathrm{SO}(2) = \{M \in \mathrm{O}(2) \mid \det M = 1\}\,, \quad I(0)\mathrm{SO}(2) = \{M \in \mathrm{O}(2) \mid \det M = -1\}$$
Therefore
$$\mathrm{O}(2) \simeq \mathbb{Z}_2 \ltimes \mathrm{SO}(2)$$
Because only SO(2) is invariant.

Lecture 7

mar 24 ott 2023 08:30

6.2 Arbitrary dimensions

Definition 6.2. The set of all transformations, including reflections, of n-dimensional Euclidean space which preserve the norm of a vector is called the Euclidean group E_n. Therefore
$$\mathrm{T}_n \subset \mathrm{ISO}(n) \subset E_n\,, \quad \mathrm{SO}(n) \subset \mathrm{ISO}(n)\,, \quad \mathrm{SO}(n) \subset \mathrm{O}(n) \subset \mathrm{E}_n\,, \quad \mathrm{D}_n \subset \mathrm{O}(n)$$
The relation above can be generalized to any dimension
$$\mathrm{O}(n) \simeq \mathbb{Z}_2 \ltimes \mathrm{SO}(n)$$

The special orthogonal group is always an invariant group
$$^{\mathrm{O}(n)}/_{\mathrm{SO}(n)} \simeq \mathbb{Z}_2$$

[r] By adding translations?
$$\mathrm{E}_n \simeq \mathrm{O}(n) \ltimes \mathrm{T}_n\,, \quad ^{\mathrm{E}_n}/_{\mathrm{T}_n} \simeq \mathrm{O}(n)$$

7 Representations of groups

A presentation ρ of G is a homomorphism $\rho : G \to \mathrm{GL}(V)$, $g \mapsto \rho(g)$. One defines

- the dimension of the vector space V over a field $\mathbb{F}$ is the dimension n of the representation;
- a representation if faithful if the homomorphism is also an isomorphism, otherwise the representation is degenerate;
- given a degenerate representation, the set $^{G}/_{\mathrm{Ker}\,\rho}$ determines a faithful representation;
- it holds
$$\rho(e) = I\,, \quad \rho(g^{-1}) = \rho^{-1}(g)\,, \quad \rho(g_1)\rho(g_2) = \rho(g_1 g_2)$$

Example 7.1. A few examples:

- every group G admits a trivial representation
$$\rho(g) = I\,, \quad \forall g \in G\,, \quad V = \mathbb{C}$$
- All groups of matrices admit a one dimensional representation
$$V = \mathbb{C}\,, \quad \forall M \in G \subset \mathrm{GL}(n,\mathbb{C})\,, \quad \rho(M) = \det M$$
The representation is degenerate
$$\rho(M_1)\rho(M_2) = \rho(M_1 M_2) = \det(M_1 M_2) = \det M_1 \, \det M_2$$
- The cyclic group $\mathbb{Z}_2 = \{e, a\}$, $a^2 = e$ admits two representations with dimension two with $V = \mathbb{R}^2$:
  - ⋄ first: $\rho(e) = I$, $\rho(a) = -I$, this can be generalized to arbitrary dimensions;
  - ⋄ second: $\rho(e) = I$, $\rho(a) = \mathrm{diag}(1, -1)$.

  There does not exist a change of basis which maps one into the other.
- The dihedral group $\mathrm{D}_2 = \{e, R_x, R_y, r\}$ has two representations in two dimensions:
$$e = I\,, \quad \rho(R_x) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\,, \quad \rho(R_y) = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\,, \quad \rho(r) = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$
From the representation one can also see that $\mathbb{Z}_2 \subset \mathrm{D}_2$. The group structure is preserved.
- A one dimensional representation of
$$\mathbb{Z}_n = \{e, a, \ldots, a^{n-1}\}\,, \quad a^n = e\,, \quad \rho(a^n) = \rho^n(a) = \rho(e) = 1$$
and then
$$\rho(a) = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}\,, \quad \rho(a^k) = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n} k}\,, \quad k = 0, 1, \ldots, n-1$$
- A representation gives a way to multiply the elements $g \in G$ by a vector $\mathbf{v} \in V$. One can see the representation ρ as a map
$$\rho : G \times V \to V\,, \quad (g, \mathbf{v}) \mapsto \rho(g)\mathbf{v}$$
Therefore ρ is a module.

Definition 7.2. The representation of a group of matrices coinciding with the group itself is a fundamental representation.

Example 7.3. Two examples:

- For the special linear group $\mathrm{SO}(2)$, one can use
$$R(\theta) = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$$
The matrix R is two dimensional acting on a vector space over $\mathbb{R}$.
- Using orthogonal matrices to represent $\mathrm{O}(n)$ defines the orthogonal group's fundamental representation.

Theorem 7.4. If a group G admits an invariant subgroup H, then every representation of G/H induces a degenerate representation of G.

Example 7.5. Consider the alternating group
$$\mathrm{A}_3 = \{e, (123), (321)\}$$
it is an invariant subgroup of S_3. Therefore
$$\mathrm{S}_3/\mathrm{A}_3 \simeq \mathbb{Z}_2\,, \quad \rho(\mathbb{Z}_2) = \{1, -1\}$$
The representation ρ induces a one dimensional representation of S_3: the parity of the elements. For every element, there is an associated cycle which has an even or odd number of two-cycles.

Definition 7.6. A similarity transformation between two matrices is defined by an invertible matrix S such that

$$M_1 = S^{-1} M_2 S$$

Notice that it is one matrix for all group elements.

Definition 7.7. Two representations ρ_1 and ρ_2 of G are equivalent if and only if

$$\rho_1(G) \sim \rho_2(G) \iff \exists s \mid \forall g \in G \,, \rho_1(g) = S^{-1} \rho_2(g) S$$

Definition 7.8. The character $\chi_\rho(g)$ for an element $g \in G$ of a representation ρ is defined as

$$\chi_\rho(g) = \mathrm{Tr}[\rho(g)]$$

The character is a function of the equivalence classes, not of the representation

$$\mathrm{Tr}[\rho_1(g)] = \mathrm{Tr}\big[S^{-1}\rho_2(g)S\big] = \mathrm{Tr}\big[\rho_2(g) S S^{-1}\big] = \mathrm{Tr}[\rho_2(g)]$$

7.1 Irreducible representations

Definition 7.9. Let ρ be a representation of G on a vector space V. Let V_1 be a subspace of V such that

$$\rho(g)\,|v_1\rangle \in V_1 \,, \quad \forall\, |v_1\rangle \in V_1$$

The set V_1 is an invariant subspace of V with respect to $\rho(G)$. If V_1 does not contain any non-trivial invariant subspace, then V_1 is said to be minimal or proper.

Definition 7.10. A representation ρ of G on V is

- irreducible (irrep) if there is no invariant subspace of V,
- reducible if there is at least one invariant subspace,
- fully reducible or decomposable if the orthogonal complement

  $$V_1^\perp = \{|v\rangle \in V \mid \langle v_1|v\rangle = 0 \,, \forall\, |v_1\rangle \in V_1\}$$

  is also invariant.

Remark 7.11. One may note:

- the representation ρ is reducible if there exists a basis for all $g \in G$ such that

  $$\rho(g) = \begin{bmatrix} \rho_1(g) & \rho_2(g) \\ 0 & \rho_3(g) \end{bmatrix}$$

  the representation is block diagonal, but the subspaces are mixed.
- the representation ρ is fully reducible if there exists a basis such that

  $$\rho(g) = \begin{bmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{bmatrix}$$

  the representation is block diagonal.

