

Given $G < \text{Sym}(U)$ split it into

$N \triangleleft G$ and G/N i.e.

$$0 \longrightarrow N \xrightarrow{\quad} G \xrightarrow{\varphi} G/N \longrightarrow 1$$

$\underset{\text{ker } \varphi}{N}$

faithfully $G \curvearrowright \Omega = \Delta \sqcup \Gamma$ disjoint union of G -invariant sets

$$\Rightarrow G \xrightarrow{\alpha} \text{Sym}(\Delta)$$

action homomorphisms

$$G \xrightarrow{\beta} \text{Sym}(\Gamma)$$

satisfy $\text{ker } \alpha \cap \text{ker } \beta = \langle 1 \rangle$.

$$\text{im } \alpha = A < \text{Sym}(\Delta)$$

$$\text{im } \beta = B < \text{Sym}(\Gamma)$$

$$\varphi: G \longrightarrow A \times B$$

$$g \longmapsto (\alpha(g), \beta(g))$$

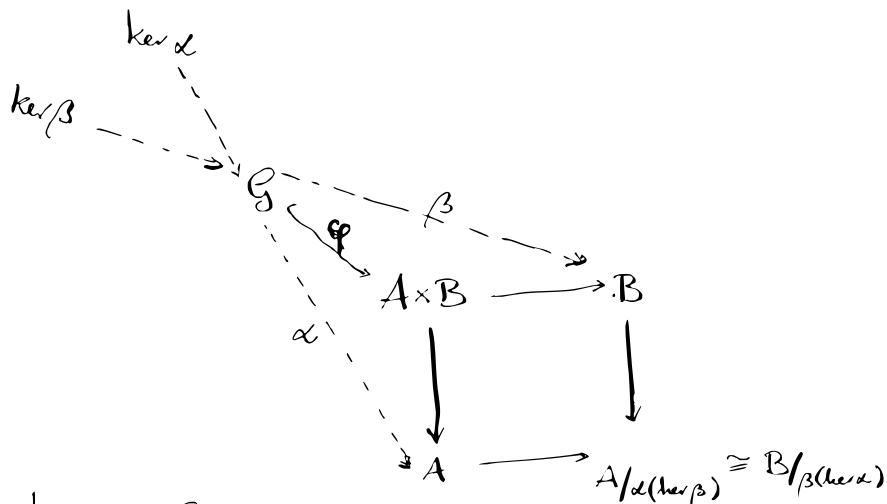
$$G \xrightarrow{\varphi} A \times B \quad \text{ker } \varphi = \langle 1 \rangle.$$

$$A \times B \xrightarrow[\text{epi}]{\pi_2} B$$

$$\text{epi} \downarrow \pi_1$$

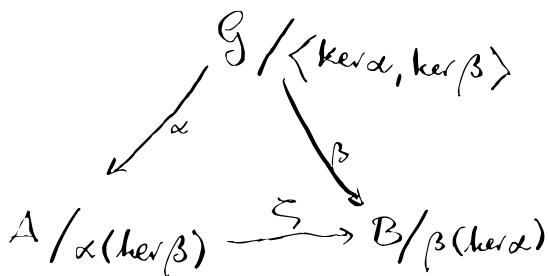
$$A$$

Defn. We say that G is (isomorphic to) a sub-direct product.



$$\text{ker } \alpha < G \Rightarrow \beta(\text{ker } \alpha) < \beta(G) = B$$

$$\alpha(\text{ker } \beta) < \alpha(G) = A$$



$$\begin{aligned} (G / \text{ker } \alpha) / \text{ker } \beta &\cong G / \langle \text{ker } \alpha, \text{ker } \beta \rangle \cong \\ &\cong (G / \text{ker } \beta) / \text{ker } \alpha \end{aligned}$$

$$\zeta: A/\text{im}(\ker\beta) \xrightarrow{\cong} B/\text{im}\beta(\ker\alpha)$$

