BACHELORARBEIT

Titel der Bachelorarbeit

Minimal Permutation Degree of Finite Groups

Verfasser

Julian Kretschmer

angestrebter akademischer Grad

Bachelor of Science (BSc.)

Wien, im Monat Juli 2020

Studienkennzahl lt. Studienblatt:	A 033621
Studienrichtung lt. Studienblatt:	Mathematik
Betreuer:	ao. Univ.-Prof. Dr. Dietrich Burde

Abriss

Der minimale Permutationsgrad einer endlichen Gruppe G ist die kleinste positive ganze Zahl für die ein Monomorphismus von G in die symmetrische Gruppe S_n existiert. Diese Arbeit legt den Fokus hauptsächlich auf einige Spezialfälle, insbesondere auf Gruppen in denen der minimale Permutationsngrad der Ordnung der Gruppe entspricht, abelsche Gruppen und semidirekte Produkte von zyklischen p-Gruppen.

Abstract

The minimal permutation degree of a finite group G is the smallest positive integer n for which an injective homomorphism from G to the symmetric group S_n exists. This thesis mainly focuses on some special cases, specifically on groups where the minimal permutation degree is the group order, abelian groups and the semidirect products of cyclic p-groups.

Contents

1 Introduction

This bachelor thesis is about finding the minimal permutation degree for finite groups and gives an introduction into this field. In the Preliminaries we reiterate the definition and some important properties of symmetric groups that are relevant for this thesis. Furthermore we will motivate the problem and recapitulate theorems that are important for the following sections. In Section 3 the problem will be introduced in a formal way and the connection to subgroup structures will be shown. The section after that categorizes all groups in which the minimal permutation degree is the group order. Section 5 focuses on abelian groups and proves a general formula to calculate the minimal permutation degree for all these groups. In the last section we take a look at semidirect products and prove a formula to calculate the minimal permutation degree for semidirect products of cyclic p-groups.

The most used references are the article "Minimal permutation of Finite Groups" by Johnson [D L71], the article "The minimal degree of permutation representations of finite groups" by Becker [Bec12] and the master thesis "Minimal Permutation Representations of Classes of Semidirect Products of Groups" by Hendriksen [Hen16].

2 Preliminaries

2.1 Symmetric Group

Definition 2.1 (Symmetric Group)**.** Let N be the set $\{1, 2, 3, ..., n\}$. The set of all bijections $N \to N$ with the group operation composition of functions forms a group, the finite symmetric group S_n.

We will just focus on finite symmetric groups, therefore the term symmetric group is equivalent to finite symmetric group in this work. We sometimes will use the notation $\mathrm{Sym}(G)$ for the group with all possible permutations of the finite group G, obviously $\mathrm{Sym}(G) \cong S_n$, for $|G| = n$. The number of bijections $\phi : N \to N$ is the same as the number of permutations, therefore the order of the group is $|S_n| = n!$.

Example 2.1. (S_3)
All possible bijections between three elements in cycle notation are id, (2 3), (1 3), (1 2), (1 2 3), (1 3 2), the order of the elements are

$$\begin{aligned}
&\mathrm{ord}(id) = 1,\\
&(2\ 3)^2 = (2\ 3) \circ (2\ 3) = id,\ \mathrm{ord}((2\ 3)) = 2,\\
&(1\ 3)^2 = (1\ 3) \circ (1\ 3) = id,\ \mathrm{ord}((1\ 3)) = 2,\\
&(1\ 2)^2 = (1\ 2) \circ (1\ 2) = id,\ \mathrm{ord}((1\ 2)) = 2,\\
&(1\ 2\ 3)^3 = (1\ 2\ 3) \circ (1\ 2\ 3) \circ (1\ 2\ 3) = id,\ \mathrm{ord}((1\ 2\ 3)) = 3,\\
&(1\ 3\ 2)^3 = (1\ 3\ 2) \circ (1\ 3\ 2) \circ (1\ 3\ 2) = id,\ \mathrm{ord}((1\ 3\ 2)) = 3.
\end{aligned}$$

S_3 is non-abelian, for example

$$(1\ 3) \circ (1\ 2) = (1\ 2\ 3) \neq (1\ 3\ 2) = (1\ 2) \circ (1\ 3).$$

In general all symmetric groups S_n with $n \geq 3$ are non-abelian. That the element of the highest order is n, isn't true for $n \geq 5$. For example, the element $(12)(345) \in S_5$ has order 6.

Example 2.2 (Order of $(12)(345) \in S_5$).

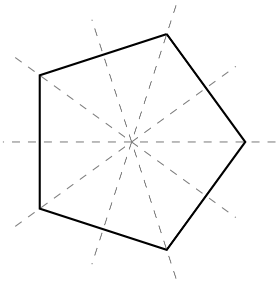
$$\begin{aligned}
(12)(345)^6 &= \\
= (354) \circ (12)(345)^4 &= (12) \circ (12)(345)^3 \\
= (345) \circ (12)(345)^2 &= (12)(354) \circ (12)(345) \\
&= id.
\end{aligned}$$

2.2 Motivation

A conclusion from Example 2.2 is, that the subgroup $\langle(12)(345)\rangle \subseteq S_5$ is isomorphic to $\mathbb{Z}_6$. We can also find a lot of other groups in S_5. For example $\langle(12345), (25)(34)\rangle \subseteq S_5$ is isomorphic to D_{10}.

Example 2.3 (D_{10}). D_{10} are the rotations and reflections of a pentagon. The group is generated by $\{r, s\}$, where $r^5 = s^2 = 1$ and $srs^{-1} = r^{-1}$. One of its representations in S_5 is

$$\begin{aligned} 1 &\mapsto id & s &\mapsto (15)(24) \\ r &\mapsto (12345) & sr &\mapsto (14)(23) \\ r^2 &\mapsto (13524) & sr^2 &\mapsto (13)(45) \\ r^3 &\mapsto (14253) & sr^3 &\mapsto (12)(35) \\ r^4 &\mapsto (15432) & sr^4 &\mapsto (25)(34). \end{aligned}$$



So we can ask the following question: Let G be a finite group. Is there a subgroup H of S_n such that $H \cong G$? In other words, when is there an injective homomorphism $G \hookrightarrow S_n$? We will see very soon that the question whether this is possible for some S_n is answered pretty quickly. So we are in particular interested in finding the smallest S_n which we can map our group. We will call this n "minimal permuation degree". At first we will state that we can always map a group of order d into the Symmetric Group S_d.

