# On $p$-groups of low power order

Gustav Sædén Ståhl
gss@kth.se

Johan Laine
johlaine@kth.se

Gustav Behm
gbehm@kth.se

Student advisor:
Mats Boij
boij@kth.se

Department of Mathematics
KTH

2010

**Abstract**

We know that groups of order $p$, where $p$ is a prime, are cyclic and are all isomorphic to $Z_p$. That there are only two groups of order $p^2$ up to isomorphisms, both of them abelian is also a well known fact. To continue this procedure we will in chapter one classify the structures of $p$-groups of order $p^3$ and $p^4$. The structure theorem of abelian groups tells us everything about structuring the abelian $p$-groups as direct products and so we will define another structure operation, namely the semi-direct product, in order to structure the non-abelian ones as well. We conclude that there are five non-isomorphic groups of order $p^3$, three of those being abelian. Furthermore, when $p > 3$, we find a semi-direct product for all non-isomorphic $p$-groups of order $p^4$ for which there are 15. Since the semi-direct product uses the automorphism groups of the groups it takes as arguments we will also study the automorphism groups of the $p$-groups of order $p^2$ and $p^3$.

Chapter two will deal with the subgroup structure of the groups discussed in chapter one. We will determine the number of subgroups in each group as well as acquire some knowledge of the relation between the different subgroups. Our approach will be combinatorial, using presentations. The purpose of the final chapter is to study the representations of the non-abelian $p$-groups of order $p^3$ and $p^4$ through their character tables. Methods for obtaining these characters are both lifting characters of abelian subgroups and by use of the orthogonality relations. The conjugacy classes of these groups will be calculated and a short introduction to representation theory will also be given.

**Sammanfattning**

Vi vet att grupper av ordning $p$, där $p$ är ett primtal, är cykliska och alla är isomorfa med $Z_p$. Att det finns två olika grupper av ordning $p^2$ upp till isomorfi, där de båda är abelska, är också ett känt faktum. För att fortsätta i detta spår kommer vi i kapitel ett att klassisficera strukturerna av $p$-grupper med ordning $p^3$ resp. $p^4$. Struktursatsen för ändligt genererade abelska grupper säger redan allt om att strukturera de abelska $p$-grupperna som direkta produkter och vi kommer att definiera en annan struktur-operation, den semi-direkta produkten, för att strukturera även de icke-abelska. Vi visar att det finns fem icke-isomorfa grupper av ordning $p^3$, därav tre stycken abelska. Vidare, när $p > 3$, finner vi semi-direkta produkter för alla icke-isomorfa $p$-grupper av ordning $p^4$, av vilka det finns 15 stycken. Eftersom den semi-direkta produkten använder automorfigrupperna av de grupper som den tar som argument kommer vi även att studera automorfigrupperna av $p$-grupperna av ordning $p^2$ och $p^3$.

Kapitel två behandlar delgruppsstrukturen hos de grupper som beaktades i kapitel ett. Vi beräknar antalet delgrupper för varje grupp samt undersöker hur de förhåller sig med varandra. Vårt tillvägagångssätt kommer vara kombinatoriskt, och använder sig av presentationer. Syftet med det sista kapitlet är att studera representationerna av de icke-abelska $p$-grupperna av ordning $p^3$ och $p^4$ med hjälp av deras karaktärstabeller. Metoderna för att hitta dessa är både att lyfta karaktärerna av de abelska delgrupperna samt använda sig av ortogonalitetsrelationerna. Konjugatklasserna av dessa grupper kommer beräknas och en kort introduktion till representationsteori kommer också att ges.

# Notation

| | |
|---|---|
| $A \triangleq B$ | $A$ is defined as $B$ |
| $H \leq G$ | $H$ is a subgroup of $G$ |
| $H \trianglelefteq G$ | $H$ is a normal subgroup of $G$ |
| $Z(G)$ | The center of $G$ |
| $H \cong K$ | $H$ is isomorphic to $K$ |
| $\ker(\varphi)$ | The kernel of $\varphi$ |
| $\mathrm{im}(\varphi)$ | The image of $\varphi$ |
| $\mathrm{Aut}(G)$ | The automorphism group of the group $G$ |
| $G \times H$ | The direct product of $G$ and $H$ |
| $Z_n^r$ | The group $\underbrace{Z_n \times Z_n \times \ldots \times Z_n}_{r}$ |
| $G \rtimes_\varphi H$ | The semi-direct product of $G$ and $H$ with respect to $\varphi$ |
| $[x, y]$ | The commutator of $x$ and $y$ |
| $G'$ | The commutator subgroup of $G$ |
| $g \leftrightarrow h$ | $g$ is isomorphically related to $h$ (cf. p. 16) |
| $f \circ g$ | The composition of the mappings $f$ and $g$ |
| $Z_n$ | The cyclic group of order $n$ |
| $\mathbb{Z}_n$ | The cyclic group of integers of order $n$ |
| $\mathbb{Z}_n^*$ | The multiplicative group of $\mathbb{Z}_n$ |
| $\mathbb{F}_n$ | The finite field of $n$ elements |
| $GL_n(\mathbb{F}_m)$ | The general linear group over $\mathbb{F}_m$ |
| $Q_8$ | The quaternion group of order 8 |
| $D_{2n}$ | The dihedral group of order $2n$ |
| $G = \langle \ldots : \ldots \rangle$ | Generators and relations for $G$, i.e. a presentation of $G$ |
| $(\varphi, \psi)$ | Inner product of class functions |
| $\delta_{ij}$ | The Kronecker delta, $\begin{cases} 1 & \text{if } i = j \\ 0 & \text{else} \end{cases}$ |

