## Group Theory

General Framework

## Definition of a group (G,o)

- A set $G$ endowed with an operation, $\circ: G \times G \rightarrow G$, 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

$$
a \circ b=b \circ a=e
$$

## 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 $\circ$, the identity $e$, the inverse element of $g$ and $\underbrace{g \circ g \circ \cdots \circ g}_{n}$ are denoted:

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


## 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 $\infty$
- 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
- $\left(\mathbb{Z}^{*}, \cdot\right),\left(\mathbb{Q}^{*}, \cdot\right),\left(\mathbb{R}^{*}, \cdot\right)$
- $(\mathbb{N},+),(\mathbb{Z}, \cdot)$
- $\left(\mathbb{Z}_{n},+\right)$
- $G L_{n}(\mathrm{~K})$, 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 $f: G_{1} \rightarrow G_{2}$ having the property that, for all $a, b \in G_{1}$,

$$
f(a) f(b)=f(a b)
$$

- Do the following hold for a homomorphism?

$$
\begin{aligned}
& \mathrm{f}\left(e_{1}\right)=e_{2} \\
& \mathrm{f}\left(a^{-1}\right)=[f(a)]^{-1}
\end{aligned}
$$

- A group isomorphism
is an invertible homomorphism, that is one for which there exists
$f^{-1}: G_{2} \rightarrow G_{1}$ such that

$$
\begin{aligned}
& f \circ f^{-1}=i d_{G_{2}} \\
& f^{-1} \circ f=i d_{G_{1}}
\end{aligned}
$$

- Show that a homomorphism is an isomorphism if and only if it is bijective
- An endomorphism
is a homomorphism $f: G \rightarrow G$, where the domain and codomain coincide An automorphism
is an isomorphism $f: G \rightarrow G$, 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 $a, b \in \mathrm{H}$ :

$$
\begin{aligned}
& a b \in \mathrm{H} \\
& a^{-1} \in \mathrm{H}
\end{aligned}
$$

- Prove that he two previous conditions can be replaced by just one,

$$
a b^{-1} \in \mathrm{H}
$$

- Notation

$$
H \leq G
$$

- Trivial examples are the improper groups

$$
\{1\}, \mathrm{G}
$$

- 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

$$
Z(G)=\{a \in G \mid a b=b a, \forall b \in G\}
$$

## Subgroup generated by a set

- Subgroup generated by a set $A \subseteq G$

We define $\langle A\rangle$ 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 $\langle A\rangle$ 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 $\mathrm{G}=\langle A\rangle$, where $A$ is a finite set
- A cyclic group
is a group generated by just one element

$$
\mathrm{G}=\langle a\rangle
$$

- 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 $a$
in a group $G$ is defined as the order of the subgroup it generates

$$
\text { ord } a=|\langle a\rangle|
$$

- For a finite order element $a$ of the group $G$ the following hold:
- ord $a=\min \left\{n \in \mathbb{N}^{*} \mid a^{n}=1\right\}$
- ord $a=n$ if and only if $a^{n}=1$ and $1, a, a^{2}, \ldots, a^{n-1}$ 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 $f: G \rightarrow H$ is a homomorphism, and $a$ is an element of $G$ of finite order, then $\operatorname{ord}(f(a))$ divides $\operatorname{ord}(a)$, 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 $\operatorname{ord}(a b)=\operatorname{ord}(b a)$. It is otherwise unrelated to $\operatorname{ord}(a)$ and $\operatorname{ord}(b)$


## 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:

$$
\begin{aligned}
& f_{1}, f_{2} \in G \Rightarrow f_{1} f_{2} \in G \\
& f \in G \Rightarrow f^{-1} \in G \\
& \text { the identity } i d_{A} \in G
\end{aligned}
$$

