Group Theory

General Framework

Definition of a group (G, \circ)

- A set G endowed with an operation, $\circ: G \times G \to G$, called the group law of G, verifying 4 axioms:
 - Closure

For all a and b in G, $a \circ b$ is also in G

Associativity For all a, b and c in G,

 $(a \circ b) \circ c = a \circ (b \circ c)$

Existence of an identity element There exists an element *e* in *G* such that, for all *g* in *G*,

$$e \circ g = g \circ e = g$$

Existence of an inverse element For each a in G, there is an element b in G such that a • b = b • a = e



Unicity, commutativity, ways of notation

- The associativity allows for the brackets to be dropped when applying the operation repeatedly, but the order remains
- Exercise:

Prove that the identity element and the inverse of a given element from the group are unique!

- Abelian (commutative) group Thus is called a group having the property that for all f si g in G, $f \circ g = g \circ f$
- Additive/multiplicative notation Often in practice the group law o, the identity e, the inverse element of g and <u>g o g o ... o g</u> are denoted:

'n

- ▶ additively (+, 0, -g, ng),
- multiplicatively $(\cdot, 1, g^{-1}, g^n)$



Group order; examples

A finite group

is a group having a finite number of elements, as opposed to an infinite group

- ► The order of the group G, denoted by |G| is the number of elements in the group, if finite, or ∞
- Simple examples (exercise!) Which of the following are groups? Which are abelian groups?
 - ▶ $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$
 - the additive group of a vector space
 - $\blacktriangleright (\mathbb{Z}^*,\cdot), (\mathbb{Q}^*,\cdot), (\mathbb{R}^*,\cdot)$
 - $\blacktriangleright (\mathbb{N},+), (\mathbb{Z},\cdot)$
 - $\blacktriangleright (\mathbb{Z}_n, +)$
 - $GL_n(K)$, the set of all invertible matrices with elements taken from the field K, together with matrix multiplication

Homomorphism, Isomorphism

A group homomorphism is a map $f: G_1 \to G_2$ having the property that, for all $a, b \in G_1$, f(a)f(b) = f(ab)

Do the following hold for a homomorphism?

$$f(e_1) = e_2$$

 $f(a^{-1}) = [f(a)]^{-1}$

• A group isomorphism is an invertible homomorphism, that is one for which there exists $f^{-1}: G_2 \rightarrow G_1$ such that

$$f \circ f^{-1} = id_{G_2}$$
$$f^{-1} \circ f = id_{G_1}$$

- Show that a homomorphism is an isomorphism if and only if it is bijective
- An endomorphism is a homomorphism $f: G \to G$, where the domain and codomain coincide An automorphism is an isomorphism $f: G \to G$, where the domain and codomain coincide
- The isomorphism relation satisfies the properties of an equivalence relation:
 - reflexivity
 - symmetry
 - Transitivity

Subgroups

Subgroup A subset *H* of the group *G* is called a subgroup if, for all $a, b \in H$: $ab \in H$ $a^{-1} \in H$

- Prove that he two previous conditions can be replaced by just one, $ab^{-1} \in H$
- Notation

 $H \leq G$

- Trivial examples are the improper groups {1},G
- Is the intersections of two subgroups a subgroup? What about their union?
- Show that a subgroup of G is the center of G, formed by all the elements in G that commute with all the other elements $Z(G) = \{a \in G | ab = ba, \forall b \in G\}$

Subgroup generated by a set

- Subgroup generated by a set A ⊆ G We define ⟨A⟩ as the minimum subgroup containing A, i.e. the intersection of all subgroups of G that contain A. An element g of G is in ⟨A⟩ if and only if is a product of a finite number of either elements of A or their inverses
- A finitely generated group is a group $G = \langle A \rangle$, where A is a finite set
- A cyclic group is a group generated by just one element $G = \langle a \rangle$
- Show that any cyclic group is isomorphic to either \mathbb{Z} or \mathbb{Z}_n , where $n \in \mathbb{N}$!
- ▶ Which of \mathbb{Z} , $\mathbb{Z} \times \mathbb{Z}$ and \mathbb{Q} are cyclic or of finite type?