# Contents

# Chapter 0

# Introduction

When studying group theory one notices almost immediately that groups of prime power orders are of great significance, with Cauchy's, Lagrange's and Sylow's theorems being three good examples of this. The study of these so called $p$-groups, where $p$ is a prime, can for example be used to give a clear understanding of other groups as being compositions of different $p$-groups. This thesis will try to classify $p$-groups of low power orders, e.g. $p^3,\ p^4$.

## 0.1 Background

We assume that the reader is familiar with group theory but we give a short summary as a recapitulation as well as to clarify the notation. This summary is extracted from [5] but could be found in any elementary book on the subject of abstract algebra such as [6].

**Definition 0.1.1.** An ordered pair $(G, \star)$ where $G$ is a set and $\star$ is a binary operation is called a *group*, often denoted simply $G$, if $\star$ satisfies:

(i) $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$.

(ii) there exists an element $e$ in $G$ with the property $a \star e = e \star a = a$ for all $a \in G$ which we call the *identity*.

(iii) for every element $a \in G$ there exists some $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$.

**Definition 0.1.2.** $H$ is a *subgroup* of $G$, denoted $H \leq G$, if $H \subseteq G$, $H \neq \varnothing$ and $H$ is closed under taking products and inverses. A *proper subgroup* is a subgroup which is not the whole group, i.e. $H \leq G$ and $H \neq G$.

**Definition 0.1.3.** The *center* of a group $G$, denoted $Z(G)$ is the subgroup of $G$ of largest order that commutes with every element in $G$.

**Definition 0.1.4.** A subgroup $N$ of $G$ is called a *normal subgroup* if $gNg^{-1} = N$ for all $g \in G$. We denote this $N \trianglelefteq G$.

**Definition 0.1.5.** Let $N$ be a normal subgroup of $G$. We define the *quotient* of $G$ and $N$ as the set

$$G/N = \{gN : g \in G\}.$$

**Theorem 0.1.6.** *The set $G/N$ defined above is a group with the operation defined by $g_1N \cdot g_2N = (g_1g_2)N$ for all $g_1N, g_2N \in G/N$.*

**Definition 0.1.7.** A group $G$ is *cyclic* if it can be generated by a single element, i.e. there is some element $g \in G$ such that $G = \{g^n : n \in \mathbb{Z}\}$ when the operation is multiplication.

**Notation.** A finite cyclic group of order $n$ will be denoted $Z_n$. When we really want to stress that the elements in the group are integers we denote $Z_n$ by $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ and use additive notation.

One important idea in group theory is that regarding a special kind of mapping.

**Definition 0.1.8.** Let $G$ be a group with operation $\bullet$ and $H$ a group with operation $\diamond$. A map $\varphi : G \mapsto H$ that preserves the structure of the groups, i.e. a mapping with the property

$$\varphi(a \bullet b) = \varphi(a) \diamond \varphi(b) \quad \text{for all } a, b \in G,$$

is called a *homomorphism.*

**Definition 0.1.9.** Let $\varphi : G \mapsto H$ be a homomorphism. Then we define the *kernel* of $\varphi$ as

$$\ker(\varphi) = \{x \in G : \varphi(x) = 0\}$$

where 0 is the identity in $H$.

**Definition 0.1.10.** Let $\varphi : G \mapsto H$ be a homomorphism. We define the *image* of $\varphi$ as

$$\mathrm{im}(\varphi) = \{\varphi(x) : x \in G\}.$$

There are several theorems regarding homomorphisms but one in particular that we will use is the following.