- $G$ is a subgroup of $S(A)$,
the set of all bijective transformations of the set $A$

$$
S(A)=\{\mathrm{f}: \mathrm{A} \rightarrow A \mid \text { f bijective }\}
$$

- A permutation group
is a transformation group of the set $\{1,2, \ldots, n\}$, where $n \in \mathbb{N}^{*}$
- The symmetric group $S_{n}$
is the set of all bijective transformations of the set $\{1,2, \ldots n\}, n \in \mathbb{N}^{*}$

$$
S_{n}=S(\{1,2, \ldots n\})
$$

- We write any of the $|S|=\mathrm{n}$ ! permutations in the form

$$
\sigma=\left(\begin{array}{cccc}
1 & 2 & \ldots & n \\
\sigma(1) & \sigma(2) & \ldots & \sigma(n)
\end{array}\right)
$$

- 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 $_{K}(V)=\{f: V \rightarrow V \mid f$ linear map $\}$ we select the bijective ones (automorphisms), defining

$$
G L(V)=\left\{f \in \operatorname{End}_{K}(V) \mid f \text { bijective }\right\}
$$

- Prove the isomorphisms
- $E n d_{K}(V) \cong M_{n}(K)$ (with addition, and with multiplication, too, as ring isomorphism)
- $G L(V) \cong G L_{n}(\mathrm{~K})$ (with multiplication)
- Prove that the translations in a vector space $V$

$$
t_{u}: V \rightarrow V, t_{u} v \equiv u+v, \forall v \in V
$$ form a transformation group isomorphic to $V, T(V)=\left\{t_{u} \mid u \in V\right\}$

## Unitary and Orthogonal Transformations

- The Unitary Group

Given a complex vector space $V$, show that $U(V) \leq G L(V)$, where

$$
U(V)=\left\{f \in \operatorname{End}_{\mathbb{C}}(V) \mid(f(u), f(v))=(u, v), \forall u, v \in V\right\}
$$

- The Orthogonal Group

Given a real vector space $V$, show that $O(V) \leq G L(V)$, where

$$
O(V)=\left\{f \in E n d_{\mathbb{R}}(V) \mid(f(u), f(v))=(u, v), \forall u, v \in V\right\}
$$

- Show that the set of unitary matrices
$U(n)=\left\{A \in \mathcal{M}_{n}(\mathbb{C}) \mid A^{*} A=I_{n}\right\}$
is a subgroup of $G L_{n}(\mathbb{C})$ 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
$O(n)=\left\{A \in \mathcal{M}_{n}(\mathbb{R}) \mid A^{\top} A=I_{n}\right\}$
is a subgroup of $G L_{n}(\mathbb{R})$ 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
$S U(n)=\{A \in U(n) \mid \operatorname{det} A=1\}$
is a subgroup of $U(n)$
- Show that the set of orthogonal matrices with unit determinant
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 $S O(n)$ and $S U(n)$ ?


## 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 $f \in G$, the sets $\{f g \mid g \in G\}$ and $\{g f \mid g \in G\}$ 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 " $\sim$ " is an equivalence relation on the set $M$ we define the above as:

$$
C_{x}=\{y \in M \mid y \sim x\}
$$

- Partition of $M$

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

$$
\begin{aligned}
& x, y \in M \Rightarrow C_{x} \cap C_{y}=\varnothing \text { or } C_{x}=C_{y} \\
& M=\bigcup_{x \in M} C_{x}
\end{aligned}
$$

- The quotient set $M / \sim$
is the set of all equivalence classes,

$$
M / \sim=\left\{C_{x} \mid x \in M\right\}
$$

## Cosets

- Left and right cosets of a subgroup $H \leq G$ with respect to an element $g$

$$
\begin{aligned}
& g H=\{g h \mid h \in H\} \\
& H g=\{h g \mid h \in H\}
\end{aligned}
$$

- Prove that the above can be defined as partition classes of $G$ introduced by equivalence relations defined as:

$$
\begin{aligned}
& x \sim{ }_{l} y \text { iff } x^{-1} y \in H \\
& x \sim_{r} y \text { iff } y x^{-1} \in H
\end{aligned}
$$