Definition 7.12. The direct sum of two representations is

$$\rho = \rho_1 \oplus \rho_2 = \begin{bmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{bmatrix}$$

acting on the vector space $V = V_1 \oplus V_2$ with $\dim V = \dim V_1 + \dim V_2$.

Definition 7.13. The direct product of two representations $\rho = \rho_1 \otimes \rho_2$ is defined on the vector space $V = V_1 \otimes V_2$ with $\dim V = \dim V_1 \, \dim V_2$ and vectors

$$|v\rangle = v^{ij} \, |e_i^{(1)}\rangle \otimes |e_j^{(2)}\rangle \in V$$

for a basis $\{ |e_i^{(j)}\rangle \}$ of V_j; such that

$$\rho(g) \, |v\rangle = v^{ij} (\rho_1(g) \, |e_i^{(1)}\rangle) \otimes (\rho_2(g) \, |e_j^{(2)}\rangle) = v^{ij} \rho_1(g)]^k{}_i [\rho_2(g)]^m{}_j \, |e_k^{(1)}\rangle \otimes |e_m^{(2)}\rangle = |v'\rangle$$

In matrix notation one has

$$v' = \rho_1(g) v \rho_2(g)^\top$$

Remark 7.14. The central problem in representation theory and physics is classification. One wants to write any representation as sums or products of irreps ρ:

$$D = \bigotimes_{\nu=1}^{m} [\rho_\nu(G)]^{b_\nu} = \bigoplus_{\mu=1}^{n} a_\mu \rho_\mu(G)$$

Example 7.15. Some examples:

- Consider the cyclic group $\mathbb{Z}_2$. The trivial representation and another representation both one dimensional are

  $$\rho_0(\mathbb{Z}_2) = \{1, 1\}, \quad \rho_1(\mathbb{Z}_2) = \{1, -1\}$$

  One can build a two dimensional representation

  $$\rho_2(\mathbb{Z}_2) = \rho_0(\mathbb{Z}_2) \oplus \rho_1(\mathbb{Z}_2) = \begin{bmatrix} \rho_0(g) & 0 \\ 0 & \rho_1(g) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

  Consider the representation

  $$\widetilde{\rho}_2(\mathbb{Z}_2) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

  Letting $V = \mathbb{R}^2$, one basis is

  $$\{ |v_1\rangle, |v_2\rangle \}, \quad |v_i\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \pm 1 \end{bmatrix}$$

  and one gets

  $$\widetilde{\rho}_2(a) \, |v_1\rangle = |v_1\rangle \, , \quad \widetilde{\rho}_2(a) \, |v_2\rangle = - \, |v_2\rangle$$

  The subspaces generated by $\widetilde{\rho}_2 \, |v_i\rangle$ are separate. One can introduce a similarity matrix

  $$S = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \implies S^{-1} \widetilde{\rho}_2(a) S = \rho_2(a)$$

  So the representations $\widetilde{\rho}_2$ and ρ_2 are equivalent. The property of equivalence can be stated by other means.

Lecture 8

lun 30 ott 2023 08:30

- The matrix

  $$\begin{bmatrix} 1 & -a \\ a & 1 \end{bmatrix}, \quad a \neq 0$$

  does not admit an invariant subspace. In fact, imposing

  $$\begin{bmatrix} 1 & -a \\ a & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} x \\ y \end{bmatrix} \implies \begin{cases} x - ay = x \\ ax + y = y \end{cases} \implies x = y = 0$$

  [r] The group S_3 admit a two dimensional representation with

  $$\rho_2((123)) = -\frac{1}{2} \begin{bmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{bmatrix}$$

- The fundamental representation of SO(2)

$$R = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$$

is an irreducible representation over $V = \mathbb{R}^2$. However, consider now $V = \mathbb{C}^2$ and

$$|v_\pm\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \pm\mathrm{i} \end{bmatrix}$$

Applying the rotation matrix, one gets

$$R(\theta)\,|v_\pm\rangle = \frac{\mathrm{e}^{\pm\mathrm{i}\theta}}{\sqrt{2}} \begin{bmatrix} 1 \\ \pm\mathrm{i} \end{bmatrix} = \mathrm{e}^{\pm\mathrm{i}\theta}\,|v_\pm\rangle$$

So the vectors $|v_\pm\rangle$ define an invariant subspace. Defining a unitary transformation to be

$$S = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \mathrm{i} \\ 1 & -\mathrm{i} \end{bmatrix}, \quad S^\dagger = S^{-1}$$

one gets a similarity transformation to diagonalize the rotation matrix

$$S^{-1} R(\theta) S = \begin{bmatrix} \mathrm{e}^{-\mathrm{i}\theta} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\theta} \end{bmatrix}$$

Thus, the representation above is not an irreducible representation over $V = \mathbb{C}^2$ and is fully reducible written as a direct sum

$$\rho_2(\theta) = \rho_1(\theta) \oplus \rho_{-1}(\theta)$$

The single representations are also representations of U(1). The fundamental representation of SO(2) over $\mathbb{C}^2$ can be written as the sum of U(1) representations.

7.2 Unitary representations

Definition 7.16. A vector space is hermitian if it admits an inner product which is sesquilinear $\varphi : V \otimes V \to \mathbb{F}$, typically $\mathbb{F} = \mathbb{C}$:

- Linear in the arguments

$$\varphi(\mathbf{v}_1 + \mathbf{v}_2, \mathbf{w}) = \varphi(\mathbf{v}_1, \mathbf{w}) + \varphi(\mathbf{v}_2, \mathbf{w}), \quad \varphi(\mathbf{v}, \mathbf{w}_1 + \mathbf{w}_2) = \cdots$$

- It holds

$$\varphi(\mathbf{v}, \lambda\mathbf{w}) = \lambda\varphi(\mathbf{v}, \mathbf{w})$$

- then [r]

$$\varphi(\mathbf{v}, \mathbf{w}) = [\varphi(\mathbf{w}, \mathbf{v})]^*$$

- it holds

$$\varphi(\mathbf{v}, \mathbf{v}) \geq 0, \quad \varphi(\mathbf{v}, \mathbf{v}) = 0 \iff \mathbf{v} = \mathbf{0}$$

Definition 7.17. If the operators $\rho(g)$ of a representation of a group G over a hermitian vector space are unitary

$$[\rho(g)]^{-1} = \rho(g^{-1}) = [\rho(g)]^\dagger, \quad \forall g \in G$$

then the representation is called unitary. That is, the representation ρ is unitary if $\rho(g)$ is a unitary matrix.

Theorem 7.18. Any representation of a finite group on a hermitian vector space V is equivalent to a unitary representation.