Theorem 2.1 (Cayley for finite groups)**.** *Any finite group G of order n can be realized as a subgroup of S_n.*

Proof. Let G be a group of order n. For every $a \in G$ we define $\tau_a : G \to G$ as $\tau_a(x) = a \cdot x$. Every τ_a is a permutation of G and therefore a member of S_n. If we consider the mapping of all those permutations $\pi : G \to S_n$ with $\pi(a) = \tau_a$, the image $\mathrm{Im}(\pi) = \{\tau_a : a \in G\}$ will be a subgroup of S_n. We establish this by showing that π is a group homomorphism and injective.

$$\tau_a \circ \tau_b = a \cdot (b \cdot x) = (a \cdot b) \cdot x = \tau_{a \cdot b}.$$

The homomorphism T is injective, because if there was a $\tau_a = \tau_b$, then in particular $a = \tau_a(e) = \tau_b(e) = b$. Now we restrict the set of destination to $\mathrm{Im}(T)$ to get an isomorphism between G and $\mathrm{Im}(T)$, which is a subgroup of S_n. □

2.3 Preliminary Theorems and Lemmas

Lemma 2.2. *A subgroup H of a cyclic group G is cyclic.*

Proof. Let the generator of G be g. Every element of G is by definition of cyclic groups of the form g^n. Therefore H has to have an element g^n, for an $n \in \mathbb{N}$. Let $\tilde{n} > 0$ be the smallest number for which $g^{n_0} \in H$. Let h=g^n be an arbitrary element of H. We can find $r, d \in \mathbb{N}$ such that $n = \tilde{n}d + r$, with $0 \leq r < \tilde{n}$. Then

$$h = g^n = g^{\tilde{n}d+r} = (g^{\tilde{n}})^d \cdot g^r.$$

Since $g^{\tilde{n}} \in H$, so is its powers $(g^{\tilde{n}})^d \in H$, and the inverse $((g^{\tilde{n}})^d)^{-1} \in H$. Then

$$((g^{\tilde{n}})^{-d}) \cdot g^n = g^r.$$

The product of two elements is an element of the group, and so we conclude $g^r \in H$, but $\tilde{n}$ is the smallest strict positive number, therefore r has to be 0. From

$$n = \tilde{n}d$$

follows

$$h = g^n = (g^{\tilde{n}})^d$$

for an arbitrary $h \in H$. So $H = \langle g^{\tilde{n}} \rangle$. □

Theorem 2.3 (Lagrange)**.** *Let G be a finite Group G and let H be a subgroup of G, then*

$$|G| = [G\colon H] \cdot |H|.$$

In particular, the order of H divides the order of G.

For a proof see [Bur17, p.8]. Note that there does not have to be a subgroup of order m, just because $m \mid |G|$.

Theorem 2.4 (Sylow's Theorem)**.** *Let G be a group of order $|G| = p^r \cdot m$, with p a prime number, $m, r \in \mathbb{N}$ and $p \nmid m$. We call a subgroup of order p^r a p-Sylow subgroup.*

(i). For every $0 \leq s \leq r$, there is a subgroup of order p^s.

(ii). If H is a p-subgroup and S a p-Sylow subgroup of G, then there exists a $g \in G$ with $H \leq gSg^{-1}$.

(iii). For the number k of p-Sylow subgroups the following holds: $k \mid m$ and $k \equiv 1 (mod\ p)$.

For a proof see [Bur17, p.20-23].

Theorem 2.5 (Krull-Schmidt Theorem)**.** *Let G be a group that satisfies* *(i). For every chain $G_1 \subseteq G_2 \subseteq G_3 \subseteq \dots$ of normal subgroups of G there is an n such that $G_i = G_n$ $\forall i > n$.*

(ii). For every chain $G_1 \supseteq G_2 \supseteq G_3 \supseteq \dots$ of normal subgroups of G there is an n such that $G_j = G_n$ $\forall j > n$.

Then, if

$$G = H_1 \times \dots \times H_r = \tilde{H}_1 \times \dots \times \tilde{H}_s$$

are decompositions of G into indecomposable factors, then $r = s$ and for every H_i there is a $\tilde{H}_j$ such that $H_i \cong \tilde{H}_j$. Moreover, if we reindex $\tilde{H}_j$ in such a way that $\tilde{H}_i \cong H_i$, we can take any $1 \leq t \leq r$ such that

$$G = H_1 \times \dots \times H_t \times \tilde{H}_{t+1} \times \dots \times \tilde{H}_r.$$

For a proof see [Hun12, p.86].

3 Permutation Representation Theory

3.1 Permutation Representations

Definition 3.1 (permutation group)**.** We call a group a permutation group if it is a subgroup of a symmetric group S_n.

So Cayley's Theorem can also be read as 'any finite group can be realized as a permutation group'.
In contrast to the linear representation theory, which studies homomorphisms $\rho : G \to GL_k(V)$, we want to study homomorphisms $\phi : G \to S_n$.

Definition 3.2 (permutation representation)**.** A permutation representation is a homomorphism from G to a symmetric group

$$\phi : G \to S_n.$$

If we were only interested in those homomorphisms, we could trivially map every group to the trivial group $S_1 = (\{id\}, \circ)$. However, when looking for a monomorphism (which adds the requirement of injectivity), the problem gets more interesting.

Definition 3.3. An injective permutation representation $\phi : G \hookrightarrow S_n$ is called a faithful permutation representation.

Finding the smallest S_n to a Group G for which a faithful permutation representation exists is non-trivial. We will consider this problem in the following.

3.2 Minimal Permutation Degree

Definition 3.4 (minimal permutation degree of finite groups)**.** The minimal permutation degree of a finite group G is defined as

$$\mathrm{d}(G) = \min\{n \in \mathbb{N} \mid G \hookrightarrow S_n\}.$$

This definition is well-defined, because we already know that the set $\{n \in \mathbb{N} \mid G \hookrightarrow S_n\}$ can't be empty, because at least all $n \geq |G|$ are by Cayley's Theorem 2.1 in it. Also Cayley's Theorem gives us an upper bound.

Lemma 3.1 (upper bound of $\mathrm{d}(G)$)**.** *The upper bound of* $\mathrm{d}(G)$ *for a group G of order n is*

$$\mathrm{d}(G) \leq n.$$

Proof. This follows directly from our considerations above. We can always construct the same monomorphism as in the proof of Cayley's Theorem 2.1 and therefore $\min\{n \in \mathbb{N} \mid G \hookrightarrow S_n\}$ is at most n. □

Now we can state that there are examples of groups for which this boundary is already sharp.

Example 3.1 ($\mathbb{Z}_2$). S_2 and $\mathbb{Z}_2$ are isomorphic and so the codomain can't be smaller without losing the injectivity. So it has to be $\mathrm{d}(\mathbb{Z}_2) = 2$.

We will try to generalize this later, but first we are going to find examples for which this bound isn't sharp. Those are not hard to find, we already saw examples in Example 2.2 and Example 2.3, other obvious ones are the symmetric groups themselves or the alternating groups.

Example 3.2 ((A_4)). The alternating group of degree 4 and is the group of all even permutations of four elements. The group has order 12 and is by definition a subgroup of S_4. There can't be a monomorphism to S_3, because S_3 is just of order 6. So $\mathrm{d}(A_4) = 4 < 12$.

We can also find a lower bound.

Lemma 3.2 (Lower Bound)**.** *Let G be a group with order g and let* $f(g)$ *be the natural number fulfilling the inequality* $f(g)! \leq g \leq (f(g)+1)!$*. Then* $f(g)$ *is a lower bound for the minimal permutation degree, i.e.*

$$f(g) \leq \mathrm{d}(G).$$

Proof. Let $d(G) = m$, $f(g)$ is a lower bound because if there exists a monomorphism $\phi : G \hookrightarrow S_m$, obviously the order of S_m can't be smaller than g. Since $f(g)! \leq g \leq |S_m| = m!$, we get $f(g) \leq m = \mathrm{d}(G)$. □

Definition 3.5 (regular representation)**.** Let G be a finite group of order n. The monomorphism $\phi : G \hookrightarrow S_n$, $\phi(g) = \varphi(g)$ with $\varphi(g) : G \hookrightarrow G$, $\varphi(g)(x) = g \cdot x$ for every $g, x \in G$ is called a regular Representation of G. We already showed that this is a monomorphism in the proof of Cayley's Theorem.

