# Permutation Blocks

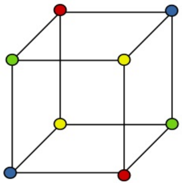
Miška Seifrtová

Katedra Algebry
MFF-UK

Spring school of Algebra
March 25. 2012

# Outline

# What is a block?

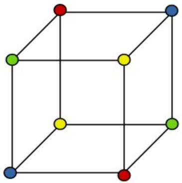


## Definition

Let $G$ be a group acting on a set $\Omega$. A block is a subset $\Delta \subseteq \Omega$ such that for all $x \in G$:

$$\Delta^x = \Delta \text{ or } \Delta^x \cap \Delta = \emptyset.$$

# What is a block?



## Definition

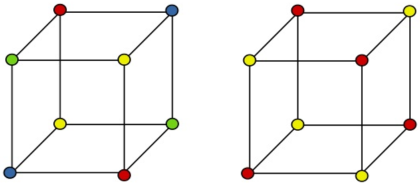
Let $G$ be a group acting on a set $\Omega$. A block is a subset $\Delta \subseteq \Omega$ such that for all $x \in G$:

$$\Delta^x = \Delta \text{ or } \Delta^x \cap \Delta = \emptyset.$$

# Blocks for the symmetry group of a cube

## Definition

The block of the smallest size (but still $> 1$) is called a minimal block.



Blocks on the left are minimal.
There can be no other blocks.

# Some simple observation about blocks

- if $G$ acts transitively on $\Omega$ and $\Delta$ is a block for $G$, then $\Sigma = \{\Delta^x, x \in G\}$ forms a partition of $\Omega$;
- each element $\omega \in \Omega$ is a (trivial) block;
- $\Omega$ also is a trivial block;

**Definition**

If $G$ acts transitively on $\Omega$ and has no non-trivial blocks, we say the group is primitive.

# Blocks and orbits of stabilizers

**Lemma**

Each block $\Delta$ for $G$ is a union of orbits for $G_\alpha$ of some $\alpha \in \Delta$.

Beware: it does not mean, that each union of orbits creates a block. In only means, that whole orbit of the stabilizer always fits into one block.

*Proof.*

For $\forall \alpha \in \Delta$, $\forall x \in G_\alpha$:

$$\alpha^x = \alpha.$$

Therefore

$$\alpha \in \Delta^x \cap \Delta \Rightarrow \Delta^x = \Delta.$$

Hence for $\forall \beta \in \Delta$

$$\beta^x \in \Delta.$$

$\square$

# Blocks and orbits of stabilizers

**Lemma**

Each block $\Delta$ for $G$ is a union of orbits for $G_\alpha$ of some $\alpha \in \Delta$.

Beware: it does not mean, that each union of orbits creates a block. In only means, that whole orbit of the stabilizer always fits into one block.

**Proof.**

For $\forall \alpha \in \Delta$, $\forall x \in G_\alpha$:

$$\alpha^x = \alpha.$$

Therefore

$$\alpha \in \Delta^x \cap \Delta \Rightarrow \Delta^x = \Delta.$$

Hence for $\forall \beta \in \Delta$

$$\beta^x \in \Delta.$$

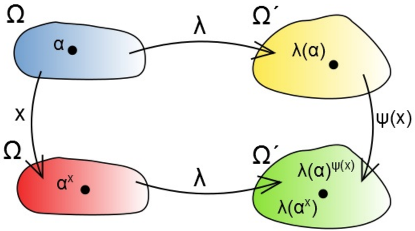
$\square$

# Permutation isomorphism definition

## Definition

Let $G \leq Sym(\Omega)$ and $H \leq Sym(\Omega')$. They are called permutation isomorphic, if there exist two mappings $\lambda$ and $\psi$ that fulfil:

- $\lambda : \Omega \to \Omega'$ is a bijection,
- $\psi : G \to H$ is a group isomorphism and
- $\lambda(\alpha^x) = \lambda(\alpha)^{\psi(x)}$ for all $\alpha \in \Omega$ and $x \in G$.



