

Representation theory of finite groups

Formalization project

Raphael Gaedtke, Paul Neumann

University of Bonn

January 10, 2025

Outline

- 1 Representation Theory
- 2 Finite abelian groups
- 3 Formalization
- 4 Mathlib
- 5 Future work

Representations of finite groups

Definition

For a group G and a field k , a **representation** of G over k is a pair (V, ρ) where V is a vector space over k and $\rho : G \rightarrow \mathrm{GL}(V)$ is an action of G on V .

Representations of finite groups

Definition

For a group G and a field k , a **representation** of G over k is a pair (V, ρ) where V is a vector space over k and $\rho : G \rightarrow \mathrm{GL}(V)$ is an action of G on V .

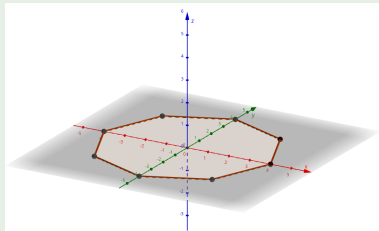
Convention: V has finite dimension, unless explicitly stated otherwise.

Definition

$\dim(V)$ is the **dimension** or **degree** of (V, ρ) .

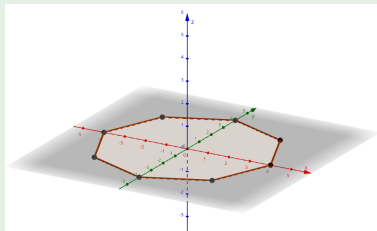
Example

$$D_{2n} = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1} \rangle$$



Example

$$D_{2n} = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1} \rangle$$



Representation $\rho : D_{2n} \rightarrow GL(\mathbb{R}^3)$ with

- $\rho(a)$ as rotation about the Z-axis
- $\rho(b)$ as a rotation about a suitable axis in the XY-plane

Invariant subspaces, Irreducibility

Definition

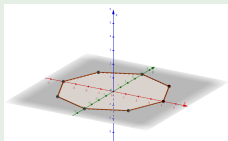
Let V be a representation and $U \subseteq V$ a subspace. U is an **invariant subspace** if $gu \in U$ for $\forall u \in U, g \in G$.

Invariant subspaces, Irreducibility

Definition

Let V be a representation and $U \subseteq V$ a subspace. U is an **invariant subspace** if $gu \in U$ for $\forall u \in U, g \in G$.

Example

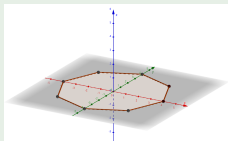


Invariant subspaces, Irreducibility

Definition

Let V be a representation and $U \subseteq V$ a subspace. U is an **invariant subspace** if $gu \in U$ for $\forall u \in U, g \in G$.

Example



The XY -Plane is an invariant subspace.

Irreducibility, Representation Homomorphisms

Definition

A representation V is **irreducible** provided $V \neq 0$ and the only invariant subspaces are 0 and V .

Irreducibility, Representation Homomorphisms

Definition

A representation V is **irreducible** provided $V \neq 0$ and the only invariant subspaces are 0 and V .

Definition

For representations V and W , a **homomorphism** is a linear map $\theta : V \rightarrow W$ with $\theta(gv) = g\theta(v)$ for $\forall g \in G, v \in V$.

Irreducibility, Representation Homomorphisms

Definition

A representation V is **irreducible** provided $V \neq 0$ and the only invariant subspaces are 0 and V .

Definition

For representations V and W , a **homomorphism** is a linear map $\theta : V \rightarrow W$ with $\theta(gv) = g\theta(v)$ for $\forall g \in G, v \in V$.

- $\text{Im}(\theta)$ and $\text{Ker}(\theta)$ are invariant subspaces
- If V and W are irreducible, then $\theta : V \rightarrow W$ is 0 or bijective.

Main theorem formalized in this project

This theorem is listed on the “Missing undergraduate mathematics in mathlib”-page.

Main theorem formalized in this project

This theorem is listed on the “Missing undergraduate mathematics in mathlib”-page.

Theorem

Let G be a finite abelian group.

Let V be a non-null vector space over an algebraically closed field k .

Let $\rho : G \rightarrow GL(V)$ be a representation.

Main theorem formalized in this project

This theorem is listed on the “Missing undergraduate mathematics in mathlib”-page.

Theorem

Let G be a finite abelian group.

Let V be a non-null vector space over an algebraically closed field k .

Let $\rho : G \rightarrow GL(V)$ be a representation.