Example 3.3 ($\mathbb{Z}_4$). We want to construct the regular representation of $\mathbb{Z}_4 \to S_4$.

$$\begin{aligned}
\varphi(0)(x) &= 0 + x \implies \phi(0) = id \\
\varphi(1)(x) &= 1 + x \implies \phi(1) = (1234) \\
\varphi(2)(x) &= 2 + x \implies \phi(2) = (13)(24) \\
\varphi(3)(x) &= 3 + x \implies \phi(3) = (1432)
\end{aligned}$$

We constructed a subgroup of S_4 which is isomorphic to $\mathbb{Z}_4$.

$$\mathbb{Z}_4 \cong \{id, (1234), (13)(24), (1432)\}$$

This regular Representation exists for every finite group. In this chapter we want to categorize all groups for which this is already minimal. So we want to find all groups G of order n with $d(G) = n$.

Definition 3.6 (transitive representations)**.** We now consider the following representation. For a group G and a normal subgroup H we define the homomorphism

$$\begin{aligned}
&\phi_H : G \to S_{|G/H|} \\
&\phi_H(g) = \varphi_H(g) \\
&\varphi_H(g) : G \to G/H \\
&\varphi_H(g)(x) = (g \cdot x)H.
\end{aligned}$$

We say ϕ_H is induced by H. ϕ_H is called the transitive representation induced by H.

Note that the representation induced by $\{e_G\}$ is the regular representation.

Example 3.4 ($\mathbb{Z}_4 \times \mathbb{Z}_2$ with subgroup $\langle(2,0)\rangle$). We construct the homomorphism induced by $\langle(2,0)\rangle$. $\phi : G \to S_{(|\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle(2,0)\rangle|}$.

$$\begin{aligned}
\varphi(0,0)(x) = \varphi(2,0)(x) = ((0,0)+x) + \langle(2,0)\rangle &\Rightarrow \phi(0,0) = \phi(2,0) = id \\
\varphi(0,1)(x) = \varphi(2,1)(x) = ((0,1)+x) + \langle(2,0)\rangle &\Rightarrow \phi(0,1) = \phi(2,1) = (12)(34) \\
\varphi(1,0)(x) = \varphi(3,0)(x) = ((1,0)+x) + \langle(2,0)\rangle &\Rightarrow \phi(1,0) = \phi(3,0) = (13)(24) \\
\varphi(1,1)(x) = \varphi(3,1)(x) = ((1,1)+x) + \langle(2,0)\rangle &\Rightarrow \phi(1,1) = \phi(3,1) = (14)(23)
\end{aligned}$$

This subgroup of S_4 is isomorphic to

$$(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle(2,0)\rangle \cong \{id, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Definition 3.7 (direct sum of permutation representations)**.** Let G be a group and $U = G/H$, $\tilde{U} = G/\tilde{H}$ for some subgroups H, $\tilde{H}$. We define the direct sum of the two by H and $\tilde{H}$ induced transitive representations $\phi : G \to S_{|U|}$ and $\tilde{\phi} : G \to S_{|\tilde{U}|}$ as the homomorphism

$$\begin{aligned}
\phi \oplus \tilde{\phi} : G &\to S_{|U|} \times S_{|\tilde{U}|} \\
\phi \oplus \tilde{\phi} &= (\phi(g), \tilde{\phi}(g)).
\end{aligned}$$

$S_{|U|} \times S_{|\tilde{U}|} \subseteq S_{|U|+|\tilde{U}|}$, so we could also say $\phi \oplus \tilde{\phi} : G \to S_{|U|+|\tilde{U}|}$. We try to clarify this with the next example.

Example 3.5 (Representations of $\mathbb{Z}_4 \times \mathbb{Z}_2$). First we will note that we can construct the regular representation $\mathbb{Z}_4 \times \mathbb{Z}_2 \to S_8$. Now the question is, if we can use the above definition to construct a faithful representation into a smaller symmetric group. For this we use the subgroups $\langle(1,0)\rangle$ and $\langle(0,1)\rangle$. We note that $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle(1,0)\rangle \cong \mathbb{Z}_2$ and $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle(0,1)\rangle \cong \mathbb{Z}_4$. We already now the regular representation of $\mathbb{Z}_4$, from Example 3.3 and we can use this here. So we can construct a homomorphism $\phi \oplus \tilde{\phi} : \mathbb{Z}_4 \times \mathbb{Z}_2 \to S_{4+2}$.

$$\begin{aligned}
\phi \oplus \tilde{\phi}((0,0)) &= (id, id) \Rightarrow id \in S_6 \\
\phi \oplus \tilde{\phi}((0,1)) &= (id, (12)) \Rightarrow (56) \in S_6 \\
\phi \oplus \tilde{\phi}((1,0)) &= ((1234), id) \Rightarrow (1234) \in S_6 \\
\phi \oplus \tilde{\phi}((1,2)) &= ((1234), (12)) \Rightarrow (1234)(56) \in S_6 \\
\phi \oplus \tilde{\phi}((2,0)) &= ((13)(24), id) \Rightarrow (13)(24) \in S_6 \\
\phi \oplus \tilde{\phi}((2,1)) &= ((13)(24), (12)) \Rightarrow (13)(24)(56) \in S_6 \\
\phi \oplus \tilde{\phi}((3,0)) &= ((1432), id) \Rightarrow (1432) \in S_6 \\
\phi \oplus \tilde{\phi}((3,1)) &= ((1432), (12)) \Rightarrow (1432)(56) \in S_6
\end{aligned}$$

We found a faithful permutation representation into a smaller symmetric group.

$\mathbb{Z}_4 \times \mathbb{Z}_2 \cong \{id, (56), (1234), (1234)(56), (13)(24), (13)(24)(56), (1432), (1432)(56)\}$.

In Section 4 we will even show that this is already the minimal faithful permutation representation.

Obviously we can expand this definition. We call the homomorphism $\phi_1 \oplus \phi_2 \oplus ... \oplus \phi_n$ induced by $\{H_1, H_2, ...H_n\}$ if every ϕ_i is induced by H_i.

Now we will state a few Lemmas without proof. For more information see [Asc00].

Definition 3.8 (core of a subgroup)**.** Let G be a group. The core of a subgroup H is defined as

$$\begin{aligned} \text{core}_G(H) :&= \bigcap_{g \in G} H^g \\ H^g :&= \{h | ghg^{-1} \in H\}. \end{aligned}$$

Lemma 3.3. *Let G be a group. The representation induced by subgroups $H_1, ..., H_n$ is faithful if and only if $\bigcap_i^n \text{core}_G(H_i) = e_G$ ($H_i^g := \{h | h^g \in H_i\}$).*

In other words, the representation is faithful if and only if the largest normal subgroups of every subgroup H_i are disjoint.