The order of an element in a group

The order of an element ain a group G is defined as the order of the subgroup it generates ord $a = |\langle a \rangle|$

- For a finite order element a of the group G the following hold:
 - ord $a = \min\{n \in \mathbb{N}^* | a^n = 1\}$
 - ▶ ord a = n if and only if $a^n = 1$ and $1, a, a^2, ..., a^{n-1}$ are all distinct
- > A finite group only has finite order elements.
- ▶ There are infinite groups whose every element has a finite order, called periodic groups, such as $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$, ad infinitum.
- > There are infinite groups whose only element of finite order is the identity, called torsion free groups, such as \mathbb{Z}
- ▶ If $f: G \to H$ is a homomorphism, and a is an element of G of finite order, then ord(f(a)) divides ord(a), being equal to it if f is injective. (in general the order of a subgroup divides the order of the group, as we shall see)
- Show that ord(ab)=ord(ba). It is otherwise unrelated to ord(a) and ord(b)

Transformation groups, examples

A transformation group

of a set A is a collection G of bijective (one to one and onto) transformations of the set A, having the properties:

$$\begin{array}{l} f_1, f_2 \in G \Rightarrow f_1 f_2 \in G \\ f \in G \Rightarrow f^{-1} \in G \\ \text{the identity } id_A \in G \end{array}$$

- ► G is a subgroup of S(A), the set of all bijective transformations of the set A $S(A) = \{f: A \rightarrow A | f \text{ bijective}\}$
- A permutation group is a transformation group of the set $\{1,2,...,n\}$, where $n \in \mathbb{N}^*$
- ▶ The symmetric group S_n is the set of all bijective transformations of the set $\{1,2,...n\}$, $n \in \mathbb{N}^*$ $S_n = S(\{1,2,...n\})$

We write any of the
$$|S| = n!$$
 permutations in the form

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Show that S_n is non-abelian if n>2 !

Transformation groups, examples

Exercise!

Express all the elements in S_3 in terms of the identity e, the transposition $\tau = (1,2)$ and the cycle $\sigma = (1,3,2)$. Write the multiplication table for this group

General linear group

Let V be a vector space over a field K. From the set of all endomorphisms of V, $End_{K}(V) = \{f: V \rightarrow V | f \text{ linear map} \}$ we select the bijective ones (automorphisms), defining

 $GL(V) = \{f \in End_K(V) | f \ bijective\}$

Prove the isomorphisms

- ► $End_{K}(V) \cong M_{n}(K)$ (with addition, and with multiplication, too, as ring isomorphism)
- ► $GL(V) \cong GL_n(K)$ (with multiplication)
- Prove that the translations in a vector space V $t_u: V \to V, t_u v \equiv u + v, \forall v \in V$ form a transformation group isomorphic to $V, T(V) = \{t_u | u \in V\}$

Unitary and Orthogonal Transformations

- ► The Unitary Group Given a complex vector space V, show that $U(V) \le GL(V)$, where $U(V) = \{f \in End_{\mathbb{C}}(V) | (f(u), f(v)) = (u, v), \forall u, v \in V\}$
- ▶ The Orthogonal Group Given a real vector space V, show that $O(V) \leq GL(V)$, where $O(V) = \{f \in End_{\mathbb{R}}(V) | (f(u), f(v)) = (u, v), \forall u, v \in V\}$
- Show that the set of unitary matrices $U(n) = \{A \in \mathcal{M}_n(\mathbb{C}) | A^*A = I_n\}$ is a subgroup of $GL_n(\mathbb{C})$ and that it is isomorphic to U(V) if V is a complex vector space of dimension n
- Show that the set of orthogonal matrices

 $O(n) = \{A \in \mathcal{M}_n(\mathbb{R}) | A^{\mathsf{T}}A = I_n\}$ is a subgroup of $GL_n(\mathbb{R})$ and that it is isomorphic to O(V) if V is a real vector space of dimension n

- Show that the set of unitary matrices with unit determinant $SU(n) = \{A \in U(n) | \det A = 1\}$ is a subgroup of U(n)
- Show that the set of orthogonal matrices with unit determinant $SO(n) = \{A \in O(n) | \det A = 1\}$ is a subgroup of U(n)
- How many independent real/complex parameters are needed to describe the groups O(n) and U(n), respectively? What about SO(n) and SU(n)?