$$\begin{array}{ccc}
 a' & \xrightarrow{\zeta} & b' \\
 \uparrow \text{wavy} & & \uparrow \text{wavy} \\
 A \ni a \cdot \alpha(x) & & b \cdot \beta(y) \quad y \in \ker\alpha \\
 \uparrow \text{wavy} & & \uparrow \text{wavy} \\
 \mathcal{G} \ni g \cdot y \cdot x & \xrightarrow{\beta} & \underline{\beta(g) \cdot \beta(y)} \\
 x \in \ker\beta & & \\
 y \in \ker\alpha & &
 \end{array}$$

thus if $g \in \text{im}\varphi(g) \in A \times B$

$$\text{then } \zeta(\alpha(g)) = \beta(g)$$

Definition: Pullback (direct product with amalgamation, external subdirect product)

A, B two groups s.t.

$$\mathcal{D} \triangleleft A, E \triangleleft B \text{ and } \zeta: A/\mathcal{D} \xrightarrow{\cong} B/E.$$

$$\text{then } A \otimes_{\zeta} B = \{ (a, b) \in A \times B : \zeta(a\mathcal{D}) = bE \}$$

Let $\varphi: A \rightarrow \mathbb{Q}$, $\sigma: B \rightarrow \mathbb{Q}$ be epimorphisms.

$$\begin{array}{ccc} A \times_{\mathbb{Q}} B & \xrightarrow{\pi_1} & A \\ \downarrow \pi_2 & & \downarrow \varphi \\ B & \xrightarrow{\sigma} & \mathbb{Q} \end{array}$$

let $A \times_{\mathbb{Q}} B$ be the subdirect product, i.e.

$$A \times_{\mathbb{Q}} B = \{(a, b) \in A \times B : \varphi(a) = \sigma(b)\}$$

Suppose that there exist G s.t.

$$\begin{array}{ccc} G & \xrightarrow{\alpha} & A \\ \downarrow \beta & & \downarrow \varphi \\ B & \xrightarrow{\sigma} & \mathbb{Q} \end{array}$$

commutes ($\varphi(\alpha(g)) = \sigma(\beta(g)) \forall g \in G$).

Then there exists a unique homomorphism

$$\mu: G \rightarrow A \times_{\mathbb{Q}} B \text{ s.t.}$$

$$\begin{array}{ccccc} G & & & & \\ \downarrow \beta & \searrow \alpha & & & \\ A \times_{\mathbb{Q}} B & \xrightarrow{\pi_1} & A & & \\ \downarrow \pi_2 & & \downarrow \varphi & & \\ B & \xrightarrow{\sigma} & \mathbb{Q} & & \end{array} \text{ commutes.}$$

Proof:

Two statements:

$$1) \exists \mu: \mathcal{G} \rightarrow A \times_{\alpha} B$$

$$\exists \varepsilon: \mathcal{G} \rightarrow A \times B \\ g \mapsto (\alpha(g), \beta(g))$$

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{\alpha} & A \\ \downarrow \beta & \searrow \pi_1 & \downarrow \sigma \\ A \times B & \xrightarrow{\pi_1} & A \\ \downarrow \pi_2 & & \downarrow \sigma \\ B & \xrightarrow{\sigma} & \mathbb{Q} \end{array} \quad \text{by commutativity:} \\ \forall g \quad \sigma(\alpha(g)) = \sigma(\beta(g))$$

$$\rightarrow \varepsilon(\mathcal{G}) \leq A \times_{\alpha} B.$$

2) let μ be the (ω -)restriction of ε .

suppose that $\mu': \mathcal{G} \rightarrow A \times_{\alpha} B$ is such map.

$\mu'(g) = (a, b)$. By commutativity (of triangles)

$$a' = \pi_1(\mu'(g)) = \alpha(g)$$

$$b' = \pi_2(\mu'(g)) = \beta(g)$$

$$\text{i.e. } \mu' \equiv \mu.$$

Corollary:

Every intransitive perm. group is a sub-direct product of two perm. groups of lower degree.