Lemma 3.4. *Every permutation representation ϕ is induced by a set of subgroups $\{H_1, ..., H_k\}$. $\phi = \phi_{H_1} \oplus ... \oplus \phi_{H_k} : G \to S_m$, with $m = |\bigcup_{i=1}^k G/H_i|$. The representations ϕ_{H_i} are the transitive representations induced by the subgroups H_i.*

Definition 3.9 (degree of a representation)**.** Let G be a finite group and ϕ a representation induced by $H_1, ..., H_k$, we call $\deg(\phi) = \sum_{i=1}^k [G\colon H_i]$ the degree of the representation ϕ.

For example, the degree of the regular representation $\phi : G \hookrightarrow S_n$ is $|G| = n$, because ϕ is induced by $\{e\}$. We can now restate the definition of the minimal permutation degree.

Lemma 3.5 (minimal permutation degree)**.** *Let G be a finite group and $\mathcal{R}$ the set of all sets of subgroups of G, then the minimal permutation degree is*

$$d(G) = \min\{\sum_{H \in R} [G : H] | R \in \mathcal{R} : \bigcap_{H \in R} \text{core}_G(H) = e\}$$

This Lemma is a very powerful tool for finding minimal permuation degrees. We will see this in the next example.

Example 3.6. The Quaternion Group Q_8, has the 8 elements $\{\pm 1, \pm i, \pm j, \pm k\}$, with

$$i \cdot i = j \cdot j = k \cdot k = i \cdot j \cdot k = -1$$

The non-trivial subgroups are $\{\pm 1\}$, $\{\pm 1, \pm i\}$,$\{\pm 1, \pm j\}$,$\{\pm 1, \pm k\}$. $\{\pm 1\}$ is subgroup of all of them, therefore the minimal representation is induced by $\{1\}$ and so $\mathrm{d}(Q_8) = 8$.

4 Groups with minimal regular Representation

4.1 Cyclic p-Groups

Definition 4.1 (Cyclic p-Group)**.** A cyclic p-group is a cyclic group $\mathbb{Z}_{p^m}$ with order p^m, where p is a prime number and $m \in \mathbb{N}$.

We already can solve $\mathrm{d}(\mathbb{Z}_p)$, because Lagrange's Theorem assures us that there can't be a non-trivial subgroup, and therefore the regular representation already has to be minimal. So $\mathrm{d}(\mathbb{Z}_p) = p$. To get a better overview of what we want to proof, we can look at the example $\mathbb{Z}_8$.

Example 4.1 ($\mathbb{Z}_8$). The group has the elements $\{0, 1, 2, 3, 4, 5, 6, 7\}$ and the non-trivial subgroups are $\{0, 4\}$ and $\{0, 2, 4, 6\}$. We can see that $\{0\} \subset \{0, 4\} \subset \{0, 2, 4, 6\} \subset \{0, 1, 2, 3, 4, 5, 6, 7\}$ and so the only set with $\{0\}$ as intersection is $\{0\}$ itself, therefore we get as minimal homomorphism the homomorphism induced by $\{0\}$, which is the regular representation.

We now try to generalize this and show that every cyclic group of order p^m has such a subgroup structure. This is kind of intuitive if we think about Lagrange's Theorem, and we note that the only orders of the possible subgroups therefore are $p \mid p^2 \mid p^3 \mid ... \mid p^m$. We already know that those subgroups are cyclic, we just have to show that they exist and form a subgroup series.

Lemma 4.1. *Let G be a cyclic group of order n and $d \mid n$, then there exists a group of order d.*

Proof. Let $\langle g \rangle$ be a generator, then we can write a element of order d as $g^{\frac{m}{d}}$ because $(g^{\frac{m}{d}})^d = g^m = e$. Therefore $\langle g^{\frac{m}{d}} \rangle$ is a subgroup of G of order d. □

Corollary 4.2. *Let G be a cyclic group and H_1 and H_2 two subgroups of G. It is $H_1 \subset H_2$ if $|H_1| \mid |H_2|$.*

Proof. We know that H_1 and H_2 are cyclic because of Lemma 2.2. Suppose $|H_1| \mid |H_2|$, then we know from Lemma 4.1 that H_2 has a subgroup M of order

$|H_1|$. Let n be the order of G and $\langle g \rangle$ a generator. Let d_1 be the order of H_1 and d_2 the order of H_2. An element of G with order d_1 is $g^{\frac{n}{d_1}}$, so $\langle g^{\frac{n}{d_1}} \rangle$ is the only subgroup of order d_1, therefore $M{=}H_1$. □

We showed now that the subgroups of $\mathbb{Z}_{p^m}$ generated by g have to fulfill, $\langle g \rangle \subset \langle g^p \rangle \subset \langle g^{p^2} \rangle \subset ... \subset \langle g^{p^{m-1}} \rangle \subset \{e\}$. Therefore the regular representation is minimal and $\mathrm{d}(\mathbb{Z}_{p^m}) = p^m$.

Example 4.2 (All groups of order 2017). 2017 is a prime Number. As a result of Lagrange's Theorem every group of order 2017 has to be isomorphic to $\mathbb{Z}_{2017}$. Therefore the minimal permutation degree is,

$$\mathrm{d}(\mathbb{Z}_{2017}) = 2017.$$

4.2 Klein Four-Group

The Klein Four-group can be written as $\mathbb{Z}_2 \times \mathbb{Z}_2$, with the elements $\{(0,0),(0,1),(1,0),(1,1)\}$. The subgroups are $H_1 = \{(0,0)\}$, $H_2 = \{(0,0),(0,1)\}$, $H_3 = \{(0,0),(1,0)\}$ and $H_4 = \{(0,0),(1,1)\}$. We get four notable faithful representations.
ϕ_1 induced by H_1, this is the regular permutation, therefore $deg(\phi_1) = 4$
ϕ_2 induced by $\{H_2, H_3\}$, $deg(\phi_2) = [G\colon H_2] + [G\colon H_3] = 2 + 2 = 4$
ϕ_3 induced by $\{H_2, H_4\}$, $deg(\phi_3) = [G\colon H_2] + [G\colon H_4] = 2 + 2 = 4$
ϕ_4 induced by $\{H_3, H_4\}$, $deg(\phi_4) = [G\colon H_3] + [G\colon H_4] = 2 + 2 = 4$
All other faithul representations can't be minimal because the inducing set would contain one of the inducing sets above. For example ϕ_5 induced by $\{H_2, H_3, H_4\}$ is faithful, but can't be minimal because $\{H_2, H_3\} \subset \{H_2, H_3, H_4\}$.
So we conclude that $\mathrm{d}(G) = 4$ and the regular representation is minimal, but not unique.

4.3 Generalized Quaternion Groups

In this section we will show that the regular representations of the Generalized Quaternion Groups are minimal. The most important source for this chapter is [Con10].

4.3.1 The Quaternion Group Q_8

We already used Q_8 as Example 3.6 and showed, that $\mathrm{d}(Q_8) = 8$. Nevertheless it is worth it to look at this group a second time and try to find a way to link it to cyclic groups. This will help us to define and understand the generalized quaternion groups later. We are constructing a group and show that this group is isomorphic to Q_8. Recall that we defined the Quaternion Group Q_8 as

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, with the condition $i \cdot i = j \cdot j = k \cdot k = i \cdot j \cdot k = -1$ and the usual rule of signs. Q_8 is a non-abelian group with the center $Z(G) = \{\pm 1\}$.