Some exercises

- Study the dihedral group D_n of the isometries of the regular polygon with n sides. Show that $D_3 \cong S_3$
- ▶ What are the subgroups of $D_3 \cong S_3$? What is the centre of this group?
- Prove the Rearrangement Theorem, For every element *f* ∈ *G*, the sets {*fg*|*g* ∈ *G*} and {*gf*|*g* ∈ *G*} contain every element once and only once.

Equivalence relations

- A binary relation on a set A is a collection of ordered pairs of elements of A, i.e. a subset of the Cartesian product $A^2 = A \times A$.
- For an equivalence relation, remember the three necessary conditions:
 - Reflexivity
 - Symmetry
 - Transitivity

The equivalence class of x

If "~" is an equivalence relation on the set M we define the above as: $C_x = \{y \in M | y \sim x\}$

Partition of M

Prove that an equivalence relation divides a set M into a set of disjoint equivalence classes whose reunion is the set M

$$x, y \in M \Rightarrow C_x \cap C_y = \emptyset \text{ or } C_x = C_y$$
$$M = \bigcup_{x \in M} C_x$$

► The quotient set M/\sim is the set of all equivalence classes, $M/\sim = \{C_x | x \in M\}$

Cosets

- ▶ Left and right cosets of a subgroup $H \le G$ with respect to an element g $gH = \{gh|h \in H\}$ $Hg = \{hg|h \in H\}$
- ▶ Prove that the above can be defined as partition classes of *G* introduced by equivalence relations defined as: $x \sim_l y \text{ iff } x^{-1}y \in H$ $x \sim_r y \text{ iff } yx^{-1} \in H$
- Do these classes form subgroups?
- Find a well-defined, bijective mapping between the quotient sets, $f: G/\sim_l \to G/\sim_r$
- ► The index of a subgroup *H* in a group *G*, |G:H|is defined as the number of elements of any of the above $|G:H| = |G/\sim_l| = |G/\sim_r|$
- Study the cosets for $D_3 \cong S_3$

Lagrange's Theorem

Prove Lagrange's Theorem

|G| = |H||G:H|

(prove all classes have a given number of elements)

- Show that the order of an element divides the order of the group
- Classification of some low order groups Show that:
- ▶ *n* prime \Leftrightarrow *G* is cyclic, isomorphic to \mathbb{Z}_p
- ▶ $n=4 \Leftrightarrow G \cong \mathbb{Z}_4$ or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (the Klein four-group)
- $\blacktriangleright \quad n=6 \Leftrightarrow G \cong \mathbb{Z}_6 \text{ or } G \cong S_3$
- ▶ n=8, non abelian $\Leftrightarrow G \cong D_4$ or $G \cong Q$ (group of quaternions)
- ▶ *n*=8, abelian \Leftrightarrow *G* \cong \mathbb{Z}_8 , *G* \cong $\mathbb{Z}_4 \times \mathbb{Z}_2$ or *G* \cong $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Conjugacy classes

- ► Two elements $x, y \in G$ are said to be conjugate if there exists an element $g \in G$ such that $x = gyg^{-1}$
- Show the above relation is an equivalence one!
- The conjugacy class of an element a is defined as:

$$(a) = \{b \in G | a \sim b\}$$

- Find the conjugacy classes of
 - An abelian group
 - ► The dihedral group *D*₃
- Argue that in general, the number of conjugacy classes in the symmetric group S_n is equal to the number of integer partitions of n

Normal groups

- ▶ A subgroup $H \le G$ is called normal (or self-conjugate) if, $\forall h \in H, g \in G \Rightarrow ghg^{-1} \in H$
- Notation: $H \trianglelefteq G$
- An inner automorphism of *G*

 $\varphi_g: \mathbf{G} \to G, \varphi_g(x) = g x g^{-1}$

- $H \leq G$ is normal iff it is invariant to any inner automorphism of G
- Show that the following are normal subgroups:
 - ► {1}, G
 - ► The kernel of a group homomorphism $f: G \to G'$ Ker $f = \{x \in G | f(x) = e_{G'}\}$
 - Any subgroup of an abelian group
 - Any subgroup of index 2 in a group G
- Notice that the image of a subgroup through a group homomorphism $f: G \rightarrow G'$ is a subgroup but if $H \trianglelefteq G$ we are not sure $f(H) \trianglelefteq G'$ Provide a counterexample!