Imprimitive groups:

- $G \curvearrowright \Omega$ transitively

Defn:

Let $\mathcal{B} = \{B_1, \dots, B_n\}$ $B_i \subset \Omega$; $B_i \cap B_j = \emptyset$ for $i \neq j$
 $\cup B_i = \Omega$ (i.e. \mathcal{B} is a partition of Ω).

\mathcal{B} is a block system for $G \curvearrowright \Omega$ when

$$B_i^g \in \mathcal{B} \quad \forall g \in G$$

(i.e. \mathcal{B} is G -invariant).

Ex: trivial block systems: $\mathcal{B}_1 = \{\{i\} : i \in \Omega\}$

$$\mathcal{B}_\infty = \{\Omega\}.$$

Ex: $G = \langle (1, 2, 3, 4) \rangle$

$$\mathcal{B} = \{\{1, 3\}, \{2, 4\}\}$$

Defn: We say that $G \curvearrowright \Omega$ imprimitively

iff $G \curvearrowright \Omega$ transitively and admits a non-trivial block system.

(Otherwise we say that $G \curvearrowright \Omega$ primitively).

Lemma: Let $B = \{B_1, \dots, B_k\}$ be a block system for $G \curvearrowright \Omega$. The action of G on blocks is transitive.

Proof: transitive = $\forall i \leq i, j \leq k \exists g \in G$ s.t. $B_i^g = B_j$.

Let $\delta \in B_i$ and $\gamma \in B_j$. since $G \curvearrowright \Omega$ transitively $\Rightarrow \exists g \in G$ s.t. $\delta^g = \gamma$. the same g moves B_i to B_j .

Corollary:

- $|\Omega| = |B| \cdot |B_1|$
- Block system is determined by a single block.
- If $|G| = p$; $G \curvearrowright \Omega$ transitively, then $G \curvearrowright$ primitively.

Lemma: Suppose $G \curvearrowright \Omega$ transitively and let $S = \text{stab}_G(x)$ for some $x \in \Omega$.

then there is a bijection between subgroups

$$\{T : S \leq T \leq G\} \text{ and}$$

Block systems $B = \{B_1, \dots, B_k\}$ for $G \curvearrowright \Omega$.

namely if $x \in B_1$ then

$$B \longleftrightarrow \text{stab}_G(B_1).$$

Proof:

Let $S \leq T \leq G$.

Set $B = X^T$, $B' = B^g$.

Claim: B is a block system for $G \curvearrowright \Omega$.

Let $B^g \cap B^h \neq \emptyset$ i.e. $\delta^g = \gamma^h$ for some $\delta, \gamma \in B$.

Since $B = X^g \Rightarrow \delta = x^a$, $\gamma = x^b$ for some $a, b \in T$.

$$\Rightarrow x^{ag} = x^{bh} \quad \text{i.e.} \quad x^{a \cdot g \cdot h^{-1} \cdot b^{-1}} = x$$

$$\Rightarrow \underline{a \cdot g \cdot h^{-1} \cdot b^{-1}} \in \text{Stab}_G(x) \leq T$$

$$\Rightarrow gh^{-1} \in T.$$

Since T stabilizes B $B^{gh^{-1}} \cap B = B$ i.e.

$$B^g = B^h.$$

G -invariance is obvious by the definition of B .

Let B be a block system, $x \in B, x' \in B$.

any $g \in G$ which fixes x stabilizes B , i.e.

$$\text{Stab}_G(x) \leq \text{Stab}_G(B).$$

Let $\delta, \gamma \in B$ $\Rightarrow \exists g \in G$ s.t. $\gamma = \delta^g$, which means that $\gamma \in B^g \Rightarrow g \in \text{Stab}_G(B).$

$$x^{\text{Stab}_G(B)} = B.$$

To finish it's enough to prove that $\text{Stab}_G(x^T) = T$

If $g \in G$ s.t. $\forall t \in T, (x^t)^g = x^t$ then $tgt^{-1} \in \text{Stab}_G(x^T) = T$ \square

Definition:

A subgroup $S < G$ is called maximal

if $S \neq G$ and there is no subgroup $T < G$

s.t. $S \neq T$.