# Permutation isomorphism and conjugacy

**Theorem**

*If $G$ and $H$ are both subgroups of $Sym(\Omega)$, then they are permutation isomorphic if and only if they are conjugate in $Sym(\Omega)$.*

**Proof.**

If $G$ and $H$ be permutation isomorphic, then there is $\lambda \in Sym(\Omega)$

$\psi$ an isomorphism, so for $\forall y \in H \ \exists! x : \psi(x) = y$.

Further:

$$\lambda(\alpha^x) = \lambda(\alpha)^{\psi(x)} = \lambda(\alpha)^y$$

$$\alpha^x = \lambda^{-1}(\lambda(\alpha)^y).$$

□

# Permutation isomorphism and conjugacy

## Theorem

*If $G$ and $H$ are both subgroups of $Sym(\Omega)$, then they are permutation isomorphic if and only if they are conjugate in $Sym(\Omega)$.*

## Proof.

If $G$ and $H$ be permutation isomorphic, then there is
$\lambda \in Sym(\Omega)$
$\psi$ an isomorphism, so for $\forall y \in H \ \exists! x : \psi(x) = y$.
Further:

$$\lambda(\alpha^x) = \lambda(\alpha)^{\psi(x)} = \lambda(\alpha)^y$$

$$\alpha^x = \lambda^{-1}(\lambda(\alpha)^y).$$

□

## Theorem

*Let $G$ be a group acting transitively on a set $\Omega$, and let $H$ be a normal subgroup of $G$. Then:*

1. *orbits of $H$ form a system of blocks for $G$;*
2. *if $\Delta$ and $\Delta'$ are two $H$-orbits, then $H^{\Delta}$ and $H^{\Delta'}$ are permutation isomorphic;*
3. *if any point in $\Omega$ is fixed by all elements of $H$, then $H$ lies in the kernel of the action on $\Omega$;*
4. *the group $H$ has at most $[G : H]$ orbits, and if the index $[G : H]$ is finite, then the number of orbits of $H$ divides $[G : H]$;*
5. *if $G$ acts primitively on $\Omega$, then either $H$ is transitive or $H$ lies in the kernel of the action.*

## Theorem

*Let $G$ be a group acting transitively on a set $\Omega$, and let $H$ be a normal subgroup of $G$. Then:*

1. *orbits of $H$ form a system of blocks for $G$;*
2. *if $\Delta$ and $\Delta'$ are two $H$-orbits, then $H^{\Delta}$ and $H^{\Delta'}$ are permutation isomorphic;*
3. *if any point in $\Omega$ is fixed by all elements of $H$, then $H$ lies in the kernel of the action on $\Omega$;*
4. *the group $H$ has at most $[G : H]$ orbits, and if the index $[G : H]$ is finite, then the number of orbits of $H$ divides $[G : H]$;*
5. *if $G$ acts primitively on $\Omega$, then either $H$ is transitive or $H$ lies in the kernel of the action.*

## Theorem

*Let $G$ be a group acting transitively on a set $\Omega$, and let $H$ be a normal subgroup of $G$. Then:*

1. *orbits of $H$ form a system of blocks for $G$;*
2. *if $\Delta$ and $\Delta'$ are two $H$-orbits, then $H^{\Delta}$ and $H^{\Delta'}$ are permutation isomorphic;*
3. *if any point in $\Omega$ is fixed by all elements of $H$, then $H$ lies in the kernel of the action on $\Omega$;*
4. *the group $H$ has at most $[G : H]$ orbits, and if the index $[G : H]$ is finite, then the number of orbits of $H$ divides $[G : H]$;*
5. *if $G$ acts primitively on $\Omega$, then either $H$ is transitive or $H$ lies in the kernel of the action.*

## Theorem

*Let $G$ be a group acting transitively on a set $\Omega$, and let $H$ be a normal subgroup of $G$. Then:*

1. *orbits of $H$ form a system of blocks for $G$;*
2. *if $\Delta$ and $\Delta'$ are two $H$-orbits, then $H^{\Delta}$ and $H^{\Delta'}$ are permutation isomorphic;*
3. *if any point in $\Omega$ is fixed by all elements of $H$, then $H$ lies in the kernel of the action on $\Omega$;*
4. *the group $H$ has at most $[G : H]$ orbits, and if the index $[G : H]$ is finite, then the number of orbits of $H$ divides $[G : H]$;*
5. *if $G$ acts primitively on $\Omega$, then either $H$ is transitive or $H$ lies in the kernel of the action.*