Lemma 4.3. *We define $H = \mathbb{Z}_4 \rtimes \mathbb{Z}_4$, and the semidirect product as*

$$(a, b)(c, d) = (a + (-1)^b c, b + d).$$

Then the quotient group with $\langle (2, 2) \rangle$ is isomorphic to Q_8, i.e.

$$H/\langle (2, 2) \rangle \cong Q_8.$$

Proof. First we note that the order of $\langle (2, 2) \rangle$ is 2.

$$(2, 2)^2 = (2 + (-1)^2 2, 2 + 2) = (0, 0)$$

This already shows us that the order of $H/\langle (2, 2) \rangle$ is $\frac{|H|}{|\langle (2,2) \rangle|} = \frac{16}{2} = 8$. We note that H is generated by $\langle (1, 0), (0, 1) \rangle$, because $(1, 0)^a (0, 1)^b = (a, 0)(0, b) = (a, b)$ for every element (a, b).
The elements of $H/\langle (2, 2) \rangle$ are

$$\{[(0, 0)], [(0, 1)], [(1, 0)], [(1, 1)], [(0, 2)], [(1, 2)], [(2, 1)], [(1, 3)]\}$$

and it is generated by $\langle [(0, 1)], [(1, 0)] \rangle$.
We will now define a homomorphism from H to Q_8. First we note that Q_8 is generated by $\{i, j\}$ because

$$\begin{aligned} i \cdot j \cdot k &= -1, \\ i \cdot j \cdot k \cdot -k &= -1 \cdot -k, \\ i \cdot j &= k. \end{aligned}$$

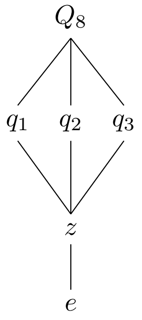
So we define the homomorphism $\phi : H \to Q_8$ as $\phi(a, b) = i^a \cdot j^b$. This is a homomorphism because

$$\begin{aligned} \phi((a, b)(c, d)) = \phi(a + (-1)^b c, b + d) = i^{a+(-1)^b c} j^{b+d} = \\ = i^a i^{(-1)^b c} j^b j^d = i^a j^b i^c j^{-b} j^b j^d = i^a j^b i^c j^d = \phi((a, b))\phi((c, d)) \end{aligned}$$

The only step we have to justify is $i^{(-1)^b c} = j^b i^c j^{-b}$. For b even it is easy to see. For b odd we have to show the conjugacy relation $jij^{-1} = i^{-1}$. We can use $k^2 = -1$. We already stated that this is $ijij = -1$, if we multiply this with i from the left it is $-jij = -i$, which is (because -1 is in the center of Q_8) the same as $ji(-j) = -i = i^{-1} = jij^{-1}$.
We note that the image has to be Q_8, because $\phi(1, 0) = i$ and $\phi(0, 1) = j$. The

kernel of ϕ is $\text{core}(\phi) = \{(0,0),(2,2)\}$, because $\phi((2,2)) = i^2j^2 = -1 \cdot -1 = 1$. So ϕ induces an epimorphism $\tilde{\phi} : H/\langle(2,2)\rangle \to Q_8$. Those two groups have the same size, so it has to be an isomorphism and we can state $H/\langle(2,2)\rangle \cong Q_8$. □

From now on we will denote Q_8 by $H/\langle(2,2)\rangle$. Since we already discussed the subgroup structure we can visualize it.



Name	**Elements**
Q_8	$\{[(0,0)],[(0,1)],[(1,0)],[(1,1)],$ $[(0,2)],[(1,2)],[(2,1)],[(1,3)]\}$
q_1	$\{[(0,0)],[(0,2)],[(1,0)],[(1,2)]\}$
q_2	$\{[(0,0)],[(0,2)],[(0,1)],[(2,1)]\}$
q_3	$\{[(0,0)],[(0,2)],[(1,1)],[(1,3)]\}$
z	$\{[(0,0)],[(0,2)]\}$
e	$\{[(0,0)]\}$

4.3.2 Generalized Quaternion Groups Q_{2^n}

Now the work we did for Q_8 pays off, because the idea of $H/\langle(2,2)\rangle$ can be generalized.

Definition 4.2 (generalized quaternion groups)**.** For $n \geq 3$ we define:

$$Q_{2^n} = (\mathbb{Z}_{2^{n-1}} \rtimes \mathbb{Z}_4)/\langle(2^{n-2},2)\rangle,$$

with the semi direct product

$$(a,b)(c,d) = (a + (-1)^b c, b + d).$$

We call these groups generalized quaternion groups.

The order of the generalized quaternion groups is $\frac{|\mathbb{Z}_{2^{n-1}}||\mathbb{Z}_4|}{|\langle(2^{n-1},2)\rangle|} = \frac{2^{n-1}4}{2} = 2^n$. So the generalized quaternion groups are 2-groups and we can use Sylow's First Theorem to see that there has to be a subgroup of order 2. We can even write a subgroup of order 2 down because for every generalized quaternion group $\{[(0,0)],[(2^{n-2},0)]\}$ is a subgroup. Note that in the previous chapter we used $[(0,2)]$ to generate the subgroup of order 2,but this is the same element as $[(2,0)]$ because $(0,2) = (2,0)(2,2)$. In general it is $[(2^{n-2},0)] = [(0,2)]$ because of $(0,2) = (2^{n-2},0)(2^{n-2},2)$. If this is the only element of order 2 we can conclude that the regular representation is minimal. This is because Lagrange's Theorem tells us that the order of the subgroups has to divide the group order, so the (non-trivial) subgroup orders have to be 2^s for $1 \leq s \leq n$. Then the subgroups are themselves 2-groups and we can use Sylow's First Theorem to state that they have to have a subgroup of order 2.

Lemma 4.4. *In every generalized quaternion group* $[(2^{n-2}, 0)]$ *is the only element of order* 2.

Proof. $\mathbb{Z}_{2^{n-1}} \rtimes \mathbb{Z}_4$ is generated by $(1,0), (0,1)$ and we can write every element as $(1,0)^a(0,1)^b$. Therefore every element in Q_{2^n} can be written as $[(1,0)]^a[(0,1)]^b$. If $b = 2$ we can write $[(1,0)]^a[(0,1)]^2 = [(a,2)][(2^{n-2,2})] = [a + 2^{n-2}, 0]$ and the element is in $\langle[(1,0)]\rangle$. If $b = 3$ we can write $[(1,0)]^a[(0,1)]^3 = [(a,3)][(2^n - 1, 2)] = [a + 2^n - 1, 1]$, so it could also be written as $[(1,0)]^{a+2^{n-2}}[(0,1)]$. We conclude that every element of Q_{2^n} can be written as $[(1,0)]^a$, or $[(1,0)]^a[(0,1)]$. There exists just one element of order 2 of the form $[(1,0)]^a$ and this is the already known $[(2^{n-2}, 0)]$. So if there is another element of order 2 it has to be of the form $[(1,0)]^a[(0,1)]$.

$$\begin{aligned}
&([(1,0)]^a[(0,1)])^2 = [(a,0)][(0,1)][(a,0)][(0,1)] = \\
&\qquad = [(a,0)][(-a,1)][(0,1)] = [(a,0)][(-a,0)][(0,1)][(0,1)] = [(0,2)].
\end{aligned}$$

So elements of this form can't be of order 2. In fact we proved that they have to be of order 4, because we already showed that $[(0,2)] = [(2^{n-2}, 0)]$. □

We indicated that there is a unique element of order 2 and therefore a unique subgroup of order 2 generated from this element and we can conlude that every (non-trivial) subgroup has to contain $\{[(0,0)], [(2^{n-1}, 0)]\}$. The regular representation is therefore minimal and we can deduce that $\mathrm{d}(Q_{2^n}) = 2^n$.