**Theorem 0.1.11** (The First Isomorphism Theorem)**.** *If $\varphi : G \mapsto H$ is a homomorphism of groups, then* $\ker(\varphi)$ *is normal in $G$ and* $G/\ker(\varphi) \cong \mathrm{im}(G)$.

From this theorem one can deduce the following.

**Corollary 0.1.12.** *If $\varphi$ is a homomorphism of groups then $\varphi$ is injective if and only if* $\ker(\varphi) = \{1\}$*, where 1 is the identity.*

**Notation.** A group that only contains an identity element, i.e. a group $\{1\}$ where 1 is the identity element, will simply be denoted 1.

It is quite fruitless to talk about groups being equal to each other since the elements in the set the groups consist of are often unimportant. Instead one looks at how the operation acts on the set and so we define the idea of isomorphisms.

**Definition 0.1.13.** An isomorphism of groups is a bijective homomorphism of groups.

**Definition 0.1.14.** Two groups, $G$ and $H$, are *isomorphic*, denoted $G \cong H$ if there exists some isomorphism between them (making them in some sense equal).

**Definition 0.1.15.** An *automorphism* is an isomorphism from a group $G$ to itself.

**Definition 0.1.16.** Let $G$ be a group. We define the *automorphism group* of $G$, denoted $\mathrm{Aut}(G)$, as the group consisting of all the automorphism on $G$.

Another way one can look at a group is by its generators and relations. We define this principal below.

**Definition 0.1.17.** Let $A$ be a subset of the group $G$. Then we define

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H.$$

This is called the *subgroup of $G$ generated by $A$*. If $A$ is a finite set $\{a_1, a_2, ..., a_n\}$ then we write $\langle a_1, a_2, ..., a_n \rangle$ instead of $\langle \{a_1, a_2, ..., a_n\} \rangle$

**Definition 0.1.18** (informal)**.** A *relation* is an equation that the generators must satisfy. Let $G$ be a group. If $G$ is generated by some subset $S$ and there is some collection of relations $R_1, R_2, ..., R_m$ such that any relation among the elements of S can be deduced from these we shall call these generators and relations a *presentation* of $G$ and write

$$G = \langle S : R_1, R_2, ..., R_m \rangle.$$

*Observation.* More correctly we say that $G$ has the above presentation if $G$ is isomorphic to the quotient of the free group of $S$ by the smallest normal subgroup containing the relations $R_1, R_2, ..., R_m$ but for more information about presentations we refer to any detailed book on the subject.

This thesis is regarding the theory of groups of prime power order. The definition of a so called $p$-group is:

**Definition 0.1.19.** Let $G$ be a group and $p$ a prime. A group of order $p^n$ for some $n \geq 0$ is called a *$p$-group*. A subgroup of $G$ which is a $p$-group is called a *$p$-subgroup*.

Now we shall state some of the most well known theorems in group theory, some of these will be used through out the text without references. They are all applicable on the theory of $p$-groups.

**Theorem 0.1.20** (Lagrange's Theorem, main part)**.** *If $G$ is a finite group and $H$ is a subgroup of $G$ then the order of $H$ divides the order of $G$.*

*Observation.* By Lagrange's theorem, all proper nontrivial subgroups of a group of order $p^\alpha$ have order $p^k$ for $k \in \{1, 2, ..., \alpha - 1\}$.

**Theorem 0.1.21** (Cauchy's Theorem)**.** *If $G$ is a finite group of order $n$ and $p$ is a prime dividing $n$ then $G$ has an element of order $p$.*

**Definition 0.1.22.** Let $G$ be a group of order $p^n m$ where $p \nmid m$ then a subgroup to $G$ of order $p^n$ is called a *Sylow $p$-subgroup* of $G$.

**Theorem 0.1.23** (Sylow's Theorem, part of)**.** *Let $G$ be a group of order $p^n m$ with $p \nmid m$. Then there exists some Sylow $p$-subgroup and furthermore, any two Sylow $p$-subgroups of $G$ are conjugate in $G$.*

Finally we add the definition of a direct product between two groups and with it, one of the most important theorems regarding abelian groups.

**Definition 0.1.24.** Let $G$ and $H$ be two groups with operations $\star$ and $\bullet$ respectively. We define the *direct product* of $G$ and $H$ as the group

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

with operation $*$ such that $(g_1, h_1) * (g_2, h_2) = (g_1 \star g_2, h_1 \bullet h_2)$.