## Theorem

*Let $G$ be a group acting transitively on a set $\Omega$, and let $H$ be a normal subgroup of $G$. Then:*

1. *orbits of $H$ form a system of blocks for $G$;*
2. *if $\Delta$ and $\Delta'$ are two $H$-orbits, then $H^{\Delta}$ and $H^{\Delta'}$ are permutation isomorphic;*
3. *if any point in $\Omega$ is fixed by all elements of $H$, then $H$ lies in the kernel of the action on $\Omega$;*
4. *the group $H$ has at most $[G : H]$ orbits, and if the index $[G : H]$ is finite, then the number of orbits of $H$ divides $[G : H]$;*
5. *if $G$ acts primitively on $\Omega$, then either $H$ is transitive or $H$ lies in the kernel of the action.*

## Proof of the theorem

1. the orbits of $H$ form a system of blocks for $G$;

**Proof.**

If $\Delta$ is an orbit of $H$, then $\alpha \in \Delta \Rightarrow \forall h \in H : \alpha^h \in \Delta$.
QUESTION: $\alpha^x \in \Delta^x \Rightarrow \forall h \in H : (\alpha^x)^h \in \Delta^x$?
$H$ normal $\Rightarrow$

$$\exists h' : (\alpha^x)^h = (\alpha^{h'})^x$$

and $(\alpha^{h'})^x \in \Delta^x$.

$\square$

# Proof of the theorem

2. if $\Delta$ and $\Delta'$ are two $H$-orbits, then $H^{\Delta}$ and $H^{\Delta'}$ are permutation isomorphic;

**Proof.**

Take blocks $\Delta, \Delta' = \Delta^c$, for some $c \in G$ and define:

$$\lambda : \Delta \to \Delta^c$$
$$\lambda(\alpha) = \alpha^c, \text{ for } \forall \alpha \in \Delta,$$

$$\psi : H^{\Delta} \to H^{\Delta^c}$$
$$\psi(x^{\Delta}) = (c^{-1}xc)^{\Delta^c} \text{ for } \forall x, y \in H.$$

$\psi$ is well defined and injective:

$$x^{\Delta} = y^{\Delta} \iff \alpha^{xy^{-1}} = \alpha \iff$$
$$\iff \alpha^{xy^{-1}c} = \alpha^c \iff \alpha^{c^{-1}xy^{-1}c} = \alpha \iff \alpha^{c^{-1}xc} = \alpha^{c^{-1}yc} \iff$$
$$\iff (c^{-1}xc)^{\Delta^c} = (c^{-1}yc)^{\Delta^c}$$

# Proof of the theorem

2. if $\Delta$ and $\Delta'$ are two $H$-orbits, then $H^{\Delta}$ and $H^{\Delta'}$ are permutation isomorphic;

## Proof.

Take blocks $\Delta, \Delta' = \Delta^c$, for some $c \in G$ and define:

$$\lambda : \Delta \to \Delta^c$$
$$\lambda(\alpha) = \alpha^c, \text{ for } \forall \alpha \in \Delta,$$

$$\psi : H^{\Delta} \to H^{\Delta^c}$$
$$\psi(x^{\Delta}) = (c^{-1}xc)^{\Delta^c} \text{ for } \forall x, y \in H.$$

$\psi$ is well defined and injective:

$$x^{\Delta} = y^{\Delta} \iff \alpha^{xy^{-1}} = \alpha \iff$$
$$\iff \alpha^{xy^{-1}c} = \alpha^c \iff \alpha^{c^{-1}xy^{-1}c} = \alpha \iff \alpha^{c^{-1}xc} = \alpha^{c^{-1}yc} \iff$$
$$\iff (c^{-1}xc)^{\Delta^c} = (c^{-1}yc)^{\Delta^c}$$

# Proof of the theorem

**Proof.**

$\psi$ is surjective, because $c^{-1}Hc = H$.