Proof. Since the vector space is hermitian one can build the conjugate representation $\rho^\dagger(g)$and construct

$$M = \sum_{g\in G} \rho^\dagger(g)\rho(g)$$

but ρ is not unitary. Therefore

$$\rho^\dagger(g)M\rho(g) = \rho^\dagger(g)\sum_{g'}\rho^\dagger(g')\rho(g')\rho(g) = \sum_{g'}\rho^\dagger(g'g)\rho(g'g) = \sum_{g''}\rho^\dagger(g'')\rho(g'') = M$$

Since $M = M^\dagger$ is hermitian then it is diagonalizable

$$M = U^\dagger \Lambda U\,, \quad \Lambda = \mathrm{diag}(\Lambda_1, \ldots, \Lambda_n)$$

The matrix M is positive definite:

$$\big\langle v^\dagger M \big| v\big\rangle = \langle v^\dagger \sum_g \rho^\dagger(g)\rho(g)|v\rangle = \sum_g \|\rho(g)\,|v\rangle\|^2 \geq \|\rho(e)\,|v\rangle\|^2 = \||v\rangle\|^2 > 0$$

Therefore its eigenvalues are real and positive. Taking the squaring root of the eigenvalues then multiply by $U^\dagger U$ one gets the square root of the matrix

$$\sqrt{M} = U^\dagger\sqrt{\Lambda}U\,, \quad \sqrt{M}\sqrt{M} = M\,, \quad \sqrt{M} = (\sqrt{M})^\dagger$$

Starting from the beginning expression of M one multiplies by $M^{-\frac{1}{2}}$:

$$M = \rho^\dagger(g)M\rho(g) = [M^{-\frac{1}{2}}\rho^\dagger(g)M^{\frac{1}{2}}][M^{\frac{1}{2}}\rho(g)M^{-\frac{1}{2}}] = I$$

Therefore, the matrix

$$M^{\frac{1}{2}}\rho(g)M^{-\frac{1}{2}}$$

is unitary. □

Theorem 7.19. If the representation ρ is reducible and unitary, then it is fully reducible.

Proof. Consider an invariant subspace V_1 and its orthogonal complement $V_1^\perp$. One needs to prove that the orthogonal complement is an invariant subspace:

$$\rho(g)\,|v\rangle \in V_1\,, \quad \rho(g^{-1})\,|v\rangle \in V_1\,, \quad |v\rangle \in V_1$$

Then, using $w \in V_1^\perp$, one gets

$$\langle w|\,\rho^\dagger(g)\,|v\rangle = \langle w|\,\rho^{-1}(g)\,|v_1\rangle = \langle w|\,\rho(g^{-1})\,|v_1\rangle = 0 \implies \rho(g)\,|w\rangle \in V_1^\perp$$

So the orthogonal complement is invariant. The representation ρ is thus fully reducible. □

Corollary 7.20 (both theorems)**.** All reducible representations of finite groups are fully reducible.

Lemma 7.21 (Schur's I)**.** Let ρ be an irreducible representation of a group G on a vector space V, and A an operator on V. If A commutes with all operators

$$A\rho(g) = \rho(g)A\,, \quad \forall g \in G$$

then $A = \lambda I$.

Proof. With no loss of generality, consider A to be a hermitian operator since one can always have

$$A_\pm = \frac{A \pm A^\dagger}{2}$$

Consider an orthonormal basis formed by the eigenvectors of A

$$A\,|u_{i,\alpha}\rangle = \lambda_i\,|u_{i,\alpha}\rangle$$

where α is the index of degeneracy of an eigenvalue. Applying the hypothesis:

$$A\rho(g)\left|u_{i,\alpha}\right\rangle = \rho(g)A\left|u_{i,\alpha}\right\rangle = \rho(g)\lambda_i\left|u_{i,\alpha}\right\rangle$$

so the vector $\rho(g)\left|u_{i,\alpha}\right\rangle$ is also an eigenvector of A, so at most ρ changes α. Defining the subspace

$$V_i = \{|u_{i,\alpha}\rangle\}$$

then

$$\rho(g)\left|u_{i,\alpha}\right\rangle \in V_i$$

so the vector space V_i is an invariant subspace. However, if ρ is an irreducible representation, then it does not admit an invariant (proper) subspace: there is only one subspace, the trivial one $V_i = V$. This means that A has only one eigenvalue

$$A = \lambda I$$

□

Lemma 7.22 (Schur's II)**.** Let ρ and ρ' be two irreducible representation of a group G on the vector space V and V'. Let $A : V \to V'$ be a linear operator satisfying

$$A\rho'(g) = \rho(g)A\,, \quad g \in G$$

It follows either $A = 0$, or $V = V'$ (so A is an isomorphism) and $\rho \sim \rho'$.

Proof. The image (or range) of A in V' is

$$\operatorname{im} A = \{|x'\rangle \in V' \mid |x'\rangle = A\left|x\right\rangle\,, \quad |x\rangle \in V\}$$

It holds

$$\forall g \in G\,, \rho'(g)\left|x'\right\rangle = \rho'(g)A\left|x'\right\rangle = A\rho(g)\left|x\right\rangle \in \operatorname{im} A$$

So the image is an invariant subspace of V' with respect to $\rho'(g)$. But ρ' is an irreducible representation, therefore either $\operatorname{im} A = 0$ implies $A = 0$, or $\operatorname{im} A = V$ so A maps on the entire V'.

One can apply the same reasoning on the kernel

$$\operatorname{Ker} A = \{|x\rangle \in V \mid A\left|x\right\rangle = |0\rangle \in V'\}$$

Considering $|x\rangle \in \operatorname{Ker} A$, then

$$A\rho(g)\left|x\right\rangle = \rho'(g)A\left|x\right\rangle = \rho'(g)\left|0\right\rangle = |0\rangle \implies \rho(g)\left|x\right\rangle \in \operatorname{Ker} A$$

Therefore, the kernel is an invariant subspace of V with respect to ρ. But ρ is an irrep so ether $\operatorname{Ker} A = V$ implies $A = 0$, or $\operatorname{Ker} A = 0$ implies

$$A\left|x'\right\rangle = A\left|y'\right\rangle \implies |x'\rangle = |y'\rangle$$

This last case, combined with the last above, the map A is a bijective map. Therefore it is invertible and is an isomorphism

$$V = V'\,, \quad \dim V = \dim V'$$

Since A is invertible, then the two representation are equivalent

$$A\rho' = \rho A \implies \rho' = A^{-1}\rho A \implies \rho' \sim \rho$$

□

Notation. The labels of irreps are μ, ν. The dimension of irrep μ is d_μ. The character χ_i^μ has the index i that labels equivalence classes. The number of equivalence classes is n_c. The number of elements in an equivalence class is n_i.

Theorem 7.23 (A)**.** Irreducible representations are orthonormal to each other, valid only for finite groups:

$$\frac{d_\mu}{|G|}\sum_{g\in G}[\rho_\mu^\dagger(g)]^i{}_j[\rho_\nu(g)]^k{}_l = \delta_{\mu\nu}\delta^i_l\delta^k_j$$

The reason it describes orthonormality can be seen by the following

$$\langle g|u,i,j\rangle = \sqrt{\frac{d_\mu}{|G|}}[\rho_\mu(g)]^i{}_j \implies \sum_g \langle u,i,j|g\rangle\langle g|\nu,k,l\rangle = \delta_{\mu\nu}\delta^i_l\delta^k_j$$

Proof. Consider two irreps ρ_μ and ρ_ν with dimensions d_μ and d_ν. Let X be a $d_\mu \times d_\nu$ matrix

$$M_x = \sum_g \rho_\mu^\dagger(g) X \rho_\nu(g)$$

From the rearrangement lemma

$$\rho_\mu^{-1}(g)M_x\rho_\nu(g) = M_x\,, \quad \forall g\in G$$

Considering

$$M_x\rho_\nu(g) = \rho_\mu(g)M_x\,, \quad \forall g\in G$$

from the second Schur's lemma one has either $\mu\neq\nu$ and $M_x = 0$, or $\mu=\nu$ and $M_x = \lambda I$ (from the first Schur's lemma). This is the first step towards $\delta_{\mu\nu}$.