Correspondence of (normal) subgroups

- Prove that for any group homomorphism $f: G \rightarrow G'$ (not necessarily bijective)
 - $\blacktriangleright H' \trianglelefteq G' \Rightarrow f^{-1}(H') \trianglelefteq G$
 - ▶ If f is surjective then H riangleq G implies f(H) riangleq G'
 - ▶ If *f* is surjective then there is a bijective correspondence between the set of all subgroups of *G* that contain Ker f and the set of all subgroups of *G*′
 - \blacktriangleright The same as the above but for subgroups \rightarrow normal subgroups
- Study the subgroups of \mathbb{Z} . Show that:
 - ▶ $n\mathbb{Z} \leq \mathbb{Z}$, where $n\mathbb{Z} = \{nz | z \in \mathbb{Z}\}$
 - ▶ If $H \leq \mathbb{Z}$, then there exists an $n \in \mathbb{N}$ such that $H = n\mathbb{Z}$
 - ▶ $n\mathbb{Z} \le m\mathbb{Z} \Leftrightarrow m$ divides n
- Determine the subgroups of \mathbb{Z}_n using the correspondence with the subgroups of \mathbb{Z} that contain kerf
- ▶ A group is called simple if $G \neq \{1\}$ and its only normal subgroups are $\{1\}$ and G
- The only abelian simple groups are the cyclic groups of prime order!

Quotient group

- Show that, if H riangledown G is a normal subgroup, then $G/\sim_l = G/\sim_r \equiv G/H$
- Also show that the above forms a group together with the operation (xH)(yH) = xyH
- Prove that a surjective homomorphism $p: G \rightarrow G/H$ is the canonical surjection, p(x) = xH
- Determine the kernel of p(x)!
- What is the order of *G*/*H*?
- Prove the first isomorphism theorem
 - ▶ The kernel of a homomorphism $f: G \to H$ is a normal subgroup of G
 - ▶ The image of a homomorphism $f: G \to H$ is a subgroup of H
 - $\operatorname{Im} f \cong G/\operatorname{ker} f$

Universality of the factor group

• Universality of the factor group Show that if $K \trianglelefteq G$, $\varphi: G \to G/K$ is the canonical surjection, and $f: G \to H$ is a group homomorphism

H

'n.

φ

G/K

- ► $\exists h: G/K \to H$ group homomorphism such that $h \circ \varphi = f \Leftrightarrow \ker \varphi \leq \ker f$ If it exists, it is unique!
- ▶ If *h* exists, then it is surjective iff *f* is surjective
- If *h* exists and is injective, then ker $\varphi = \ker f$
- Fundamental theorem on homomorphisms let $K \triangleleft G$ (0: $G \rightarrow G/K$ is the canonical surjection and

Let $K \trianglelefteq G, \varphi: G \to G/K$ is the canonical surjection, and $f: G \to H$ is a group homomorphism.

If $K \leq \ker f$ then $\exists !$ a homomorphism $h:G/K \rightarrow H$ such that $f = h \varphi$.

▶ If $K = \ker f$ then $\exists! h:G/Ker f \rightarrow Im f$ isomorphism, called the canonical one

Exercises

► If *G* is a group, *Z*(*G*) is its center, and $\Psi: G \to \operatorname{Aut}(G)$ with $\Psi(g) = \varphi_g$, where $\varphi_g: G \to G, \varphi_g(x) = gxg^{-1}$ (inner automorphisms, forming the set $\operatorname{Inn}(G)$) show that $G/Z(G) \cong \operatorname{Inn}(G)$. (Show first that Ψ is a group homomorphism, that $\operatorname{Im}\Psi \equiv \operatorname{Inn}(G) \trianglelefteq \operatorname{Aut}(G)$, that $\operatorname{Ker}\Psi = Z(G)$)

Show that

$$\mathbb{Z}/(n\mathbb{Z})\cong\mathbb{Z}_n$$

Show that the signature of a permutation,

 $\varepsilon(\sigma) = \prod_{i < j}^{\prime} \frac{\sigma(j) - \sigma(i)}{j - i}$

is a morphism from S_n to $\{-1,1\}$ with multiplication as group law.