4.4 Completeness

In this section we will show that all groups with minimal regular representation are one of the above.

Theorem 4.5. *A group satisfies* $\mathrm{d}(G) = |G|$ *if and only if it is one of the following:*

- *A Cyclic group with order* p^m*, with* p *prime number and* $m \in \mathbb{N}$
- *The Klein Four-Group*
- *A generalized Quaternion Group.*

Proof. There can't be two distinct primes, so a group with minimal regular representation has to be a p-group. Now suppose $p \neq 2$, then it has a unique subgroup of order p and is a Cyclic Group. Now suppose $p = 2$, then if there is an element g of order 4, then g^2 must be the unique element of order 2 and it has to be a Cyclic Group $\mathbb{Z}_{2^m}$ or a generalized Quaternion Group. If there is no element of order 4, then it has to be an elementary abelian 2-group. We will show in the next section that $\mathrm{d}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times ... \times \mathbb{Z}_2) = 2n$, n being the number of $\mathbb{Z}_2$. So it just can be one or two times $\mathbb{Z}_2$. So it is either $\mathbb{Z}_2$ itself or the Klein-Four Group. □

5 Minimal Permutation Degree of finite Abelian Groups

In this section we want to find a general valid formula to calculate the minimal permuatation degree of finite abelian groups. The most important source for this section is [D L71, s.860-s.862]. We will start with proving some general results for direct products, because knowing how the minimal permutation degree and direct products interact will help us a lot to prove the formula for the minimal permutation degree of abelian groups.

5.1 Direct Products

Theorem 5.1. *For any two finite groups G and H, the following inequality holds*

$$\mathrm{d}(G \times H) \leq \mathrm{d}(G) + \mathrm{d}(H)$$

Proof. Let ϕ_1 be the minimal faithful representation induced by $\{G_1, G_2, ..., G_n\}$, with $G_i \subset G$ and ϕ_2 be the minimal faithful representation induced by $\{H_1, H_2, ..., H_m\}$, with $H_i \subset H$. Then the representation ϕ induced by $\{G_1 \times H, ..., G_n \times H, G \times H_1, ..., G \times H_m\}$ is a representation of $G \times H$.

$$\deg(\phi) = \sum_{i=1}^{n} [G \times H : G_i \times H] + \sum_{j=1}^{m} [G \times H : G \times H_j] =$$

$$= \sum_{i=1}^{n} [G : G_i] + \sum_{j=1}^{m} [H : H_i] = \deg(\phi_1) + \deg(\phi_2)$$

This has to be a upper bound for $\mathrm{d}(G \times H)$ because

$$\mathrm{d}(G) + \mathrm{d}(H) = \deg(\phi_1) + \deg(\phi_2) = \deg(\phi) \geq \mathrm{d}(G \times H)$$

□

Lemma 5.2. *For two finite Groups G and H, with* $\gcd(|G|, |H|) = 1$ *it is*

$$\mathrm{d}(G \times H) = \mathrm{d}(G) + \mathrm{d}(H)$$

Proof. We already showed $\mathrm{d}(G \times H) \leq \mathrm{d}(G) + \mathrm{d}(H)$ generally, so we just have to proof $\mathrm{d}(G \times H) \geq \mathrm{d}(G) + \mathrm{d}(H)$. Let ϕ_{min} be the minimal faithful representation for $G \times H$ induced by some set of subgroups $M = \{M_1, M_2, ..., M_n\}$. By Lagrange's Theorem we know that the order of any subgroup has to divide the order of the group. Therefore the subgroups of G and H have to be distinct. We can conclude that for all $1 \leq i \leq n$ there are subgroups $G_i \subseteq G$ and $H_i \subseteq H$ with

$$M_i = H_i \times G_i = (G_i \times H) \cap (G \times H_i)$$

That means that the transitive representation θ induced by $M \backslash M_i \cup \{(G_i \times H), (G \times H_i)\}$ is also a faithful representation. ϕ_{min} has minimal degree so

$$\begin{aligned} \mathrm{d}(\theta) &\geq \mathrm{d}(\phi_{min}) \\ \sum_{j=1}^{i-1} [G \times H \colon M_j] + [G \times H \colon G_i \times H] + & \\ [G \times H : G \times H_i] + \sum_{k=i+1}^{n} [G \times H \colon M_k] &\geq \sum_{l=1}^{n} [G \times H \colon G_l \times H_l] \\ [G \times H \colon G_i \times H] + [G \times H \colon G \times H_i] &\geq [G \times H \colon G_i \times H_i] \\ [G \colon G_i] + [H \colon H_i] &\geq [G \colon G_i] \cdot [H \colon H_i]. \end{aligned}$$

This inequality just holds for $[G \colon G_i] = 1$, $[H \colon H_i] = 1$ or $[G \colon G_i] = [H \colon H_i] = 2$. Because of $\gcd(|G|, |H|) = 1$ it has to be either $[G \colon G_i] = 1$ or $[H \colon H_i] = 1$. So every M_i has to have the form $G_i \times H$ or $G \times H_i$. Let $M_G = \{G_i | \forall i : M_i \text{ is of the form } G_i \times H\}$ and $H_G = \{H_i | \forall i : M_i \text{ is of the form } G \times H_i\}$. If $N \lhd G$ is in every element of M_G, it has to be in every element of the subset of subgroups that induces the minimal faithful representation. So $N = \{e\}$ and M_G induces a faithful representation of G. The same argument wokrs for H and M_H. Therefore

$$\mathrm{d}(G \times H) = \deg(M) = \deg(M_G) + \deg(H_G) \geq \mathrm{d}(G) + \mathrm{d}(H).$$

□

5.2 Abelian Groups

Theorem 5.3 (Fundamental Theorem of Finite Abelian Groups)**.** *Every finite abelian group is a unique direct product of cyclic p-groups.*

In the proof of this Theorem one shows first that every abelian group is a unique direct product of p-groups by induction. Furthermore we show by induction, that every p-group itself is a direct product of cyclic p-groups. A detailed proof can be found in [Nav03].