Consider the following matrices X^k_l indexed by k,l

$$[X^k_l]^i{}_j = \delta^k{}_j\delta^i{}_l$$

Therefore

$$[M^k_l]^m{}_n = \sum_g [\rho_\mu^\dagger(g)]^m{}_i[X^k_l]^i{}_j[\rho_\mu(g)]^j{}_n = \sum_g[\rho_\mu^\dagger(g)]^m{}_l[\rho_\mu(g)]^k{}_n = [\lambda^k_l]I_{d_\mu}$$

Taking the trace one gets

$$\mathrm{Tr}\big[M^k_l\big] = \sum_g[\rho_\mu^\dagger(g)]^m{}_l[\rho_\mu(g)]^k{}_m = \sum_g[\rho_\mu(g)\rho^\dagger_{mu}]^k{}_l = \sum_g I^k{}_l = |G|\delta^k_l \equiv \lambda^k_l d_\mu \implies \lambda^k_l = \frac{|G|}{d_\mu}\delta^k_l$$

from which the thesis follows. □

Example 7.24. Consider the cyclic group $\mathbb{Z}_2 = \{e,a\}$. One wants to construct all possible irreps using the theorem above. Starting from an irrep, one can build perpendicular irreps so independent. Starting from the trivial irrep

$$\rho(e) = \rho(a) = 1$$

One can write it as a vector $(1,1)$ which has only one orthogonal vector $(1,-1)$. So the cyclic group $\mathbb{Z}_2$ admits only two irreps.

Remark 7.25. Abelian groups have all irreps with dimension $d=1$. The theorem above is then

$$\frac{1}{|G|}\sum_g \rho_\mu^\dagger(g)\rho_\mu(g) = \delta_{\mu\nu}$$

Corollary 7.26. The number of inequivalent irreps of a finite group is

$$\sum_\mu d_\mu^2 \leq |G|$$

where the sum over μ is the sum over the irreps.

Proof. Consider the vector notation $\langle g|u,i,j\rangle$ which means the g-th component of the vector $|\mu,i,j\rangle$. This vector has two indices, so it is a matrix and as such has d_μ^2 components. The number of linearly independent vectors lass than $\dim V$ is $|G|$. □

Lecture 9

mar 31 ott 2023 08:30

Theorem 7.27 (B)**.** Irreducible representations are complete. It holds

$$\sum_\mu d_\mu^2 = |G|\,, \quad \frac{1}{|G|}\sum_\mu d_\mu \sum_{i,j=1}^{d_\mu} [\rho_\mu(g_1)]^i{}_j [\rho_\mu^\dagger(g_2)]^j{}_i = \delta_{g_1 g_2}$$

The argument of the second relation is the trace of $\rho\rho^\dagger$. The proof of the first relation can be found in the proof of Theorem 7.37.

Proposition 7.28 (Properties of characters)**.** A few properties of characters:

- the character χ labels equivalence classes of irreps; in fact, two irreps are equivalent $\rho \sim \rho'$ if it exists a matrix S such that $\rho' = S^{-1}\rho S$, therefore

$$\chi_{\rho'}(g) = \mathrm{Tr}[\rho'(g)] = \mathrm{Tr}\big[S^{-1}\rho(g)S\big] = \chi_\rho(g)$$

- The character χ also depends on conjugacy classes; two elements are conjugate if

$$g \sim g' \iff hgh^{-1} = g'\,, \quad \forall h$$

then

$$\chi_\rho(g') = \mathrm{Tr}[\rho(g')] = \mathrm{Tr}\big[\rho(h)\rho(g)\rho(h^{-1})\big] = \mathrm{Tr}\big[\rho(h)\rho(g)\rho(h)^{-1}\big] = \chi_\rho(g)$$

- One defines

$$\chi_\mu(g) = \chi_\mu^i = \mathrm{Tr}[\rho_\mu(g)]\,, \quad g \in \zeta_i$$

where ζ_i is a conjugacy class.

- The character of the identity is

$$\chi_\rho(e) = \mathrm{Tr}[\rho(e)] = \dim\rho = \dim V$$

For an irrep one has $\chi_\mu(e) = d_\mu$.

Theorem 7.29 (C.1)**.** The characters of irreducible representations are orthonormal

$$\frac{1}{|G|}\sum_{i=1}^{n_c} (\chi_\mu^i)^* \chi_\nu^i n_i = \delta_{\mu\nu}$$

Proof. Consider Theorem 7.23

$$\frac{d_\mu}{|G|}\sum_g [\rho_\mu^\dagger(g)]^k{}_i [\rho_\nu(g)]^j{}_l = \delta_{\mu\nu}\delta_l^k\delta_i^j$$

Setting $i = k$ and $j = l$ then

$$\frac{1}{|G|}\sum_g \chi_\mu^*(g)\chi_\nu(G) = \delta_{\mu\nu}$$

The sum can be decomposed in a sum over classes

$$\sum_g = \sum_i \sum_{h\in\zeta_i}$$

where ζ_i is a class. However, the character χ is invariant of classes so

$$\sum_g = \sum_{i=1}^{n_c}\sum_{h\in\zeta_i} \implies \sum_g = \sum_{i=1}^{n_c} n_i$$

therefore the thesis. □

Lemma 7.30. It holds

$$\sum_{h\in\zeta_i}\rho_\mu(h)=\frac{n_i}{d_\mu}\chi^i_\mu I_{d_\mu}$$

Proof. Defining

$$A\equiv\sum_{h\in\zeta_i}\rho_\mu(h)$$

it follows

$$\rho_\mu(g)A\rho^{-1}_\mu(g)=\sum_{h\in\zeta_i}\rho_\mu(ghg^{-1})=A$$

From the first Schur's lemma one has $A=\lambda I$ and its trace is

$$\operatorname{Tr}A=\sum_{h\in\zeta_i}\operatorname{Tr}[\rho_\mu(h)]=\sum_h\chi^i_\mu=n_i\chi^i_\mu=\lambda\operatorname{Tr}I=\lambda d_\mu\implies\lambda=\frac{n_i}{d_\mu}\chi^i_\mu$$

from which follows the thesis. □

Theorem 7.31 (C.2)**.** The characters obey a completeness relation

$$\frac{n_i}{|G|}\sum_\mu\chi^i_\mu(\chi^j_\mu)^*=\delta^{ij}$$

Proof. Consider the second thesis of Theorem 7.27

$$\delta_{g_1g_2}=\frac{1}{|G|}\sum_\mu d_\mu\sum_{kl}[\rho(g_1)]^k{}_l[\rho^\dagger_\mu(g_2)]^l{}_k$$