$\psi$ is homomorphism:

$$\psi(x^{\Delta}y^{\Delta}) = \psi((xy)^{\Delta}) = (c^{-1}xyc)^{\Delta^c} = (c^{-1}xcc^{-1}yc)^{\Delta^c} = \\ = (c^{-1}xc)^{\Delta^c}(c^{-1}yc)^{\Delta^c} = \psi(x^{\Delta})\psi(y^{\Delta})$$

These $\psi$ and $\lambda$ really do work:

$$\lambda(\alpha^x) = (\alpha^x)^c = \alpha^{xc}$$
$$\lambda(\alpha)^{\psi(x)} = \lambda(\alpha)^{c^{-1}xc} = (\alpha^c)^{c^{-1}xc} = \alpha^{cc^{-1}xc} = \alpha^{xc}$$

$\square$

# Proof of the theorem

## Proof.

$\psi$ is surjective, because $c^{-1}Hc = H$.

$\psi$ is homomorphism:

$$\psi(x^\Delta y^\Delta) = \psi((xy)^\Delta) = (c^{-1}xyc)^{\Delta^c} = (c^{-1}xcc^{-1}yc)^{\Delta^c} = \\ = (c^{-1}xc)^{\Delta^c}(c^{-1}yc)^{\Delta^c} = \psi(x^\Delta)\psi(y^\Delta)$$

These $\psi$ and $\lambda$ really do work:

$$\lambda(\alpha^x) = (\alpha^x)^c = \alpha^{xc}$$
$$\lambda(\alpha)^{\psi(x)} = \lambda(\alpha)^{c^{-1}xc} = (\alpha^c)^{c^{-1}xc} = \alpha^{cc^{-1}xc} = \alpha^{xc}$$

# Proof of the theorem

**Proof.**

$\psi$ is surjective, because $c^{-1}Hc = H$.

$\psi$ is homomorphism:

$$\psi(x^\Delta y^\Delta) = \psi((xy)^\Delta) = (c^{-1}xyc)^{\Delta^c} = (c^{-1}xcc^{-1}yc)^{\Delta^c} = \\ = (c^{-1}xc)^{\Delta^c}(c^{-1}yc)^{\Delta^c} = \psi(x^\Delta)\psi(y^\Delta)$$

These $\psi$ and $\lambda$ really do work:

$$\lambda(\alpha^x) = (\alpha^x)^c = \alpha^{xc}$$
$$\lambda(\alpha)^{\psi(x)} = \lambda(\alpha)^{c^{-1}xc} = (\alpha^c)^{c^{-1}xc} = \alpha^{cc^{-1}xc} = \alpha^{xc}$$

$\square$

# Proof of the theorem

3. if any point in $\Omega$ is fixed by all elements of $H$, then $H$ lies in the kernel of the action on $\Omega$;

**Proof.**

If $H$ fixes some $\alpha \in \Omega$, then $\alpha^H$ is of length 1
$\Rightarrow$ all orbits are of length 1
$\Rightarrow$ H fixes all points of $\Omega$. $\square$

# Proof of the theorem

4. the group $H$ has at most $[G : H]$ orbits, and if the index $[G : H]$ is finite, then the number of orbits of $H$ divides $[G : H]$;

**Proof.**

Look at the action of $G$ on the orbits of $H$ - $\Sigma$, defined as:

$$g : \Delta^x \mapsto \Delta^{xg} \forall x \in G.$$

Obviously the number of all orbits of $H$ is $[G : G_\Delta]$, $G_\Delta \geq G$, and

$$[G : G_\Delta] \text{ divides } [G : H].$$

□

# Proof of the theorem

5. if $G$ acts primitively on $\Omega$, then either $H$ is transitive or $H$ lies in the kernel of the action.