Corollary:

- A transitive group G is primitive iff a point stabilizer is a maximal subgroup.
 - Subgroup $S < G$ is maximal iff $G \uparrow S \downarrow G$ is primitive.
-

Finding blocks:

- Let $X \subset \Omega$ be a subset (a seed) we want to be $\subset B_i$.
- Start with $B_X = X$, $\{B_y = \{y\} \text{ for } y \in \Omega \setminus X\}$
- Act via $G = \langle S \rangle$ on each of B_i and merge those which intersect.
- Each B_i is represented by a unique element \rightarrow the representative
- for each $x \in \Omega$ we store the representative of B_i which x belongs to.

ALGORITHM: Union!

Input: C_1 - a subset of Ω
 C_2 - a subset of Ω

Output: the union of C_1 and C_2

begin

$r_1 = \text{representative}(C_1)$

$r_2 = \text{representative}(C_2)$

if $r_1 \neq r_2$

for $x \in \Omega$

if $\text{representative}(x) = r_2$
set-representative: (x, r_1)

end
end

return C_1

end

ALGORITHM: Block-system

INPUT:

- S - a generating set for $G = \langle S \rangle$
- Ω - a set with G -action
- \tilde{B}_1 - a subset of Ω

OUTPUT: \mathcal{B} - the finest Block system for $G \curvearrowright \Omega$
s.t. $\tilde{B}_1 \subset \mathcal{B}_1$

begin

$r = []$

queue = $[\]$ // a queue of points that have changed
for $x \in \Omega$ their blocks.

if $x \in \tilde{B}_1$

$r[x] = \text{first}(\tilde{B}_1)$

else push x to queue

$r[x] = x$

end
end

```

for  $x \in q$ 
   $\delta = \text{representative}(x)$ 
  for  $s \in S$ 
     $\alpha = \text{representative}(x^s)$ 
     $\beta = \text{representative}(\delta^s)$ 
    if  $\alpha \neq \beta$ 
      Union  $(\alpha, \beta)$ 
      push  $\beta$  to queue
    end
  end
end
return  $r$ 
end

```

Exercise: Rewrite this algorithm using Union-find tree-like data structure.

Theorem:

The algorithm converges.

Proof: Since we're taking only unions the returned partition contains \tilde{B}_1 in one of its blocks.

Since every Union! moves up on the lattice of all partitions of Ω and $\{\Omega\}$ - the trivial block system is the maximal element the algorithm has to stop unique

We need to prove that the reduced partition is in fact a block system i.e. it is G -invariant.

$$\forall x, y \in B_i \in \mathcal{B} \quad \forall s \in G$$

x^s and y^s are in the same cell B_i^s .

Note: it's enough to enforce this

for $x = \text{representative}(B_i)$, i.e. $y \rightarrow x$.

Observe that the queue collects all points for which the condition must be enforced.

If we've added all points whose representative is β we would be ok.

let $\omega \rightarrow \beta$. If we reassign $\omega \rightarrow \alpha$ this is in call to union!, so at the same time as $\beta \rightarrow \alpha$.

therefore enforcing the condition for $\beta \rightarrow \alpha$ will automatically do so for $\omega \rightarrow \alpha$

Lemma: Let $1 \in B_1 \in \mathcal{B}$ ← block system for $G \curvearrowright \Omega$.

$\Rightarrow B_1$ is union of orbits of $\text{Stab}_G(1)$.

Proof: Let $g \in \text{Stab}_G(1)$ and $\alpha, \beta \in \Omega$ s.t. $\alpha^g = \beta$.