**Theorem 0.1.25** (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Let $G$ be a finitely generated group, i.e. there exists some finite subset $H$ of $G$ such that $G = \langle H \rangle$. Then*

1. $$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_s} \times \ldots \times Z_{n_s}$$

   *for some integers $r, n_1, n_2, \ldots, n_s$ satisfying:*

   (a) *$r \geq 0$ and $n_j \geq 2$ for all $j$*

   (b) *$n_{i+1} | n_i$ for $1 \leq i \leq s - 1$*

2. *the expression in 1. is unique.*

# Chapter 1

# Factorization of $p$-groups as semi-direct products

## 1.1 Introduction and preliminaries

The theory for this chapter is mostly based on the book *Abstract algebra* by David S. Dummit and Richard M. Foote [5].

The structure theorem of abelian groups, Theorem 0.1.25, says that all abelian groups can be decomposed into direct products of cyclic groups. We want to study and see if we can show something similar for non-abelian groups. The structure of groups of orders $p$ and $p^2$ are widely known and will therefore only be mentioned in passing at the end of this section. First of all we will here state some important results in group theory which will come in handy further on. This first one is a good aid in determining the center of a group.

**Proposition 1.1.1.** [5, Exercise 3.1.36] *Let $G$ be a finite group of order $n$. If $G/Z(G)$ is cyclic then $G$ is abelian.*

*Proof.* Let $Z(G) = \{1, z_1, z_2, ..., z_{q-1}\}$ have order $q$. Suppose that

$$G/Z(G) = \{x_1Z(G), x_2Z(G), ..., x_nZ(G)\}$$

is cyclic. That implies that there exists $g \in G$, with order $m$ say, such that

$$G/(Z(G) = \langle gZ(G)\rangle = \{Z(G), gZ(G), g^2Z(G), ..., g^{m-1}Z(G)\}$$

for some $m \in \mathbb{Z}^+$ with $m \leq n$.
Therefore, for all $k \in \{1, 2, ..., n\}$ there exists some $i \in \{1, 2, ..., m\}$ such that

$$\{x_k, x_kz_1, x_kz_2, ..., x_kz_{q-1}\} = x_kZ(G) = g^iZ(G) = \{g^i, g^iz_1, g^iz_2, ..., g^iz_{q-1}\}$$

$$\Rightarrow x_k \in \{g^i, g^i z_1, g^i z_2, ..., g^i z_{q-1}\}$$
$$\Rightarrow \ x_k = g^i \text{ or } x_k = g^i z_j \text{ for some } j \in \{1, 2, ..., q-1\}.$$

We have thus concluded that there exists some $g \in G$ such that for all $x \in G$, $x = g^i z$ for some $1 \leq i \leq m$ and some $z \in Z(G)$ from which the rest follows trivially. ⨳

There are several useful properties regarding $p$-groups, some of which we state in the following theorem.

**Theorem 1.1.2.** *Let $G$ be a $p$-group of order $p^n$. Then*

1. *The center of $G$ is non-trivial, i.e. $Z(G) \neq 1$.*
2. *For every $k \in \{0, 1, ..., n\}$, $G$ has a normal subgroup of order $p^k$.*
3. *Every subgroup of order $p^{n-1}$ is normal in $G$.*

*Proof.* See [5, p. 188-189]. ⨳

**Theorem 1.1.3.** *Any group of order $p$, where $p$ is a prime, is isomorphic to the cyclic group $Z_p$.*

*Proof.* Follows from Cauchy's Theorem. Let $G$ be a group of order $p$. Since $p$ divides $p$ we have that there exists some element, say $g$, of order $p$ in the group. Then we have that $\langle g \rangle$, which is isomorphic to $Z_p$, has order $p$ and so it must be that $G$ is isomorphic to $Z_p$. ⨳

**Theorem 1.1.4.** *A group of order $p^2$, where $p$ is a prime, is isomorphic to either $Z_{p^2}$ or $Z_p \times Z_p$.*

*Proof.* Let $G$ be a group of order $p^2$. From Theorem 1.1.2 we have that the center of any $p$-group is non-trivial. Therefore we have that the order of $G/Z(G)$ is either 1 or $p$ and so $G/Z(G)$ must be cyclic and from Proposition 1.1.1 we have therefore that $G$ is abelian. If $G$ has an element of order $p^2$ then we have that $G$ is cyclic and isomorphic to $Z_{p^2}$. Suppose therefore that any non-identity element of $G$ has order $p$. Let $g$ be such an element and take some $h \in G \setminus \langle g \rangle$. It is clear that $\langle g, h \rangle$ must have an order greater than $p$, otherwise we would have $\langle g, h \rangle = \langle g \rangle$ which would be a contradiction. Since $p$ is a prime the only choice left is that the order of $\langle g, h \rangle$ is $p^2$ and therefore we have that $G = \langle g, h \rangle$. Furthermore, since both $g$ and $h$ has order $p$ it follows that $\langle g \rangle \times \langle h \rangle \cong Z_p \times Z_p$. Now we can define the mapping $\Psi : \langle g \rangle \times \langle h \rangle \mapsto \langle g, h \rangle$

$$(g^i, h^j) \mapsto g^i h^j \qquad \text{for all } i, j \in \mathbb{Z}$$

and since this clearly is an isomorphism we have that $G \cong Z_p \times Z_p$.
Hence, $G$ is isomorphic to either $Z_{p^2}$ or $Z_p \times Z_p$. ⨳

## 1.2 The semi-direct product

### 1.2.1 Definitions and useful results

Here we will explain the concept of one important structure operation, namely the semi-direct product which is a generalization of the direct product and will be shown to be a very useful tool to structure certain kinds of groups.