Show that

Ker
$$\varepsilon \equiv A_n \trianglelefteq S_n$$

 $S_n / A_n \cong \{-1, 1\}$
 $|A_n| = \frac{n!}{2}$

What is the order of a cycle? How can a permutation be decomposed uniquely into cycles?

Cayley's Theorem

Theorem

Any permutation can be decomposed uniquely (up to permutations of the factors) into a product of disjoint cycles!

Do this for:

σ =	(1)	2	3	4	5	6	7	8	9)
	(3)	9	5	8	7	4	1	6	2)

Theorem

Any group with n elements is isomorphic to a subgroup of the permutation subgroup S_n Proof:

```
Define u_g: G \to G, u_g(x) = gx
```

Prove that:

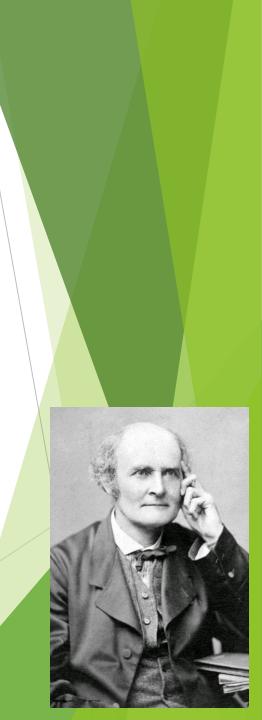
```
u_g u_h = u_{gh}, so u_g u_{g^{-1}} = id_G and therefore u_g \in S(G)

\Psi: G \to S(G), \Psi(g) = u_g is a group homomorphism

\text{Ker}\Psi = \{1\}

Therefore \text{Im}\Psi \cong G
```

- **Definition:** A group G is called simple iff $G \neq \{1\}$ and it has no normal groups apart from $\{1\}$ and G
- Prove that an abelian group G is simple iff it is isomorphic to \mathbb{Z}_p , where p is a prime number.



Direct and semidirect products

Direct product

If G_1, G_2 are groups, $G_1 \times G_2$ forms a group together with the group law $(g_1, g_2)(h_1, h_2) \equiv (g_1h_1, g_2h_2)$

• Theorem 1 about $G_1 \times G_2$

i) it contains a subgroup isomorphic to G_1 , formed by the elements (g_1, e_2) ii) it contains a subgroup isomorphic to G_2 , formed by the elements (e_1, g_2) iii) the elements of these two subgroups commute with each other iv) the only common element of the two subgroups is (e_1, e_2) v) any element of the group is the product of two elements of the two subgroups

Extending the above definition, any group that is isomorphic to one constructed as above is called a direct product group

Theorem 2

If a group G contains two subgroups, G'_1 and G'_2 , such that:

i) any two ellements from different subgroups commute with each other,

ii) G_1' and G_2' only have the identity in common,

iii) any element of the group is the product of two elements of the two subgroups, then G is a direct product group

Direct and semidirect products

- Prove that O(3) is a direct product group
- Prove that the first condition in theorem 2 is equivalent to the following: G'_1 and G'_2 are both normal subgroups of G
- To define a semi-direct group we weaken this condition by allowing G'_2 to be any kind of subgroup
- Definition: A group G is called a semi-direct product group if it possesses two subgroups, G'₁ and G'₂, such that:
 i) G'₁ ≤ G
 ii) G₁' and G₂' only have the identity in common,
 iii) any element of the group is the product of two elements of the two

iii) any element of the group is the product of two elements of the two subgroups

For both direct and semi-direct products, ii) implies that the decomposition iii) is unique