If $\{1, \alpha\} \subset B_1 \Rightarrow \{1, \beta\} \subset B_1^g \Rightarrow B_1 \cap B_1^g \neq \emptyset \Leftrightarrow B_1 = B_1^g$
 $\Rightarrow \beta \in B_1$ □

Corollary: It is enough to start with

$$B = \{1\} \cup \alpha^{\text{stab}_G(1)}$$

since this will be definitely contained in any block that contains $\{1, \alpha\}$.

Practical tip: It's enough to find a few random elements from $\text{stab}_G(1)$ to compute

(the orbit of α).

→ e.g. schreier generators from the transversal.

Recall: Every intransitive group is a sub-direct product of its transitive parts.

Is there a universal description for imprimitive groups?

Defn: Let G, H be groups. let $\varphi: H \rightarrow \text{Aut}(G)$ be a homomorphism. then

$$G \rtimes_{\varphi} H = \langle (g, h) \in G \times H, \cdot_{\varphi}, (1, 1) \rangle$$

is a group with

$$(g_1, h_1) \cdot_{\varphi} (g_2, h_2) = (g_1 \cdot \varphi(h_2)(g_2), h_1 \cdot h_2)$$

$$(g_1, h_1) \cdot_{\varphi} (g_1, h_1)^{-1} = (1, 1)$$

$$(\varphi(h_1^{-1})(g_1^{-1}), h_1^{-1})$$

Defn: Wreath product of G and

$H < \text{Sym}(n)$ is
permutation group

$$G \wr H := G^n \rtimes H$$

the natural action of H
on coordinates of G^n .

$$\begin{aligned} & ((g_1, \dots, g_n), h) \cdot ((a_1, \dots, a_n), b) = \\ & = ((g_1, \dots, g_n) \cdot (a_1, \dots, a_n)^b, h \cdot b) = \\ & = ((g_1 \cdot a_{b^{-1}(1)}, g_2 \cdot a_{b^{-1}(2)}, \dots, g_n \cdot a_{b^{-1}(n)}), h \cdot b). \end{aligned}$$

Suppose that $G \curvearrowright \Omega \Rightarrow G \wr H \curvearrowright \bigsqcup_n \Omega$

\uparrow \downarrow
 i -th copy acts on i -th copy of Ω

H permutes G 's $\rightarrow H$ permutes copies of Ω .

the imprimitive action of $G \wr H$

Theorem: Let G be a transitive, imprimitive group.

Let B be a non-trivial block system for G .

Let $1 \in B \in \mathcal{B}$ and let $T = \text{stab}_G(B) < G$.

Let $\psi: G \rightarrow \text{Sym}(B)$ (action homomorphism)

$\varphi: T \rightarrow \text{Sym}(B)$ (action homomorphism)

Then $G \xrightarrow{\mu} \varphi(T) \times \psi(G)$ as follows:

$\left\{ \begin{array}{l} \text{Let } \tau_1, \dots, \tau_n \text{ be representatives for } \frac{G}{T}. \\ \text{Let } g \in G. \text{ then } g \text{ "permutes" the} \\ \text{cosets i.e. } \tau_i \cdot g \text{ belongs to } \psi(g)(i)\text{-th} \\ \text{coset.} \\ \Rightarrow \tau_i \cdot g \cdot \tau_{\psi(g)(i)}^{-1} =: \tilde{g}_i \text{ stabilizes} \\ \text{i-th coset.} \\ \Rightarrow \tilde{g}_i \in T \end{array} \right.$

we define

$$\mu(g) = ((\varphi(\tilde{g}_1), \dots, \varphi(\tilde{g}_n)); \psi(g))$$

that's almost correct...

$$\varphi(\tilde{g}_i) \rightsquigarrow \varphi(\widetilde{g_{\psi(g)(i)}})$$

Exercise: check that μ is actually a
homomorphism.

Classification of primitive groups

Lemma:

If $G \curvearrowright \Omega$ transitively and $N \triangleleft G$ then orbits of $N \curvearrowright \Omega$ form a block system for $G \curvearrowright \Omega$.