- Do these classes form subgroups?
- Find a well-defined, bijective mapping between the quotient sets,

$$
\mathrm{f}: \mathrm{G} / \sim_{l} \rightarrow \mathrm{G} / \sim_{r}
$$

- The index of a subgroup $\boldsymbol{H}$ in a group $\boldsymbol{G},|\boldsymbol{G}: \boldsymbol{H}|$ is defined as the number of elements of any of the above

$$
|G: H|=\left|\mathrm{G} / \sim_{l}\right|=\left|\mathrm{G} / \sim_{r}\right|
$$

- 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)
- $n=6 \Leftrightarrow G \cong \mathbb{Z}_{6}$ 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 $x=g y g^{-1}$
- Show the above relation is an equivalence one!
- The conjugacy class of an element $a$ is defined as:

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

- 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 $H \leq G$ is called normal (or self-conjugate)
if, $\forall h \in H, g \in G \Rightarrow g h g^{-1} \in H$
- Notation: $\boldsymbol{H} \unlhd \boldsymbol{G}$
- An inner automorphism of $G$

$$
\varphi_{g}: G \rightarrow G, \varphi_{g}(x)=g x g^{-1}
$$

- $H \leq G$ 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 $f: G \rightarrow G^{\prime}$

$$
\operatorname{Ker} \mathrm{f}=\left\{x \in G \mid f(x)=e_{G^{\prime}}\right\}
$$

- 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 $f: G \rightarrow G^{\prime}$ is a subgroup but if $H \unlhd G$ we are not sure $\mathrm{f}(H) \unlhd G^{\prime}$ Provide a counterexample!


## Correspondence of (normal) subgroups

- Prove that for any group homomorphism $f: G \rightarrow G^{\prime}$ (not necessarily bijective)
- $H^{\prime} \unlhd G^{\prime} \Rightarrow f^{-1}\left(H^{\prime}\right) \unlhd G$
- If $f$ is surjective then $H \unlhd G$ implies $\mathrm{f}(H) \unlhd G^{\prime}$
- 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 $G^{\prime}$
- 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 $n \mathbb{Z}=\{n z \mid z \in \mathbb{Z}\}$
- If $H \leq \mathbb{Z}$, then there exists an $\mathrm{n} \in \mathbb{N}$ such that $\mathrm{H}=n \mathbb{Z}$
- $n \mathbb{Z} \leq m \mathbb{Z} \Leftrightarrow m$ divides $n$
- Determine the subgroups of $\mathbb{Z}_{n}$ using the correspondence with the subgroups of $\mathbb{Z}$ that contain $\operatorname{ker} f$
- A group is called simple if $\mathrm{G} \neq\{1\}$ 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 $H \unlhd G$ is a normal subgroup, then

$$
\mathrm{G} / \sim_{l}=\mathrm{G} / \sim_{r} \equiv G / H
$$

- Also show that the above forms a group together with the operation

$$
(x H)(y H)=x y H
$$

- Prove that a surjective homomorphism $p: \mathrm{G} \rightarrow G / H$ is the canonical surjection,

$$
p(x)=x H
$$

- Determine the kernel of $p(x)$ !
- What is the order of $G / H$ ?
- Prove the first isomorphism theorem
- The kernel of a homomorphism $f: G \rightarrow H$ is a normal subgroup of $G$
- The image of a homomorphism $f: G \rightarrow H$ 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 $\mathrm{K} \unlhd \boldsymbol{G}, \varphi: \mathrm{G} \rightarrow G / K$ is the canonical surjection, and $f: \mathrm{G} \rightarrow H$ is a group homomorphism

- $\exists h: G / K \rightarrow H$ group homomorphism such that $h \circ \varphi=f \Leftrightarrow \operatorname{ker} \varphi \leq \operatorname{ker} f$ If it exists, it is unique!
- If $h$ exists, then it is surjective iff $f$ is surjective
- If $h$ exists and is injective, then $\operatorname{ker} \varphi=\operatorname{ker} f$
- Fundamental theorem on homomorphisms


Let $\mathrm{K} \unlhd \boldsymbol{G}, \varphi: \mathrm{G} \rightarrow G / K$ is the canonical surjection, and $f: \mathrm{G} \rightarrow H$ is a group homomorphism.
If $\mathrm{K} \leq \operatorname{ker} f$ then $\exists$ ! a homomorphism $\mathrm{h}: \mathrm{G} / \mathrm{K} \rightarrow \mathrm{H}$ such that $\mathrm{f}=\mathrm{h} \varphi$.