**Proof.**

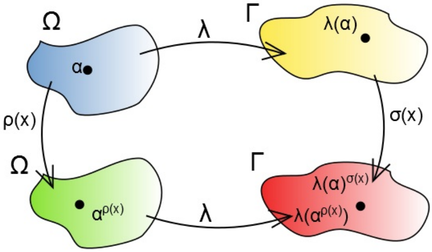
There are only trivial blocks
$\Rightarrow$ whole orbit is one block or all blocks are of size 1.
In the first case $H$ also has to act transitively.
In the other it is in the kernel of $G$. $\square$

# Equivalence of actions definition

## Definition

Having two permutation representations $\rho : G \to Sym(\Omega)$ and $\sigma : G \to Sym(\Gamma)$, we say they are equivalent, if there exists a mapping $\lambda$, such that:

- $\lambda : \Omega \to \Gamma$ is a bijection and
- $\lambda(\alpha^{\rho(x)}) = (\lambda(\alpha))^{\sigma(x)}$.



# An example of equivalent representations

## Example

Regular representation $\rho : G \to Sym(\Omega)$ of a group $G$ is equivalent to the Cayley representation $\sigma : G \to Sym(G)$, defined as $\sigma(g) \mapsto (x \mapsto xg)$.

## Proof.

We need to define $\lambda$. Take some (fixed) $\beta \in \Omega$, then for $\forall \alpha \in \Omega \exists ! g : \alpha = \beta^{\rho(g)}$.

$$\lambda : \Omega \mapsto G$$
$$\lambda : \alpha \mapsto g, \text{ such that } \alpha = \beta^{\rho(g)}.$$

This sure is a bijection. Does hold that $\lambda(\alpha^{\rho(x)}) = (\lambda(\alpha))^{\sigma(x)}$?

$$\lambda(\alpha^{\rho(x)}) = \lambda((\beta^{\rho(g)})^{\rho(x)}) = \lambda(\beta^{\rho(gx)}) = gx$$
$$(\lambda(\alpha))^{\sigma(x)} = \lambda((\beta^{\rho(g)})^{\sigma(x)}) = g^{\sigma(x)} = gx$$

# An example of equivalent representations

## Example

Regular representation $\rho : G \to Sym(\Omega)$ of a group $G$ is equivalent to the Cayley representation $\sigma : G \to Sym(G)$, defined as $\sigma(g) \mapsto (x \mapsto xg)$.

## Proof.

We need to define $\lambda$. Take some (fixed) $\beta \in \Omega$, then for $\forall \alpha \in \Omega \exists ! g : \alpha = \beta^{\rho(g)}$.

$$\lambda : \Omega \mapsto G$$
$$\lambda : \alpha \mapsto g, \text{ such that } \alpha = \beta^{\rho(g)}.$$

This sure is a bijection. Does hold that $\lambda(\alpha^{\rho(x)}) = (\lambda(\alpha))^{\sigma(x)}$?

$$\lambda(\alpha^{\rho(x)}) = \lambda((\beta^{\rho(g)})^{\rho(x)}) = \lambda(\beta^{\rho(gx)}) = gx$$
$$(\lambda(\alpha))^{\sigma(x)} = \lambda((\beta^{\rho(g)})^{\sigma(x))} = g^{\sigma(x)} = gx$$

□

# Counterexample

## Example

Let $S_2 \times S_2$ be a group acting on $\{1,2\}$.
Let $\rho : S_2 \times S_2 \to Sym(\{1,2\})$ be defined as

$$\rho(g,h) = g,$$

and $\sigma : S_2 \times S_2 \to Sym(\{1,2\})$ as

$$\sigma(g,h) = h.$$

Then $\rho(g,h)$ is permutation isomorphic to $\sigma(g,h)$, but the representations are not equivalent.

# Counterexample

## Proof.

Just realize, that both groups $\rho(g, h)$ and $\sigma(g, h)$ actually are $S_2$.
For the proof on non-equivalence of $\rho$ and $\sigma$ see the images

$$\rho((12), id) = (12)$$
$$\sigma((12), id) = id.$$

What can be $\lambda$? If it was identity, then

$$\lambda(1^{\rho((12),id)}) = \lambda(2) = 2$$
$$\lambda(1)^{\sigma((12),id)} = 1^{id} = 1.$$

If $\lambda$ was (12), then

$$\lambda(1^{\rho((12),id)}) = \lambda(2) = 1$$
$$\lambda(1)^{\sigma((12),id)} = 2^{id} = 2.$$

□

Thank you for your attention ☺ !!