Proof: Δ - N -orbit, $g \in G$.

We will show that Δ^g is N -orbit.

If $\delta, \gamma \in \Delta \Rightarrow \delta^g, \gamma^g \in \Delta^g$.

Let $n \in N$ s.t. $\delta^n = \gamma$ then

$(\delta^g)^{\underbrace{ng}_{m \in N}} = \delta^{ng} = \gamma^g \Rightarrow \gamma^g$ and δ^g are in the same N -orbit.

If Δ^g is not the whole N -orbit

then $(\Delta^g)^{g^{-1}}$ is a proper subset of Δ



□.

Corollary: If G is primitive then N acts transitively.

Defn:

$N \triangleleft G$ is called minimally normal if the only normal in G proper subgroup of N is $\{1\}$.

$(M \triangleleft G \text{ \& } M \triangleleft N \Rightarrow M = \{1\})$

Lemma:

Minimally normal subgroups are of the form

$$N = \bigoplus_k T$$

where T is a simple group.

Definition: The socle of G is the subgroup generated by minimally normal subgroups:

$$\text{soc}(G) = \langle N \mid N \triangleleft G \text{ -minimally} \rangle.$$

Lemma:

$$\text{soc}(G) = \bigoplus_i N_i \quad N_i \text{ -minimally normal}$$

Proof:

← subgroups

$$\text{If } H = \langle N, M \rangle \text{ and } N \cap M = \langle 1 \rangle \Rightarrow$$

$$H \cong N \oplus M$$

Let H - maximal subgroup of $\text{soc}(G)$ which is a product of minimally normal subgroups

$$\text{If } H \neq \text{soc}(G) \Rightarrow \exists N \triangleleft G \text{ s.t. } N \not\leq H.$$

then $N \cap M \triangleleft G$ ↑ minimally normal.

by minimality of N : $N \cap M = \langle 1 \rangle$

$$\Rightarrow \langle N, M \rangle = N \times M$$

⚡ \square

Lemma:

let $G \curvearrowright \Omega$ primitively.

$\Rightarrow \text{soc}(G)$ is minimally normal or

$$\text{soc}(G) = N \times M, \quad N \cong M \text{ minimally normal and non-abelian.}$$

Types of Socles:

- $\text{soc}(G) \cong \bigoplus_m T$ ← homogeneous of type T
↳ T -abelian i.e. $T \cong C_p$ -cyclic of order p .
⇒ primitive $G \cong \text{soc}(G) \rtimes \text{Stab}_G(1)$

Proof:

$\text{Soc}(G)$ -abelian, minimally normal ⇒
 $\text{Soc}(G) \cong C_p^m \cong \mathbb{F}_p^m$. By transitivity & faithfulness
 p -prime
 $|\Omega| = p^m$.

Let $S = \text{Stab}_G(1)$ ← by primitiveness S
is a maximal subgroup, but
 $\text{soc}(G) \not\leq S$ ($\text{soc}(G) \curvearrowright \Omega$ transitively!.)
⇒ $G = \text{soc}(G)S$. Since $\text{soc}(G)$ is abelian
 $S \cap \text{soc}(G) \triangleleft \text{soc}(G)$. Since we also have
 $S \cap \text{soc}(G) \triangleleft S \Rightarrow S \cap \text{soc}(G) = \langle 1 \rangle$
⇒ $G \cong \text{soc}(G) \rtimes S$.

□

Note: the action of G on Ω is through
an affine map where each element of S
acts through a matrix representation

$$S \rightarrow \text{GL}(m, \mathbb{F}_p)$$

and $\text{soc}(G)$ corresponds to translations.

- $\text{soc}(G)$ is non-abelian.

$$\hookrightarrow \text{If } Z(\text{soc}(G)) = \langle 1 \rangle \Rightarrow G \leq \text{Aut}(\text{soc}(G)).$$

Proof: If $G \curvearrowright \text{soc}(G)$ by conjugation, then $C_G(\text{soc}(G))$ is the kernel of the action.

$$Z(\text{soc}(G)) = \{z \in \text{soc}(G) \mid \forall g \in \text{soc}(G) \quad gz = zg\}$$

is a normal subgroup of $C_G(\text{soc}(G))$.