- If $\mathrm{K}=\operatorname{ker} f$ then $\exists$ ! $\mathrm{h}: \mathrm{G} / \operatorname{Ker} \mathrm{f} \rightarrow$ Im f isomorphism, called the canonical one


## Exercises

- If $G$ is a group, $Z(G)$ is its center, and $\Psi: \mathrm{G} \rightarrow \operatorname{Aut}(G)$ with

$$
\Psi(g)=\varphi_{g} \text {, where } \varphi_{g}: G \rightarrow G, \varphi_{g}(x)=g x g^{-1}
$$

(inner automorphisms, forming the set $\operatorname{Inn}(G)$ )
show that $G / Z(G) \cong \operatorname{Inn}(G)$.
(Show first that $\Psi$ is a group homomorphism, that $\operatorname{Im} \Psi \equiv \operatorname{Inn}(G) \unlhd \operatorname{Aut}(G)$, that $\operatorname{Ker} \Psi=Z(G)$ )

- Show that

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

- Show that the signature of a permutation,

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

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

- Show that

$$
\begin{aligned}
& \operatorname{Ker} \varepsilon \equiv A_{n} \unlhd S_{n} \\
& S_{n} / A_{n} \cong\{-1,1\} \\
& \left|A_{n}\right|=\frac{n!}{2}
\end{aligned}
$$

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:

$$
\sigma=\left(\begin{array}{lllllllll}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
3 & 9 & 5 & 8 & 7 & 4 & 1 & 6 & 2
\end{array}\right)
$$

- Theorem

Any group with $n$ elements is isomorphic to a subgroup of the permutation subgroup $S_{n}$ Proof:
Define $u_{g}: \mathrm{G} \rightarrow G, u_{g}(x)=g x$
Prove that:
$u_{g} u_{h}=u_{g h}$, so $u_{g} u_{g^{-1}}=i d_{G}$ and therefore $u_{g} \in S(G)$
$\Psi: \mathrm{G} \rightarrow \mathrm{S}(G), \Psi(g)=u_{g}$ is a group homomorphism
$\operatorname{Ker} \Psi=\{1\}$
Therefore $\operatorname{Im} \Psi \cong G$

- Definition: A group G is called simple iff $\mathrm{G} \neq\{1\}$ 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

$$
\left(g_{1}, g_{2}\right)\left(h_{1}, h_{2}\right) \equiv\left(g_{1} h_{1}, g_{2} h_{2}\right)
$$

- Theorem 1 about $G_{1} \times G_{2}$
i) it contains a subgroup isomorphic to $G_{1}$, formed by the elements $\left(g_{1}, e_{2}\right)$
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, $G_{1}^{\prime}$ and $G^{\prime}{ }_{2}$, such that:
i) any two ellements from different subgroups commute with each other,
ii) $G_{1}{ }^{\prime}$ and $G_{2}{ }^{\prime}$ 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 $\mathrm{O}(3)$ is a direct product group
- Prove that the first condition in theorem 2 is equivalent to the following: $G_{1}^{\prime}$ and $G_{2}^{\prime}$ are both normal subgroups of $G$
- To define a semi-direct group we weaken this condition by allowing $G_{2}^{\prime}$ to be any kind of subgroup
- Definition: A group $G$ is called a semi-direct product group if it possesses two subgroups, $G_{1}^{\prime}$ and $G^{\prime}{ }_{2}$, such that:
i) $G_{1}^{\prime} \unlhd G$
ii) $G_{1}{ }^{\prime}$ and $G_{2}{ }^{\prime}$ only have the identity in common,
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 $T=\{R(T), \boldsymbol{t}(T)\}$, where R describes a rotation and $\mathbf{t}$ a translation so that:

$$
\mathbf{r}^{\prime}=\operatorname{Tr}=\mathrm{R}(\mathrm{~T}) \mathbf{r}+\boldsymbol{t}(T)
$$