Then ρ is irreducible if and only if $\dim_k(V) = 1$.

Proof of the theorem

Theorem

ρ is irreducible if and only if $\dim_k(V) = 1$.

“ \Leftarrow ” is trivial.

For “ \Rightarrow ”, we use the following two lemmas:

Lemma

For all $g \in G$, $\rho(g)$ is a Representation Endomorphism.

Lemma

Every Representation Endomorphism is given by multiplication with a scalar.

Proof of the theorem

With these two lemmas, we can prove the following fact:

Lemma

Every one-dimensional subspace of V is an invariant subspace.

Proof of the theorem

With these two lemmas, we can prove the following fact:

Lemma

Every one-dimensional subspace of V is an invariant subspace.

Now, we can use proof by contradiction:

Proof of the theorem

With these two lemmas, we can prove the following fact:

Lemma

Every one-dimensional subspace of V is an invariant subspace.

Now, we can use proof by contradiction:

- 1 Assume $\dim(V) > 1$.

Proof of the theorem

With these two lemmas, we can prove the following fact:

Lemma

Every one-dimensional subspace of V is an invariant subspace.

Now, we can use proof by contradiction:

- 1 Assume $\dim(V) > 1$.
- 2 Then, V has a proper subspace with dimension 1.

Proof of the theorem

With these two lemmas, we can prove the following fact:

Lemma

Every one-dimensional subspace of V is an invariant subspace.

Now, we can use proof by contradiction:

- 1 Assume $\dim(V) > 1$.
- 2 Then, V has a proper subspace with dimension 1.
- 3 So V has a proper invariant subspace.

Proof of the theorem

With these two lemmas, we can prove the following fact:

Lemma

Every one-dimensional subspace of V is an invariant subspace.

Now, we can use proof by contradiction:

- 1 Assume $\dim(V) > 1$.
- 2 Then, V has a proper subspace with dimension 1.
- 3 So V has a proper invariant subspace.
- 4 This is a contradiction to the irreducibility of V .

Representations in Mathlib

Representations are already defined in Mathlib:

```
abbrev Representation :=  
  G →* V →1[k] V  
  
end
```

Representations in Mathlib

Representations are already defined in Mathlib:

```
abbrev Representation :=  
  G →* V →1[k] V  
  
end
```

Apart from that, the definitions introduced in the beginning of this presentation are missing in Mathlib.

Definitions

```
/-- A predicate for a subspace being invariant -/
def IsInvariantSubspace {k G V : Type*} [CommSemiring k]
  [Monoid G] [AddCommMonoid V] [Module k V]
  (U : Submodule k V) (ρ : Representation k G V) :=
  ∀ g : G, ∀ u : U, ρ g u ∈ U

/-- defines degree of a representation as rank of its
    module -/
def degree {k G V : Type*} [CommSemiring k] [Monoid G]
  [AddCommMonoid V] [Module k V]
  (ρ : Representation k G V) : Cardinal := (Module.rank k
    V)
```

Representation Homomorphisms

```
-- Definition of Homomorphisms between Representations --  
@[ext] class RepresentationHom {k G V W : Type*}  
  [CommSemiring k] [Monoid G] [AddCommMonoid V] [Module  
    k V] [AddCommMonoid W] [Module k W]  
  (ρ : Representation k G V) (ψ : Representation k G W)  
  extends LinearMap (RingHom.id k) V W where  
  reprStructure : ∀ g : G, ∀ v : V, toLinearMap (ρ g v) =  
    ψ g (toLinearMap v)
```

Coercions

```
-- Coercions of RepresentationHom to Function and Linear
Map-/
instance {k G V W : Type*} [CommSemiring k] [Monoid G]
  [AddCommMonoid V] [Module k V] [AddCommMonoid W]
  [Module k W] {ρ : Representation k G V} {ψ :
    Representation k G W} : CoeFun (RepresentationHom ρ ψ
  ) (fun _ ↦ V →1 [k] W) where
coe := by
  intro θ
  use ⟨θ.toFun, ?_⟩
  simp; intro x y; simp
```

Registering Instances

Lemma

For all $g \in G$, $\rho(g)$ is a Representation Endomorphism.

```
instance repr_yields_reprHom_commMonoid {k G V : Type*}
  [CommSemiring k] [CommMonoid G] [AddCommMonoid V]
  [Module k V]
  (ρ : Representation k G V) (g : G) : (RepresentationHom
    ρ ρ) where
toFun := ρ g
map_add' := by intro x y; simp
map_smul' := by intro m x; simp
reprStructure := sorry
```