**Definition 1.2.1.** Let $H$ and $K$ be non-trivial finite groups and $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. Through out the text the operators in $H$ and $K$ will consequently be written as "$\cdot$" except when we want to stress the fact that one of them is abelian and will in that case write the operation as "$+$". We define the operation $\rtimes_\varphi$ as the following: Let $H \rtimes_\varphi K$ be the set $\{(h,k) : h \in H, k \in K\}$ on which it acts an operation $*$ as

$$(h_1, k_1) * (h_2, k_2) = (h_1 \cdot \varphi(k_1)(h_2), k_1 \cdot k_2).$$

We define $G \triangleq H \rtimes_\varphi K$ as the semi-direct product of $H$ and $K$ with respect to $\varphi$. When there is no doubt about which homomorphism, $\varphi$, that defines the group, $\varphi$ will be omitted and the semi-direct product will be written $H \rtimes K$.

**Theorem 1.2.2.** *If $H$, $K$ and $\varphi$ is as in the above definition then $G = H \rtimes_\varphi K$ is a group of order $|G| = |H||K|$.*

*Proof.* To show that $(G, *)$ is a group we have to show that it satisfies associativity and has both an identity element as well as an inverse for every element in $G$. The operation $*$ is of course well defined in $G$. That it is associative is a simple verification,

$$\begin{aligned}
\big((h_1, k_1) * (h_2, k_2)\big) * (h_3, k_3) &= (h_1 \cdot \varphi(k_1)(h_2), k_1 \cdot k_2) * (h_3, k_3) \\
&= \Big(\big(h_1 \cdot \varphi(k_1)(h_2)\big) \cdot \varphi(k_1 \cdot k_2)(h_3), k_1 \cdot k_2 \cdot k_3\Big) \\
&= \Big(\big(h_1 \cdot \varphi(k_1)(h_2)\big) \cdot \big(\varphi(k_1) \circ \varphi(k_2)(h_3)\big), k_1 \cdot k_2 \cdot k_3\Big) \\
&= \Big(\big(h_1 \cdot \varphi(k_1)(h_2)\big) \cdot \big(\varphi(k_1)(\varphi(k_2)(h_3))\big), k_1 \cdot k_2 \cdot k_3\Big) \\
&= \Big(h_1 \cdot \big(\varphi(k_1)(h_2 \cdot \varphi(k_2)(h_3))\big), k_1 \cdot k_2 \cdot k_3\Big) \\
&= (h_1, k_1) * (h_2 \cdot (\varphi(k_2)(h_3)), k_2 \cdot k_3) \\
&= (h_1, k_1) * ((h_2, k_2) * (h_3, k_3)).
\end{aligned}$$

That $e = (1, 1)$ is the unit in $G$ is trivial (remembering that a homomorphism takes the identity on the identity). We shall now see that $(\varphi(k^{-1})(h^{-1}), k^{-1})$ is the inverse

of $(h,k) \in G$:

$$\begin{aligned}(h,k) * (\varphi(k^{-1})(h^{-1}), k^{-1}) &= (h \cdot \varphi(k)(\varphi(k^{-1})(h^{-1})), k \cdot k^{-1}) \\ &= (h \cdot (\varphi(k) \circ \varphi(k^{-1}))(h^{-1}), k \cdot k^{-1}) \\ &= (h \cdot (\varphi(k) \circ \varphi(k)^{-1})(h^{-1}), k \cdot k^{-1}) \\ &= (h \cdot id(h^{-1}), 1) \\ &= (h \cdot h^{-1}, 1) \\ &= (1,1),\end{aligned}$$

$$\begin{aligned}(\varphi(k^{-1})(h^{-1}), k^{-1}) * (h,k) &= (\varphi(k^{-1})(h^{-1}) \cdot \varphi(k^{-1})(h), k \cdot k^{-1}) \\ &= (\varphi(k^{-1})(h^{-1} \cdot h), 1) \\ &= (\varphi(1), 1) \\ &= (1,1).\end{aligned}$$

To conclude it is clear that the order of the group is $|H||K|$. ⨳

*Observation.* $\varphi(k_1)(h_2)$ is equivalent to the group K acting on the group H and is then denoted $k_1.h_2$

*Observation.* If $\varphi$ would be the trivial homomorphism then the semi-direct product would become the direct product. So one can in fact see the direct product as a special case of the semi-direct product.