- 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 $\boldsymbol{t}=\mathbf{0}$ as pure rotations and to those with $\mathrm{R}=\mathrm{I}$ 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

$$
D: G \rightarrow G L(V)
$$

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

$$
D: G \rightarrow G L_{n}(\mathrm{~K})
$$

- 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 $D_{1}: G \rightarrow G L_{n}(\mathrm{~K}), D_{2}: G \rightarrow G L_{n}(\mathrm{~K})$ are said equivalent if there exists $S \in G L_{n}(\mathrm{~K})$ such that

$$
D_{2}(g)=S D_{1}(g) S^{-1}, \forall g \in G
$$

## Further examples

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


## The characters, invariant spaces, irreducible representations

- The character of a representation D is the set

$$
\begin{aligned}
& \chi=\{\chi(\mathrm{g}) \mid \mathrm{g} \in G\} \text {, where } \\
& \chi(\mathrm{g})=\operatorname{Tr}[\mathrm{D}(\mathrm{~g})]
\end{aligned}
$$

- The characters are functions of equivalence classes
- Definition: Let $D: G \rightarrow G L(V)$ be a linear representation. A subspace W of $V$ is called invariant with respect to D if $\mathrm{D}(\mathrm{g}) W \subseteq W, \forall g \in G$
- Definition: A linear representation $D: G \rightarrow G L(V)$ is said to be irreducible if its only invariant subspaces are the trivial ones, $\{0\}$ and $V$
- Definition: A linear representation $D: G \rightarrow G L(V)$ is said to be reducible if it is not irreducible.
- Prove that $R: \mathbb{R} \rightarrow G L\left(\mathbb{R}^{3}\right)$, given by the rotation matrix with angle $\alpha \rightarrow R(\alpha)$ around the Oz axis, is a reducible representation of the group $(\mathbb{R},+)$
- Definition: Sum of representations

If $D_{1}: G \rightarrow G L\left(V_{1}\right), D_{2}: G \rightarrow G L\left(V_{2}\right)$ are linear representations, show that we can define a linear representation $D: G \rightarrow G L\left(V_{1} \oplus V_{2}\right)$, by

$$
D(g)\left(x_{1}, x_{2}\right)=\left(D_{1}(g) x_{1}, D_{2}(g) x_{2}\right), \forall\left(x_{1}, x_{2}\right) \in V_{1} \oplus V_{2}
$$

## Reducible representations

- Definition: A linear representation $D: G \rightarrow G L(V)$ is said to be completely reducible if for any invariant space $U \leq V$ there exists a complement invariant subspace $W \leq V$ such that $V=U \oplus W$
- Describe the one-dimensional representations of a group in terms of reductibility.
- Two linear representations of a group, $D_{1}: G \rightarrow G L(V)$ and $D_{2}: G \rightarrow G L(V)$ are called equivalent if there exists a linear isomorphism $S: G \rightarrow G L(V)$, such that, for any $\mathrm{g} \in G$

$$
S D_{1}(g)=D_{2}(g) S
$$

- Prove that if two linear representations of a group, $D_{1}: G \rightarrow G L(V)$ and $D_{2}: G \rightarrow G L(V)$ are equivalent and $D_{1}$ is irreducible, the same holds for $D_{2}$, too.
- Prove that if $D: G \rightarrow G L(V)$ 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 $G$ onto a real vector space $V$ is a group homomorphism

$$
D: G \rightarrow O(V)
$$

- Similarly define unitary/orthogonal matrix representations