Any minimally normal subgroup of $C_G(\text{soc}(G))$ would be inside $Z(\text{soc}(G))$ which is trivial

\Rightarrow the kernel of the action of G on $\text{soc}(G)$ is trivial \Rightarrow

$$G \hookrightarrow \text{Aut}(\text{soc}(G)).$$

Lemma: for T -simple $\text{Aut}(T^m) = \text{Aut}(T) \wr \text{Sym}(m)$

□

Product action of $G \wr H$:

$$G \leq \text{Sym}(\Omega)$$

$$H \leq \text{Sym}(\Delta)$$

$$\Rightarrow G \wr H \curvearrowright \Omega^\Delta \cong \Omega^{|\Delta|}$$

\uparrow
 (Δ) -tuples of
 elts from Ω

$$d = |\Delta|$$

$$G^d \curvearrowright \Omega^d \quad \text{"dimension-wise"}$$

$$H \curvearrowright \Omega^d \quad \text{"permuting the dimensions"}$$

the product action of $G \wr H$

Let $\mathcal{D} < T^m$ be the image of

$$T \hookrightarrow T^m \quad g \mapsto (g, \dots, g). \quad (\text{diagonal embedding}).$$

$$T^m \curvearrowright \mathcal{D} \backslash T^m \quad (\text{action homomorphism into } \text{Sym}(|\mathcal{D} \backslash T^m|) \text{ of degree } n = |T^{m-1}|)$$

$\underbrace{\hspace{10em}}_{\Omega}$

$$\mathcal{N} = \mathcal{N}_{\text{Sym}(n)}(T^m) \curvearrowright T^m \text{ by conjugation}$$
$$\mathcal{N} \triangleleft \text{Aut}(T^m)$$

However we don't necessarily have $\mathcal{G} < \mathcal{N}$.

In the case this happens we say that \mathcal{G} is of diagonal type.

Lemma:

\mathcal{G} of diagonal type is primitive iff $m=2$ or $\mathcal{G} \curvearrowright T^m$ is primitive.

Theorem: (Scott-O'Nan theorem).

$G \curvearrowright \Omega$ primitively, faithfully with $|\Omega| = n$.

Let $H = \text{soc}(G)$ and assume that $H = T^m$ is of type T. Then one of the points below describes the action:

1) T is abelian of order p , $n = p^m$,

$$G \cong H \rtimes \text{Stab}_G(x) \quad (x \in \Omega)$$

$G \curvearrowright \Omega$ through an affine action.

2) $m = 1$, $H \triangleleft G \leq \text{Aut}(H)$ " G is almost simple".

3) $m \geq 2$, $n = |T|^{m-1}$, $G \leq \text{Aut}(T) \wr \text{Sym}(m)$
and either

3a) $m = 2$ $G \curvearrowright \{T_1, T_2\}$ intransitively

3b) $m \geq 2$ $G \curvearrowright \{T_1, \dots, T_m\}$ primitively

the action of G on Ω is of the diagonal type.

4) $m = rs$, $s > 1$ then

$G \leq A \wr B$ where $A \wr B$ acts

through the product action.

Therefore $B < \text{Sym}(d)$, $|\Omega| = n = d^s$ and B is transitive. A is primitive

4a) of type 3a with $\text{soc}(A) = T^2$ (i.e. $r=2$)

4b) of type 3b with $\text{soc}(A) = T^r$

4c) of type 2 (i.e. $r=1$, $s=m$).

- 5) "Twisted wreath type". H is freely and $n = |T^m|$.
 $\text{Stab}_g(x)$ is a transitive subgroup of $\text{Sym}(m)$.
(note: this type occurs only for groups of order 60^6).