**Theorem 1.2.3.** *If $G \cong H \rtimes_\varphi K$ then the following must be true:*
*$H \cap K = 1$, $G \cong HK$ and $H \trianglelefteq G$.*

*Proof.* This follows from identifying the subgroups $H, K$ of $G$ with being isomorphic to $\widetilde{H} = \{(h,1) : h \in H\}$ and $\widetilde{K} = \{(1,k) : k \in K\}$ respectively (an omitted, simple verification). Noting that $\widetilde{H} \cap \widetilde{K} = 1$ we have proved the first statement. From that it follows that the mapping, $\Psi$, from $HK$ to $H \rtimes_\varphi K$ defined by $\Psi(hk) = (h,k)$ is an isomorphism and therefore we have proved also the second statement. Furthermore, we have that for all $k \in K$ and for all $h \in H$ that

$$\begin{aligned}(1,k) * (h,1) * (1,k)^{-1} &= (\varphi(k)(h), k) * (1, k^{-1}) \\ &= (\varphi(k)(h) \cdot \varphi(k)(1), k \cdot k^{-1}) \\ &= (\varphi(k)(h), 1) \leq \widetilde{H}\end{aligned}$$

so $\widetilde{K} \leq N_G(\widetilde{H})$ and therefore $K \leq N_G(H)$. With $G \cong HK$ and $H, K \leq N_G(H)$ it follows that $G = N_G(H)$. Hence $H$ is normal in $G$. ⨳

*Observation.* We see through our calculations that we have in some sense defined conjugation in the semi-direct product as $khk^{-1} = \varphi(k)(h)$ since $h$ and $k$ are related to $(h,1)$ and $(1,k)$ respectively.

**Corollary 1.2.4.** *The Quaternion group $Q_8$ can not be decomposed into a semi-direct product of two groups.*

*Proof.* Since every nontrivial subgroup of $Q_8$ must contain the element $-1$ ($i^2 = -1, j^2 = -1, k^2 = -1$) there can be no two subgroups whose intersection is only 1. ⨳

**Corollary 1.2.5.** *No simple group can be decomposed as a semi-direct product of two groups.*

*Proof.* A simple group has no normal subgroups except itself and the trivial one. ⨳

Now we will state two theorems that will become very important for finding the structures of $p$-groups. The first one is a converse to Theorem 1.2.3.

**Theorem 1.2.6.** *If $G$ is a group with subgroups $H$ and $K$ such that $G = HK$, $H \trianglelefteq G$ and $H \cap K = 1$ then there exists some homomorphism $\varphi : K \to \mathrm{Aut}(H)$ such that $G \cong H \rtimes_\varphi K$*

*Proof.* Since we are dealing with finite groups it is clear that the order of the groups are equal, i.e. $|HK| = |H \rtimes_\varphi K|$. Therefore, in order to prove that they are isomorphic we only need to show that there exists some injective homomorphism from one into the other. It is a known fact that if $H \cap K = 1$ there is a unique way to write any element of $HK$ in the form $hk$ for some $h \in H$ and some $k \in K$, see more in [5, Proposition 5.8]. As stated in the observation of Theorem 1.2.3 we have that $khk^{-1} = \varphi(k)(h)$. Let us now define a mapping $\Psi : HK \mapsto H \rtimes_\varphi K$ by $hk \mapsto (h, k)$. This is clearly an homomorphism since

$$\begin{aligned}(h_1k_1)(h_2k_2) = h_1(k_1h_2k_1^{-1})k_1k_2 = (h_1\varphi(k_1)(h_2))(k_1k_2) \\ \overset{\Psi}{\mapsto} (h_1 \cdot \varphi(k_1)(h_2), k_1 \cdot k_2) = (h_1, k_1) * (h_2, k_2),\end{aligned}$$

and furthermore, since any element in $HK$ can be written uniquely as a product of $h$ and $k$ it is clear that $\varphi$ is a injective homomorphism and therefore an isomorphism. ⨳

**Theorem 1.2.7.** *Let $H$ and $K$ be finite groups. If $K$ is cyclic and there are two homomorphisms, $\varphi_1$ and $\varphi_2$, from $K$ into $\mathrm{Aut}(H)$ such that $\mathrm{im}(\varphi_1)$ and $\mathrm{im}(\varphi_2)$ are conjugate subgroups of $\mathrm{Aut}(H)$, then $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$.*