Summing over all elements g_1, g_2 in two classes, one gets

$$\begin{aligned}n_i\delta^{ij}&=\frac{1}{|G|}\sum_\mu d_\mu\sum_{kl}\left[\sum_{g_1\in\zeta_i}[\rho(g_1)]^k{}_l\right]\left[\sum_{g_2\in\zeta_j}[\rho(g_2)]^l{}_k\right]\\&=\frac{1}{|G|}\sum_\mu d_\mu\sum_{kl}\left(\frac{n_i}{d_\mu}\chi^i_\mu\delta^k_l\right)\left(\frac{n_j}{d_\mu}(\chi^j_\mu)^*\delta^l_k\right)\\&=\frac{1}{|G|}\sum_\mu\sum_{kl}(n_i\chi^i_\mu\delta^k_l)\left(\frac{n_j}{d_\mu}(\chi^j_\mu)^*\delta^l_k\right)\\&=\frac{1}{|G|}\sum_\mu\frac{n_in_j}{d_\mu}(\chi^i_\mu)(\chi^j_\mu)^*d_\mu\end{aligned}$$

from which the thesis

$$\frac{1}{|G|}=\sum_\mu n_j(\chi^i_\mu)(\chi^j_\mu)^*=\delta^{ij}$$

□

Corollary 7.32. The number of inequivalent irreducible representations for any finite group is equal to the number n_c of conjugacy classes. The characters χ^i_μ can be put in an $n_c\times n_c$ matrix called character table. Sometimes they are normalized as

$$\chi^i_\mu\to\sqrt{\frac{n_i}{|G|}}\chi^i_\mu$$

Theorem 7.33. One can reduce a generic representation into irreducible representations

$$\rho(G)=\bigoplus_{\mu=1}^{n_c}a_\mu\rho_\mu(G)$$

then the number a_μ of times an irreducible representation ρ_μ occurs is

$$a_\mu=\sum_i\frac{(\chi^i_\mu)^*\chi^in_i}{|G|}$$

Proof. A generic representation for a finite group is similar to a unitary representation which is fully reducible, therefore it can be written as a direct sum. Since the number of irreducible representations is the number of conjugacy class, the sum runs from 1 to n_c.

Defining

$$\chi_i = \mathrm{Tr}[\rho(G)] = \sum_\mu a_\mu \chi^i_\mu$$

and using Theorem 7.29

$$\frac{1}{|G|}\sum_i n_i(\chi^i_\mu)^* \chi^i = \frac{1}{|G|}\sum_{i\nu} n_i(\chi^i_\mu)^* a_\nu \chi^i_\nu = \sum_\nu a_\nu \delta_{\mu\nu} = a_\nu$$

□

Theorem 7.34 (Irreducibility condition)**.** A necessary and sufficient condition for a representation ρ with characters χ_i to be irreducible is

$$\sum_{i=1}^{n_c} n_i |\chi_i|^2 = |G|$$

Proof. Using Theorem 7.29

$$\sum_i \frac{n_i}{|G|}(\chi^i)^* \chi^i = \sum_i \frac{n_i}{|G|}\sum_{\mu\nu} a_\mu (\chi^i_\mu)^* a_\nu \chi^i_\nu = \sum_\mu |a_\mu|^2$$

If ρ is an irreducible representation, then for one μ one has $a_\mu = 1$, while for all others $a_\mu = 0$. Conversely, if

$$\sum_i \frac{n_i}{|G|}|\chi_i|^2 = 1$$

then

$$\sum_\mu |a_\mu|^2 = 1$$

Since $a_\mu \in \mathbb{N}_0$, this is possible only if $a_\mu = 1$ for one μ and $a_\mu = 0$ for all others. □

7.3 Regular representations

Theorem 7.35. Every finite group admits a representation with $|G| \times |G|$ matrices called regular representation. For all $g_i, g_j \in G$ it holds

$$g_i g_j = g_k = g_m [\rho^{\mathrm{R}}(g_i)]^m{}_j$$

where

$$[\rho^{\mathrm{R}}(g_i)]^m{}_j = \begin{cases} 1\,, & m = k \\ 0\,, & m \neq k \end{cases}, \quad i,j,m = 1,2,\ldots,|G|$$

Remark 7.36. One may notice:

- The matrices ρ^{R} have one 1 and all zeros in each row. Consider the cyclic group $\mathbb{Z}_3 = \{e, a, a^2\}$. The relations between the elements can be written as a linear system of equations

$$\begin{cases} ea = a \\ ea^2 = a^2 \\ ee = e \end{cases} \implies X \begin{bmatrix} e \\ a \\ a^2 \end{bmatrix} = \begin{bmatrix} e \\ a \\ a^2 \end{bmatrix} \implies X = \rho^{\mathrm{R}}(e) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

  Consider now the relations with a:

$$X \begin{bmatrix} e \\ a \\ a^2 \end{bmatrix} = \begin{bmatrix} a \\ a^2 \\ e \end{bmatrix} \implies X = \rho^{\mathrm{R}}(a) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

  Note that $\rho^{\mathrm{R}}(a)$ permutes the elements.

- The matrices ρ^{R} are representations of $\mathrm{S}_{|G|}$ group elements. This is again Cayley's theorem.
- Since the matrices are permutations then

$$\mathrm{Tr}\big[\rho^{\mathrm{R}}(e)\big] = |G|\,, \quad \mathrm{Tr}\big[\rho^{\mathrm{R}}(g)\big] = 0\,, \quad g \neq e$$

Theorem 7.37. The regular representation contains every inequivalent irreducible representation d_μ times

$$\rho^{\mathrm{R}}(G) = \bigoplus_{\mu=1}^{n_c} d_\mu \rho_\mu(G)\,, \quad \sum_\mu d_\mu^2 = |G|$$

Proof. Using Theorem 7.33, since any representation can be written as sum of irreducible representations it holds

$$\rho^{\mathrm{R}}(G) = \bigoplus_{\mu=1}^{n_c} a_\mu \rho_\mu(G)\,, \quad a_\mu = \sum_i \frac{(\chi^i_\mu)^* \chi^i n_i}{|G|}\,, \quad \chi_i = \mathrm{Tr}\big[\rho^{\mathrm{R}}(G)\big]$$

Using the last property above one gets

$$\chi^i = \mathrm{Tr}\big[\rho^{\mathrm{R}}(G)\big] = \mathrm{Tr}\big[\rho^{\mathrm{R}}(e)\big] = \chi^0 = |G|$$

therefore

$$a_\mu = \frac{(\chi^0_\mu)^* \chi^0 n_0}{|G|} = (\chi^0_\mu)^* n_0 = (\chi^0_\mu)^* = \mathrm{Tr}[\rho_\mu(e)] = \mathrm{Tr}\big[I_{d_\mu}\big] = d_\mu$$

in the third equality one considers that the conjugacy class of the identity has only one element and that is the identity

$$geg^{-1} = e\,, \quad \forall g$$

so $n_0 = 1$. So every irreducible representation appears always d_μ times.

The second statement follows from

$$\mathrm{Tr}\big[\rho^{\mathrm{R}}(e)\big] = \sum_\mu d_\mu \,\mathrm{Tr}[\rho_\mu(e)] = \sum_\mu d_\mu^2 = |G|$$

the first equality is a consequence of the first thesis of the theorem. □

Lecture 10

lun 06 nov 2023 08:30

Example 7.38. One would like to construct all irreducible representations. The symmetric group S_3 has order $3! = 6$. One can count the irreducible representations. The trivial one always exists, $d = 1$ and $\rho_0 : G \to 1$. Knowing that abelian groups have only representations of dimension one, since S_3 is not abelian, it must have a representation with dimension greater than one.