Lemma 5.4. *For an arbitrary minimal representation $\phi_{\mathcal{G}}$ of a group G induced by $\mathcal{G} = \{G_1, ..., G_n\}$, there exists a minimal representation $\phi_{\mathcal{H}}$ induced by $\mathcal{H}$ with the properties that every inducing element is primitive and $G_i \in \mathcal{H}$ if $[G\colon G_i] = 2n + 1$ for an $n \in \mathbb{N}_0$.*

Proof. Suppose that G_i is not primitive, then $G_i = H \cap K$, with $G_i \subset H$, $K \subseteq G$. This means that $\mathcal{H}' = \{G_1, ..., G_{i-1}, H, K, G_{i+1}, ..., G_n\}$ is also faithful. The degree is

$$\deg(\mathcal{H}') = \mathrm{d}(G) - [G\colon G_i] + [G\colon H] + [G\colon K] \geq \mathrm{d}(G)$$
$$[G\colon H] + [G\colon K] = \frac{[G\colon G_i]}{[G_i\colon H} + \frac{[G\colon G_i]}{[G_i\colon K]} \geq [G\colon G_i]$$

Therefore $[G_i\colon H] = [G_i\colon K] = 2$, proving that $[G\colon G_i]$ is even and that H is minimal. If another element is not primitive we can repeat the steps with this element, after a finite amount of steps we will have a minimal representation with the desired properties. □

Theorem 5.5. *Let G be a finite abelian group and $G \cong \prod_{i=1}^{n} \mathbb{Z}_{p_i^{e_i}}$ the unique primary decomposition. Then the minimal permutation degree is*

$$\mathrm{d}(G) = \sum_{i=1}^{n} {p_i}^{e_i}$$

Proof. We now have to show the equality $\mathrm{d}(G \times H) = \mathrm{d}(G) + \mathrm{d}(H)$ for abelian p-groups, this is sufficient for all abelian groups, because we already proved the additivity for coprime groups in Lemma 5.2. We show it for abelian p-groups by induction. To prepare for the induction we sort the summands $\sum_{i=1}^{n} {p_i}^{e_i} = \sum_{i=1}^{n} g_i$, such that $g_1 \geq g_2 \geq ... \geq g_n$. Now we make the induction on n, for n=1 it is a cyclic prime-power-order group, with $\mathrm{d}(G) = g_1 = {p_1}^{e_1}$. Let ϕ induced by $\mathcal{B} = \{B_1, ..., B_m\}$ be a faithful minimal permutation of G with primitive elements and $[G : B_i] = 2n + 1$ for an $n \in \mathbb{N}_0$, so that G/B_i is cyclic. The order of G/B_i is b_i with $b_1 \geq b_2 \geq ... \geq b_m$ for all $1 \leq i \leq m$. Therefore $g_1 \geq$b$_1$, but if g_1 were equal to b_1, the kernel of ϕ couldn't be trivial and the representation couldn't be faithful. So it has to be $b_1 = g_1$ and let bB_1 be a generator of G/B_1, then $G = \langle b \rangle \times B_1$. $\{B_1 \cap B_2, ..., B_1 \cap B_m\}$ is inducing a faithful representation of B_1, so that

$$\begin{aligned}
\mathrm{d}(G) &\leq g_1 + \mathrm{d}(B_1) \\
&\leq g_1 + [B_1\colon B_1 \cap B_2] + ... + [B_1\colon B_1 \cap B_m] \\
&= g_1 + [B_1B_2\colon B_2] + ... + [B_1B_m\colon B_m] \\
&\leq g_1 + [G\colon B_2] + ... + [G\colon B_m] \\
&= \mathrm{d}(G).
\end{aligned}$$

So $\mathrm{d}(G) = g_1 + \mathrm{d}(B_1)$, but $B_1 \cong G_2 \times ... \times G_n$ by Theorem 2.5 (Krull-Schmidt). So by induction $\mathrm{d}(B_1) = g_2 + ... + g_n$. Therefore it is $\mathrm{d}(G) = \sum_{i=1}^{n} g_i = \sum_{i=1}^{n} {p_i}^{e_i}$ □

Example 5.1 ($\mathrm{d}(\mathbb{Z}_{1729})$). The prime factorization of 1729 is $7 \cdot 13 \cdot 19$. Therefore we get $\mathbb{Z}_{1729} \cong \mathbb{Z}_7 \times \mathbb{Z}_{13} \times \mathbb{Z}_{19}$. Theorem 5.5 now tells us that the minimal permutation degree is

$$\mathrm{d}(\mathbb{Z}_{1729}) = \mathrm{d}(\mathbb{Z}_7 \times \mathbb{Z}_{13} \times \mathbb{Z}_{19}) = 7 + 13 + 19 = 39.$$

6 Minimal Permutation Degree of Semidirect Products

The most important source for this section is [Hen16, s.16-23]. We start with recalling the definition of a semidirect Product.

Definition 6.1 ((internal) semidirect product)**.** Let $N \lhd G$ be a normal subgroup of a group G and let H be a subgroup of G, such that $NH = G$ and $N \cap H = e_G$. Then we call G the (internal) semidirect product of N and H. We write $G = N \rtimes H$

Definition 6.2 ((external) semidirect product)**.** For two groups G and H, a homomorphism $\theta_{h_1} : H \to \mathrm{Aut}(G)$, we define the (external) semidirect product $G \rtimes_{\theta_{h_1}} H$ as

$$(g_1, h_1)(g_2, h_2) = (g_1\theta_{h_1}(g_2), h_1h_2).$$

Note that $G \rtimes_{\theta_{h_1}} H$ forms a group, with $e_{G \rtimes_{\theta_{h_1}} H} = (e_G, e_H)$ and the inverse of an element $(g, h)^{-1} = (\theta_{h_1}^{-1}(g^{-1}), (h^{-1}))$. The semidirect product is a generalization of the direct product, for $\theta_{h_1} = id$ we get the direct product.

Lemma 6.1. *For G and H nontrivial finite groups, the following inequality is true:*

$$\mathrm{d}(G \rtimes H) \leq |G| + \mathrm{d}(H)$$

Proof. We define a function $\phi : G \rtimes_{\theta_{h_1}} H \to S_{|H|} \times H$ with $\phi(g,h) = (g\theta_h(x), h)$. Now we show that this is a monomorphism. It is a homomorphism, because

$$\begin{aligned}\phi((g_1,g_2)(h_1,h_2)) = \phi(g_1\theta_{h_1}(g_2), h_1h_2) = \\ = (g_1\theta_{h_1}(g_2\theta_{h_1h_2}(x)), h_1h_2) = \\ = (g_1\theta_{h_1}(x), h_1)(g_2\theta_{h_2}(x), h_2) = \phi((g_1,g_2))\phi((h_1,h_2)).\end{aligned}$$

Furthermore it is injective, because $\phi(g,h) = (id, e_H)$ requires $h = e_H$ and $g\theta_h(x) = id$, so $g = e_G$. Therefore the core is trivial and ϕ a monomorphism. □

6.1 Semidirect Products of Cyclic p-Groups

We will now provide a formula to calculate the minimal permutation degree for a specific class of semidirect products, namely for the semidirect product of two cyclic p-groups.