*Proof.* We prove this by constructing a isomorphism between the groups. Let the operation in $H \rtimes_{\varphi_1} K$ be written $*_1$ and the operation in $H \rtimes_{\varphi_2} K$ be written $*_2$. Since $K$ is cyclic it is abelian in the "second coordinate" but we will in this case still use multiplicative notation due to simplify the compatibility with the "first coordinate". Suppose that $\mathrm{im}(\varphi_1)$ and $\mathrm{im}(\varphi_2)$ are conjugate, i.e. $\sigma\varphi_1(K)\sigma^{-1} = \varphi_2(K)$ for some

$\sigma \in \mathrm{Aut}(H)$. Therefore we have that for some $a \in \mathbb{Z}^+$ that $\sigma\varphi_1(k)\sigma^{-1} = \varphi_2(k)^a$ for all $k \in K$. Let

$$\Psi : H \rtimes_{\varphi_1} K \to H \rtimes_{\varphi_2} K$$
$$(h,k) \mapsto (\sigma(h), k^a)$$

First we prove that $\Psi$ is a homomorphism,

$$\begin{aligned}
\Psi((h,k) *_1 (h',k')) &= \Psi((h \cdot \varphi_1(k)(h'), k \cdot k') \\
&= (\sigma(h \cdot \varphi_1(k)(h')), (k \cdot k')^a) \\
&= (\sigma(h) \cdot \sigma(\varphi_1(k)(h')), k^a \cdot (k')^a) \\
&= (\sigma(h) \cdot (\sigma \circ \varphi_1(k))(h'), k^a \cdot (k')^a) \\
&= (\sigma(h) \cdot (\varphi_2(k)^a \circ \sigma)(h'), k^a \cdot (k')^a) \\
&= (\sigma(h) \cdot \varphi_2(k^a)(\sigma(h')), k^a \cdot (k')^a) \\
&= (\sigma(h), k^a) *_2 (\sigma(h'), (k')^a) \\
&= \Psi((h,k)) *_2 \Psi((h',k')).
\end{aligned}$$

We now prove that this is a bijection by showing that it has a two-sided inverse. This is easily seen by defining $\Psi^{-1}(h,k) = ((\varphi_2(k)^{-a} \circ \sigma)(h^{-1}), k^{-a})$. From this we get

$$\begin{aligned}
\Psi(h,k) *_2 \Psi^{-1}(h,k) &= (\sigma(h), k^a) *_2 (\varphi_2(k)^{-a} \circ \sigma(h^{-1}), k^{-a}) \\
&= (\sigma(h) \cdot \varphi_2(k^a)(\varphi_2(k)^{-a} \circ \sigma(h^{-1})), k^a \cdot k^{-a}) \\
&= (\sigma(h) \cdot (\varphi_2(k)^a \circ \varphi_2(k)^{-a} \circ \sigma)(h^{-1}), k^0) \\
&= (\sigma(h) \cdot (id \circ \sigma)(h^{-1}), 1) \\
&= (\sigma(h) \cdot \sigma(h^{-1}), 1) \\
&= (\sigma(h \cdot h^{-1}), 1) \\
&= (1,1),
\end{aligned}$$

$$\begin{aligned}
\Psi^{-1}(h,k) *_2 \Psi(h,k) &= (\varphi_2(k)^{-a} \circ \sigma(h^{-1}), k^{-a}) *_2 (\sigma(h), k^a) \\
&= ((\varphi_2(k)^{-a} \circ \sigma)(h^{-1}) \cdot \varphi_2(k^{-a})(\sigma(h)), k^a \cdot k^{-a}) \\
&= ((\varphi_2(k)^{-a} \circ \sigma)(h^{-1}) \cdot (\varphi_2(k)^{-a} \circ \sigma)(h)), 1) \\
&= ((\varphi_2(k)^{-a} \circ \sigma)(h^{-1} \cdot h), 1) \\
&= ((\varphi_2(k)^{-a} \circ \sigma)(1), 1) \\
&= (1,1),
\end{aligned}$$

so $\Psi$ does indeed have a two-sided inverse and is therefore bijective and we have found our isomorphism. ⨳

The converse of this theorem, that if $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$ and $K$ is cyclic then $\mathrm{im}(\varphi_1)$ is conjugate to $\mathrm{im}(\varphi_2)$, might hold as well but we will have to leave that as a conjecture.

Now that we have defined this structure operation we can set our minds to the problem in hand. We make the following, non-standard, definition.

**Definition 1.2.8.** A $p$-group that can be written as semi-direct products of cyclic groups is called *completely factorizable*.