The number of irreducible representations is equal to the number of conjugacy classes χ^i_μ. The symmetric group has a subgroup $\mathrm{A}_3 = \{e, (123), (132)\} \simeq \mathbb{Z}_3$ which is invariant: the effect of conjugation keeps all elements in the group [r]. The equivalence classes are

$$\{e\}\,, \quad \{(12), (13), (23)\}\,, \quad \{(123), (321)\}$$

One looks for the next irreducible representations ρ_1. Knowing that the quotient ${}^{\mathrm{S}_3}/_{\mathrm{A}_3} \simeq \mathbb{Z}_2$ induces a representation of the entire group, one gets the parity $\sigma(p) = \pm 1$, $p \in \mathrm{S}_3$.

The last irreducible representation can be built from orthogonality. Looking at the character table

	1	2	3
0	1	1	1
1	1	−1	1
2	2	0	−1

where the last row has been constructed considering the entries as vectors and finding the vector perpendicular to both first and second vector. In fact, one has seen that

$$\rho_2(a) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho_2(r) = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}, \quad \rho_2(\sigma) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

for r and σ in D_3, but $\mathrm{S}_3 \simeq \mathrm{D}_3$.

One can build the regular representation of the symmetric group S_3:

$$\rho^{\mathrm{R}}(\mathrm{S}_3) = \rho_0(\mathrm{S}_3) \oplus \rho_1(\mathrm{S}_3) \oplus 2\rho_2(\mathrm{S}_3)$$

Example 7.39. Consider the dihedral group D_2 with order $|\mathrm{D}_2| = 4$. Knowing the trivial representation to exist and that the group is abelian, it must have four irreducible representations of dimension one. The strategy is to find invariant subgroups, consider the quotient and induce the representations.

The subgroup $\{e, r, \sigma_1, \sigma_2\}$ is an invariant and has a subgroup $\mathbb{Z}_2 \simeq \{e, r\}$. The quotient is isomorphic to another $\mathbb{Z}_2$

$$\rho_1(e) = 1\,, \quad \rho_1(r) = 1\,, \quad \rho_1(\sigma_1) = -1\,, \quad \rho_1(\sigma_2) = -1$$

The group has another subgroup $\{e, \sigma_1\} \simeq \mathbb{Z}_2$ whose quotient is another $\mathbb{Z}_2$. One can then build

$$\rho_2 \begin{pmatrix} e \\ r \\ \sigma_1 \\ \sigma_2 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$$

The character table is then

	e	r	σ_1	σ_2
0	1	1	1	1
1	1	1	−1	−1
2	1	−1	1	−1
3	1	−1	−1	1

[r] One has four conjugacy classes $\{e\}$, $\{r\}$, $\{\sigma_1\}$ and $\{\sigma_2\}$. In fact, one can note that $ghg^{-1} = h$ therefore every element is its own conjugacy class.

Example 7.40. Consider the cyclic group $\mathbb{Z}_n$. It is abelian, so one expects n one-dimensional irreps. Previously, a representation has been constructed as

$$\rho_1(a^k) = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}k} \implies \rho_\mu(a^k) = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}\mu k}\,, \quad \mu, k = 0, \dots, n-1$$

7.4 Representations of the symmetric group

The cycle decomposition is invariant under conjugation. This means that the classes are given by cycle structures.

Suppose to have ν_n n-cycles for $n \in \mathbb{N}$, then for each class of S_n, one has

$$n = \sum_{k=1}^{n} k\nu_k$$

[r]

Definition 7.41. A Young tableau of order k is a way of stacking k squares in columns ordered such that the $(i+1)$-th column is not longer than the i-th. [r] for S_4 remember that $2, 1, 1$ exists.

Theorem 7.42. The number of Young tableau is equal to the number of classes, which itself is equal to the number of irreps.

Example 7.43. The cyclic group appears in physics as a parity symmetry:

$$\mathcal{L} = \partial_\mu \phi \, \partial^\mu \phi + m\phi^2 + \lambda \phi^4 \,, \quad \phi \to -\phi$$

For a vector field, one has instead

$$m\phi^\top \phi \implies \phi \to \rho(g)\phi \implies \rho(g) \in \mathrm{O}(n)$$

[r] In quantum field theory, the tame divergences, one discretizes space-time into a lattice: the continuous symmetries become finite group symmetries.

8 Continuous groups

Definition 8.1. A topological space is a set X where a topology is defined, which is a set U of subsets $U_i \subseteq X$ such that

- the empty set and X belong both to U,
- every union of U_i is a subset of U,
- every intersection of U_i is a subset of U.

Definition 8.2. The subsets U_i are called open neighbourhoods.

Remark 8.3. A topological space is the most general structure where continuity is defined.

Definition 8.4. A topological space has a Hausdorff topology if all pairs of elements $(x, y) \in X$ admit a disjoint neighbourhood. [r] disjoint?

Definition 8.5. A homeomorphism ϕ between two topological spaces A and B with Hausdorff topology is a continuous bijective (therefore invertible) map, with the inverse ϕ^{-1} also continuous. The spaces A and B are said to be homeomorphic.

Definition 8.6. A manifold M of dimension $N = \dim M$ is a space locally homeomorphic to $\mathbb{R}^n$: for every point $p \in M$ there exists an open neighbourhood U_p homeomorphic to an open neighbourhood of $\mathbb{R}^n$.

Definition 8.7. A chart (U, φ) is an open set $U \subseteq M$ with $\varphi : U \to V \subseteq \mathbb{R}^n$, $x \mapsto \{x^i\}$ an homeomorphism, where x^i are the coordinates on the chart.

Definition 8.8. An atlas is a set of charts $\{(U_\alpha, \varphi_\alpha\}$ such that

- the union of all charts is $\bigcup_\alpha U_\alpha = M$,
- the transition functions $f_{\beta\alpha} = \varphi_\beta \circ \varphi_\alpha^{-1}$ are differentiable C^k, then the atlas is C^k.

Remark 8.9. The transition functions are functions $f_{\beta\alpha} : \mathbb{R}^n \to \mathbb{R}^n$ so the notion of derivative is well-defined. In an intersection $U_\alpha \cap U_\beta$ there are two charts, so two coordinate systems x and y. A change of coordinates is given by

$$y^i(p) = \varphi_\beta \circ \varphi_\alpha^{-1}(x^i(p)) = \varphi_\beta(\varphi_\alpha^{-1}(x^i(p))) = f_{\beta\alpha}(x^i(p))$$

Definition 8.10. A smooth manifold is a manifold M with an atlas C^p (typically C^∞).

Example 8.11. Consider the two-sphere S^2 embedded in $\mathbb{R}^3$: $x^2 + y^2 + z^2 = 1$. One can have two charts

$$U_\mathrm{S} = S^2 - (0, 0, 1) \,, \quad U_\mathrm{N} = S^2 - (0, 0, -1)$$

which are the sphere without one of the poles, with the homeomorphism $\varphi_{\mathrm{S,N}}$ a stereographic projection. The stereographic projection is singular at the poles, so one must remove one of them. The dimension of the manifold is 2 because

$$\varphi_\mathrm{S} : U_\mathrm{S} \to \mathbb{R}^2 \,, \quad \varphi_\mathrm{S} = \begin{cases} \frac{x}{1-z} \\ \frac{y}{1-z} \end{cases}$$

so a point $p \in S^2$ is given by the embedding (x, y, z) in $\mathbb{R}^3$. There is only one transition function $f_\mathrm{SN} = \varphi_\mathrm{S} \circ \varphi_\mathrm{N}^{-1}$ and it is C^∞, so one has a smooth manifold.