Theorem 6.2. *Let $\mathbb{Z}_{p^n} \rtimes_\theta \mathbb{Z}_{q^m}$ be a semidirect product with p, q distinct primes, then*

$$\mathrm{d}(\mathbb{Z}_{p^n} \rtimes_\theta \mathbb{Z}_{q^m}) = \begin{cases} p^n, & \text{if } \theta \text{ injective} \\ p^n + p^m, & \text{if } \theta \text{ not injective} \end{cases}$$

Proof. Let a be a generator of $\mathbb{Z}_{p^n}$ and b a generator of $\mathbb{Z}_{q^m}$. $d(\mathbb{Z}_{p^n} \rtimes \mathbb{Z}_{q^m})$ contains a subgroup isomorphic to $\mathbb{Z}_{p^n}$, therefore $p^n \leq d(\mathbb{Z}_{p^n} \rtimes \mathbb{Z}_{q^m})$. We can interpret $\mathbb{Z}_{p^n} \rtimes_\theta \mathbb{Z}_{q^m}$ as the internal semidirect product of $\mathbb{Z}_{p^n}$ and $\mathbb{Z}_{q^m}$, because p and q are distinct primes.

First we look at the case θ injective. We can look at the conjugation $x^{-1}yxy^{-1}$, with $x \in \mathbb{Z}_{p^n}$ and y element from a normal subgroup of $\mathbb{Z}_{p^n} \rtimes \mathbb{Z}_{q^m}$ that is subgroup of $\langle b \rangle$. Then $x^{-1}yxy^{-1} \in \langle a \rangle \cap \langle b \rangle$, but $\langle a \rangle \cap \langle b \rangle = 1$. Then $yxy^{-1} = x$ and we conclude that $y \in \mathrm{core}(\theta)$. θ is injective so we get $y = 1$. Hence we get a faithful representation of degree $[G : \langle b \rangle] = p^n$.

Now suppose θ is not injective, then $\mathrm{core}(\theta)$ is not-trivial and there is a non trivial normal subgroup of $(\langle a \rangle)$, the non trivial subgroups are of order p^s $1 \leq s \leq m$, so we can conclude $\theta(b)^{q^m - 1} = id \in Aut(\langle a \rangle)$. From this we can conclude that $\langle a \rangle$ and $\langle b \rangle$ are normal and the unique subgroups of $\mathbb{Z}_{p^n} \rtimes_\theta \mathbb{Z}_{q^m}$ with order p, q. Therefore there must be at least two groups of at least index p^n and p^m to induce the minimal representation. So the lower bound has to be $p^n + p^m$.

The faithful representation ϕ induced by $\{\langle a \rangle, \langle b \rangle\}$ has degree

$$\deg(\phi) = [\mathbb{Z}_{p^n} \rtimes_\theta \mathbb{Z}_{q^m} : \langle a \rangle] + [\mathbb{Z}_{p^n} \rtimes_\theta \mathbb{Z}_{q^m} : \langle b \rangle] = p^m + p^n.$$

So we get $\deg(\phi) = d(\mathbb{Z}_{p^n} \rtimes_\theta \mathbb{Z}_{q^m}) = p^m + p^n$ □

Our final example will be the calculation of the minimal permutation degree for all groups of order 2019. For this we will need the results from Theorem 5.5 and from our final Theorem 6.2.

Example 6.1 (Groups of Order 2019)*.* 2019 is semiprime because the prime factorization of 2019 is just a product of two primes $2019 = 673 \cdot 3$. There are always either one abelian group or two (one abelian and one non-abelian) groups of semiprime order. The abelian group of order 2019 is $\mathbb{Z}_{2019} \cong \mathbb{Z}_{673} \times \mathbb{Z}_3$. The minimal permutation degree of this group is

$$d(\mathbb{Z}_{673} \times \mathbb{Z}_3) = d(\mathbb{Z}_{673}) + d(\mathbb{Z}_3) = 673 + 3 = 676.$$

A conclusion of Sylow's Theorem is, that if p and q are prime numbers with $p < q$ and $p \nmid (q-1)$ every finite group of order $|G| = p \cdot q$ is isomorphic to $\mathbb{Z}_{p \cdot q}$. But $3 \mid (673-1)$ so there can be a distinct group of order 2019. This group has to be non-abelian and is a semidirect product (with $\theta(h) = h^{-1}$) of $\mathbb{Z}_{673} \rtimes H$ where H is a subgroup of $\mathbb{Z}_{673}$ with 3 elements. H has to be $\{1, h, h^{-1}\}$ for elements $h, h^{-1} \in \mathbb{Z}_{673}$ and $h \cdot h^{-1} = 1$. The group product of two elements (g_1, h_1) and (g_2, h_2) is $(g_1 + h_2^{-1} g_2, h_1 h_2)$. This group is non-abelian and has order 2019. θ is injective, therefore the minimal permutation degree of $\mathbb{Z}_{673} \rtimes H$ is

$$d(\mathbb{Z}_{673} \rtimes H) = d(\mathbb{Z}_{673}) = 673.$$

References

[Asc00] M. Aschbacher. *Finite Group Theory*. 2nd ed. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2000.

[Bec12] Becker, Oren. *The minimal degree of permutation representations of finite groups*. 2012. URL: https://arxiv.org/pdf/1204.1668.pdf.

[Bur17] Dietrich Burde. *Group Theory*. 2017. URL: https://homepage.univie.ac.at/Dietrich.Burde/papers/burde_54_groups.pdf.

[Con10] Keith T. Conrad. *GENERALIZED QUATERNIONS*. 2010. URL: https://kconrad.math.uconn.edu/blurbs/grouptheory/genquat.pdf.

[D L71] D. L. Johnson. “Minimal permutation of Finite Groups”. In: *American Journal of Mathematics* 93.4 (Oct. 1971).

[EP88] David Easdown and Cheryl E. Praeger. “On minimal faithful permutation representations of finite groups”. In: *Bulletin of the Australian Mathematical Society* 38.2 (1988), pp. 207–220.

[Hen16] Hendriksen, Michael. *Minimal Permutation Representations of Classes of Semidirect Products of Groups*. 2016. URL: https://ses.library.usyd.edu.au/bitstream/handle/2123/14353/Hendriksen_MA_thesis.pdf.

[Hun12] T.W. Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2012. URL: https://books.google.at/books?id=e-YlBQAAQBAJ.

[JS05] J.C. Jantzen and J. Schwermer. *Algebra*. Springer-Lehrbuch. Springer, 2005. URL: https://books.google.at/books?id=Fx%5C_1SXB78zkC.

[KP00] L. G. Kovács and Cheryl E. Praeger. “On minimal faithful permutation representations of finite groups”. In: *Bulletin of the Australian Mathematical Society* 62.2 (2000), pp. 311–317.

[Nav03] Gabriel Navarro. “On the Fundamental Theorem of Finite Abelian Groups”. In: *The American Mathematical Monthly* 110.2 (2003), pp. 153–154. URL: http://www.jstor.org/stable/3647777.

[Nei12] Neil Saunders. *Minimal faithful permutation degrees of finite groups*. 2012. URL: https://www.austms.org.au/Publ/Gazette/2008/Nov08/TechPaperSaunders.pdf.

[Wri75] D. Wright. “Degrees of Minimal Embeddings for Some Direct Products”. In: *American Journal of Mathematics* 97.4 (1975), pp. 897–903. URL: http://www.jstor.org/stable/2373679.