The Euclidean group of \mathbb{R}^3

The group of all linear transformation of the Euclidean space, has elements of the form $T = \{R(T), t(T)\}$, where R describes a rotation and t a translation so that:

$$\mathbf{r}' = T\mathbf{r} = \mathbf{R}(\mathbf{T})\mathbf{r} + \mathbf{t}(T)$$

- Show that indeed this forms a group, writing the explicit form of the group law and of the inverse.
- We refer to the transformations with t=0 as pure rotations and to those with R=I as pure translations
- Prove that this group is a semi-direct product group

Group representations

A linear representation of a group *G*

onto a vector space V, having the scalar field K (real/complex numbers in our applications) is a group homomorphism

 $D: G \to GL(V)$

The dimension of the representation is said to be the dimension of V

A matrix representation of a group *G* onto a vector space *V*, having the scalar field *K* (real/complex numbers in our applications) is a group homomorphism $D: G \rightarrow GL_n(K)$

- Real/complex representations
- Find a linear representation for Klein's group and for the cyclic group of order 3
- Construct matrix representations starting from a linear representation of a group G
- Two n-dimensional matrix representations $D_1: G \to GL_n(K), D_2: G \to GL_n(K)$ are said **equivalent** if there exists $S \in GL_n(K)$ such that $D_2(g) = SD_1(g)S^{-1}, \forall g \in G$

Further examples

- ► $R: \mathbb{R} \to GL(\mathbb{R}^2)$ given by the rotation with angle $\alpha \to R(\alpha)$ is a two-dimensional real representation of the group $(\mathbb{R}, +)$
- ▶ The trivial representation, $D: G \to \mathbb{C}^*$, D(g) = 1
- For a group of matrices, $D: G \to \mathbb{C}^*$, $D(g) = \det(g)$ provides a non-trivial 1D representation

The characters, invariant spaces, irreducible representations

- ► The character of a representation D is the set $\chi = \{\chi(g) | g \in G\}$, where $\chi(g) = Tr[D(g)]$
- The characters are functions of equivalence classes
- ▶ Definition: Let $D: G \to GL(V)$ be a linear representation. A subspace W of V is called **invariant** with respect to D if $D(g)W \subseteq W, \forall g \in G$
- ▶ Definition: A linear representation $D: G \rightarrow GL(V)$ is said to be irreducible if its only invariant subspaces are the trivial ones, $\{0\}$ and V
- Definition: A linear representation $D: G \rightarrow GL(V)$ is said to be reducible if it is not irreducible.
- Prove that $R: \mathbb{R} \to GL(\mathbb{R}^3)$, given by the rotation matrix with angle $\alpha \to R(\alpha)$ around the Oz axis, is a reducible representation of the group $(\mathbb{R}, +)$
- Definition: Sum of representations If $D_1: G \to GL(V_1)$, $D_2: G \to GL(V_2)$ are linear representations, show that we can define a linear representation $D: G \to GL(V_1 \oplus V_2)$, by $D(g)(x_1, x_2) = (D_1(g)x_1, D_2(g)x_2), \forall (x_1, x_2) \in V_1 \oplus V_2$

Reducible representations

- ▶ Definition: A linear representation $D: G \to GL(V)$ is said to be completely reducible if for any invariant space $U \le V$ there exists a complement invariant subspace $W \le V$ such that $V = U \oplus W$
- Describe the one-dimensional representations of a group in terms of reductibility.
- Two linear representations of a group, $D_1: G \to GL(V)$ and $D_2: G \to GL(V)$ are called equivalent if there exists a linear isomorphism $S: G \to GL(V)$, such that, for any $g \in G$

$$SD_1(g) = D_2(g)S$$

- Prove that if two linear representations of a group, $D_1: G \to GL(V)$ and $D_2: G \to GL(V)$ are equivalent and D_1 is irreducible, the same holds for D_2 , too.
- Prove that if $D: G \rightarrow GL(V)$ is completely reducible, it can be written as a direct sum of irreducible representations.

Unitary/Orthogonal representations

- A unitary representation of a group *G* onto a complex vector space *V* is a group homomorphism $D: G \rightarrow U(V)$
- Prove that any unitary representation is a completely reducible one.
- An orthogonal representation of a group Gonto a real vector space V is a group homomorphism $D: G \rightarrow O(V)$
- Similarly define unitary/orthogonal matrix representations