Definition 8.12. A scalar function $g : M \to \mathbb{R}$ is smooth, C^∞, if given a chart (U, φ) then $g \circ \varphi^{-1}$ is also smooth C^∞. This definition considers just one point.

Remark 8.13. The homeomorphism is $\varphi^{-1} : \mathbb{R}^n \to M$ and the function is $g : M \to \mathbb{R}$ therefore one has a notion of derivative through $f \circ \varphi^{-1} : \mathbb{R}^n \to \mathbb{R}$.

[r]

Definition 8.14. Consider two smooth manifolds M_1 and M_2. A map $g : M_1 \to M_2$ smooth C^∞ at $p \in M_1$ if for a chart $(U, \varphi) \in M_1$ nd $(V, \psi) \in M_2$ then $\psi \circ g \circ \varphi^{-1}$ is smooth C^∞. If g is bijective (therefore invertible) and g, g^{-1} are smooth C^∞ everywhere, then g is a diffeomorphism.

Definition 8.15. A Lie group G is a smooth manifold C^∞ with composition $\varphi : G \times G \to G$ of class C^∞ and smooth inverse such that it holds

- closure $\forall x, y \in G$, $\exists! z \in G \mid z = \varphi(x, y)$,
- associativity $\forall x, y, z \in G$, $\varphi(x, \varphi(y, z)) = \varphi(\varphi(x, y), z)$,
- identity $\exists e \in G$, $\forall x \in G$ such that $\varphi(e, x) = \varphi(x, e) = x$,
- inverse $\forall x \in G$, $\exists x^{-1} \in G$ such that $\varphi(x, x^{-1}) = \varphi(x^{-1}, x) = e$.

Example 8.16. Examples of Lie groups already known are

$$\begin{aligned}
&\mathrm{GL}(n, \mathbb{R}) \,, \quad \dim[\mathrm{GL}(n, \mathbb{R})] = n^2 \\
&\mathrm{SL}(n, \mathbb{R}) \,, \quad \dim[\mathrm{SL}(n, \mathbb{R})] = n^2 - 1 \\
&\mathrm{O}(n) \,, \quad \dim \mathrm{O}(n) = \frac{n(n+1)}{2} \\
&\mathrm{SO}(n) \,, \quad \dim \mathrm{SO}(n) = \frac{n(n-1)}{2}
\end{aligned}$$

Lecture 11

mar 07 nov 2023 08:30

Definition 8.17. The center of a group is a subgroup of all commuting elements

$$Z(G) = \{a \in G \mid g^{-1} a g = a \,, \forall g \in G\}$$

It is an invariant abelian subgroup of G, so it admins a quotient ${}^{G}/_{Z(G)} \simeq H$.

Remark 8.18. Matrices that commute with unitary matrices are of the form cI.

Example 8.19. One can study the center of the unitary group $\mathrm{U}(n)$ for which $M^\dagger = M^{-1}$. Let $M = cI$, then

$$M^\dagger M = I \implies \det\left(M^\dagger M\right) = c^* c = |c|^2 = 1 \implies c = \mathrm{e}^{i\theta}$$

therefore, the center and the quotient group are

$$Z(\mathrm{U}(n)) = \mathrm{U}(1) \,, \quad {}^{\mathrm{U}(n)}/_{\mathrm{U}(1)} \simeq \mathrm{SU}(n)$$

Example 8.20. Consider $\mathrm{SU}(n)$ and take $M = cI$ since it is a subgroup of the above. Therefore

$$1 = \det M = c^n \,, \quad |c|^2 = 1 \implies c = \mathrm{e}^{\frac{2\pi \mathrm{i} k}{n}}$$

The center and the quotient are

$$Z(\mathrm{SU}(n)) = \mathbb{Z}_n \,, \quad {}^{\mathrm{SU}(n)}/_{\mathbb{Z}_n} \otimes \mathrm{U}(1) \simeq \mathrm{U}(n)$$

Definition 8.21. A curve γ passing through a point p is a smooth function

$$\gamma : I \to M \,, \quad t \mapsto \gamma(t)$$

where $\gamma(0) = p$, $I = [0, 1] \subset \mathbb{R}$ and M is manifold.

Remark 8.22. Considering a scalar function $g : M \to \mathbb{R}$, one can define the derivative of g along a curve γ. One evaluates g over γ

$$g_\gamma : I \subset \mathbb{R} \to \mathbb{R}\,, \quad t \mapsto g \circ \gamma(t) = g(\gamma(t))$$

Taking a chart $(U_\alpha, \varphi_\alpha) \in M$, one assigns the coordinates such that

$$x^\mu_\alpha(t) = \varphi_\alpha(\gamma(t))$$

and one has

$$g \circ \varphi_\alpha^{-1} \circ \varphi_\alpha \circ \gamma(t) = g(\gamma(t))$$

Definition 8.23. Given a curve γ passing through a point p, and a scalar function g, the tangent vecotr $t_p^{(\alpha)}$ in the chart $(U_\alpha, \varphi_\alpha)$ is

$$\mathrm{d}_t g_\gamma(t)\big|_{t=0} = \partial_{x^\mu_\alpha} g\, \mathrm{d}_t x^\mu_\alpha\big|_{t=0} = \partial_{x^\mu_\alpha} g\, b^\mu_\alpha \equiv t_p^{(\alpha)} g$$

Definition 8.24. Consider the space of curves γ passing through a point p

$$\Gamma_p = \{\gamma : \mathbb{R} \to M \mid \gamma(0) = p\}$$

Two curves are equivalent if the tangent vectors coincide for a given chart $(U_\alpha, \varphi_\alpha)$ to which p belongs:

$$\mathrm{d}_t(\varphi_\alpha \circ \gamma_1)\big|_{t=0} = \mathrm{d}_t(\varphi_\alpha \circ \gamma_2)\big|_{t=0} \implies \gamma_1 \sim \gamma_2$$

The equivalence class

$$T_pM = \{\gamma_1, \gamma_2 \in \Gamma_p \mid \gamma_1 \sim \gamma_2\}$$

is called tangent space. It is a vector space with dimension $\dim M = n$. [r]

Remark 8.25. The tangent vector $t_p^{(\alpha)}$ is a map from the algebra of smooth functions at p into itself

$$t_p^{(\alpha)} : C^\infty(U^\alpha) \to C^\infty(U^\alpha)\,, \quad g_\gamma \mapsto t_p^{(\alpha)} g_\gamma$$

Definition 8.26. A vector field v over a manifold M is a linear operator from the space of smooth functions $C^\infty(M)$ into itself, such that on each chart $(U_\alpha, \varphi_\alpha)$ is a directional derivative

$$v = b^\mu_\alpha = \partial_{x^\mu_\alpha}$$

Remark 8.27. A change of coordinates, that is a change of charts

$$(U_\alpha, \varphi_\alpha) \to (U_\beta, \varphi_\beta)\,, \quad p \in U_\alpha \cap U_\beta$$

is given by

$$\mathrm{d}_t g_\gamma(0) = \partial_{x^\mu_\alpha} g\, \mathrm{d}_t x^\mu_\alpha(0) = \partial_{x^\mu_\beta} g\, \mathrm{d}_t x^\mu_\beta(0)$$

and one can rewrite

$$b^\mu_\alpha = \mathrm{d}_t x^\mu_\alpha(0) = \partial_{x^\nu_\beta} x^\mu_\alpha\, \mathrm{d}_t x^\nu_\beta(0) = \partial_{x^\nu_\beta} x^\mu_\alpha\, b^\nu_\beta$$

A vector field transforms with the Jacobian.

Definition 8.28. The Lie bracket of two vector fields v and w is the commutator

$$[v, w](f) = v(w(f)) - w(v(f))$$

where one has

$$[v, w] = v^\mu \partial_\mu(w^\nu \partial_\nu) - w^\mu \partial_\mu(v^\nu \partial_\nu)$$

Remark 8.29. The Lie bracket is invariant under change of coordinates

$$u = [v, w]\,, \quad (U_\alpha, \varphi_\alpha) \to (U_\beta, \varphi_\beta)\,, \quad p \in U_\alpha \cap U_\beta$$

Given

$$u = u^\nu \partial_\nu = v^\mu \partial_\mu(w^\nu \partial_\nu) - w^\mu \partial_\mu(v^\nu \partial_\nu)\,, \quad u^\nu_\alpha = u^\sigma_\beta\, \partial_{x^\sigma_\beta} x^\nu_\alpha$$

one has

$$\begin{aligned} v^\mu_\alpha \partial_\mu w^\nu_\alpha &= v^\mu_\alpha \partial_\mu(w^\sigma_\beta\, \partial_{x^\sigma_\beta} x^\nu_\alpha) = v^\delta_\beta\, \partial_{x^\delta_\beta} x^\mu_\alpha\, \partial_{x^\mu_\alpha}(w^\sigma_\beta\, \partial_{x^\sigma_\beta} x^\nu_\alpha) \\ &= v^\delta_\beta\, \partial_{x^\delta_\beta}(w^\sigma_\beta)\, \partial_{x^\sigma_\beta} x^\nu_\alpha + v^\sigma_\beta w^\delta_\beta\, \partial_{x^\sigma_\beta x^\delta_\beta} x^\nu_\alpha \end{aligned}$$

doing the same for the second addendum, one finds that the double derivatives cancel.

Example 8.30. The orthogonal group $\mathrm{O}(n)$ is a Lie group so a manifold. To build the tangent space one needs a curve

$$O : \mathbb{R} \to \mathrm{O}(n)\,, \quad t \mapsto O(t)\,, \quad O(0) = I$$

Starting from the group defining relation

$$O(t)O^\top(t) = I$$

taking the derivative in the parameter and then evaluating at $t = 0$ one gets

$$0 = (\partial_t O)O^\top + O\,\partial_t O^\top = \partial_t O + \partial_t O^\top = A + A^\top \implies A = -A^\top$$

so the matrix A is anti-symmetric over $\mathbb{R}$. Therefore, the tangent space at the identity is

$$\mathrm{o}(n) \equiv T_e\mathrm{O}(n) = \{A \in \mathrm{M}(n, \mathbb{R}) \mid A + A^\top = 0\}$$

Example 8.31. The unitary group $\mathrm{U}(n)$ is a Lie group. Taking the curve $U(t)$ such that $U(0) = I$. From the group relation one has

$$U^\dagger U = I \implies 0 = \partial_t U^\dagger\, U + U^\dagger\, \partial_t U = \partial_t U^\dagger + \partial_t U$$

[r] The tangent space is composed of anti-hermitian matrices

$$\mathrm{u}(n) = T_e U(n) = \{A \in \mathrm{M}(n, \mathbb{C}) \mid A + A^\dagger = 0\}$$

Example 8.32. Consider $\mathrm{SU}(n)$ and take a curve $U(t)$ such that $U(0) = I$. Since this is a subgroup of $\mathrm{U}(n)$ then the tangent space is made of anti-hermitian matrices. At an infinitesimal time t one can write the curve as

$$U(t) = I + tA + o(t)$$

From the determinant one has

$$\det U(t) = 1\,, \quad \det U(t) = 1 + t\,\mathrm{Tr}(A) + o(t)$$

Using the derivative, one has

$$\partial_t \det U(0) = 0 \implies \mathrm{Tr}\, A = 0$$

Therefore the tangent space is

$$\mathrm{su}(n) = T_e\mathrm{SU}(n) = \{A \in \mathrm{u}(n) \mid \mathrm{Tr}(A) = 0\}$$

Example 8.33. The same can be done for $\mathrm{SO}(n)$ which has traceless anti-symmetric matrices.

Example 8.34. Considering $\mathrm{GL}(n, \mathbb{F})$ and curve $M(t)$ such that $M(0) = I$, one can expand

$$M(t) = I + tA + o(t)\,, \quad A \in \mathrm{M}(n, \mathbb{F})$$

and then the tangent space is

$$\mathrm{gl}(n, \mathbb{F}) = T_e\mathrm{GL}(n, \mathbb{F}) = \mathrm{M}(n, \mathbb{F})$$

Similarly for $\mathrm{SL}(n, \mathbb{F})$, one has

$$\mathrm{sl}(n, \mathbb{F}) = T_e\mathrm{SL}(n, \mathbb{F}) = \{A \in \mathrm{M}(n, \mathbb{F}) \mid \mathrm{Tr}\, A = 0\}$$

Remark 8.35. In all the cases above, the elements of the tangent space are not elements of the manifold.

Definition 8.36. A Lie algebra is a vector space $\mathcal{G}$ over a field $\mathbb{F}$ (typically $\mathbb{R}$ or $\mathbb{C}$) with a bracket (called Lie product) $[\cdot, \cdot] : \mathcal{G} \times \mathcal{G} \to \mathcal{G}$ such that

- linearity

$$[x, \alpha y + \beta z] = \alpha[x, y] + \beta[x, z]\,, \quad [\alpha x + \beta y, z] = \alpha[x, z] + \beta[y, z]\,, \quad \alpha, \beta \in \mathbb{F}\,, \quad x, y, z \in \mathcal{G}$$

- anti-symmetry

$$[x, y] = -[y, x]\,, \quad \forall x, y \in \mathcal{G}$$

- Jacobi identity

$$[x, [y, z] + [y, [z, x]] + [z, [x, y]] = 0\,, \quad \forall x, y, z \in \mathcal{G}$$

Example 8.37. A vector space $M(n, \mathbb{F})$ is a Lie algebra with

$$[M_1, M_2] = M_1 M_2 - M_2 M_1$$

Remark 8.38. Any associative algebra can be turned into a Lie algebra by imposing

$$[a_1, a_2] \equiv a_1 a_2 - a_2 a_1$$

Definition 8.39 (Structure constants)**.** Let $\mathcal{G}$ be a Lie algebra and $\{t_i\}$ a basis, that is $x = x^i t_i$ with $x^i \in \mathbb{F}$ for all $x \in \mathcal{G}$. The bracket of two elements is closed in $\mathcal{G}$

$$[t_i, t_j] = c_{ij}{}^k t_k$$

where $c_{ij}{}^k$ are called structure constants. Their properties are

- anti-symmetry $c_{ij}{}^k = -c_{ji}{}^k$,
- Jacobi identity

$$c_{ij}{}^m c_{km}{}^l + c_{ki}{}^m c_{jm}{}^l + c_{jk}{}^m c_{im}{}^l = 0$$

- change of basis $t'_i = S_i{}^j t_j$

$$(c')_{ij}{}^k = S_i{}^m S_j{}^n c_{mn}{}^l (S^{-1})_l{}^k$$

The first two follow from the properties of the Lie bracket.