With this definition it follows that $p$-groups of both order $p$ and $p^2$ are always completely factorizable with the semi-direct product being trivial in all cases, see Theorems 1.1.3 and 1.1.4, and this will also hold for every abelian $p$-group.

## 1.3 Automorphisms of $p$-groups

It is clear from the previous section that the automorphism group of $p$-groups will play an important role in the factorization of groups into semi-direct products. Therefore we will take a moment to study them.

We will see that we can, for every automorphism, find an element relating to that one which makes the following, nonstandard, definition useful.

**Definition 1.3.1.** Let the automorphism group of a group $G$ be isomorphic to some other group $H$, i.e. $\mathrm{Aut}(G) \cong H$, for some isomorphism $\Psi : \mathrm{Aut}(G) \mapsto H$. If an element $h \in H$ is the image of some automorphism $\varphi \in \mathrm{Aut}(G)$ under $\Psi$, i.e. $\Psi(\varphi) = h$, we say that $\varphi$ and $h$ are *isomorphically related*. We denote this $\varphi \leftrightarrow h$.

### 1.3.1 The automorphism group of $Z_{p^n}$

The automorphism group of a cyclic $p$-group, $Z_{p^n}$ (with addition as an operator), is isomorphic to the multiplicative group $\mathbb{Z}^*_{p^n}$, i.e.

$$\mathrm{Aut}(Z_{p^n}) \cong \mathbb{Z}^*_{p^n}.$$

That can be seen by looking at the composition of the elements of the automorphism group. Take $\pi, \sigma \in \mathrm{Aut}(Z_{p^n})$ (non-identity elements). We now take a generator for $Z_{p^n}$, say 1 (where we have the operation in $Z_{p^n}$ as addition), and study the behavior of these two automorphisms. Let $\pi(1) = g$ and $\sigma(1) = h$. We get

$$\pi \circ \sigma(1) = \pi(h) = \pi(\underbrace{1 + 1 + ... + 1}_{h}) = \underbrace{\pi(1) + \pi(1) + ...\pi(1)}_{h} = h \cdot \pi(1) = h \cdot g$$

so we see that the composition of $\pi$ and $\sigma$ is the same thing as multiplication in our original group, from which the result follows. From [5, Corollary 9.20] we have that $\mathbb{Z}^*_{p^n}$ is a cyclic group of order $p^{n-1}(p-1)$. Indeed, an element is invertible if and only if it is not divisible by $p$ so $|\mathbb{Z}^*_{p^n}| = p^n - p^{n-1} = p^{n-1}(p-1)$.

### 1.3.2 The automorphism groups of $Z_p \times Z_p$ and $Z_p^n$

We shall now study the automorphism group of $Z_p \times Z_p$. Similar to what we just did we take the generators of the group and see what they map to. This group is generated by two elements, e.g. $(1,0)$ and $(0,1)$, so we have to see what these two maps unto. Take $\varphi \in \mathrm{Aut}(Z_p \times Z_p)$ and let $\varphi((1,0)) = (a,b)$ and $\varphi((0,1)) = (c,d)$. If we now take $(g,h) \in Z_p \times Z_p$ we get

$$\begin{aligned}\varphi((g,h)) &= \varphi((g,0)+(0,h)) = \varphi((g,0)) + \varphi((0,h)) = \\ &= g \cdot \varphi((1,0)) + h \cdot \varphi((0,1)) = g \cdot (a,b) + h \cdot (c,d) = (ga+hc, gb+hd).\end{aligned}$$

We can see that this is very similar to the components from a matrix multiplication

$$(g,h) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ga+hc, gb+hd).$$

Let $\sigma \in \mathrm{Aut}(Z_p \times Z_p)$ be defined as $\sigma((1,0)) = (i,j)$ and $\sigma((0,1)) = (k,l)$. We then get

$$\begin{aligned}\sigma \circ \varphi(g,h) &= \sigma(ga+hc, gb+hd) \\ &= (ga+hc) \cdot \sigma((1,0)) + (gb+hd) \cdot \sigma((0,1)) \\ &= (ga+hc) \cdot (i,j) + (gb+hd) \cdot (k,l) \\ &= (gai+hci, gaj+hcj) + (gbk+hdk, gbl+hdl) \\ &= (g(ai+bk)+h(ci+dk), g(aj+bl)+h(cj+dl)).\end{aligned}$$

This we can see is the same thing as

$$\begin{aligned}(g,h) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} = (g,h) \cdot \begin{pmatrix} ai+bk & aj+bl \\ ci+dk & cj+dl \end{pmatrix} = \\ = (g(ai+bk)+h(ci+dk), g(aj+bl)+h(cj+dl)),\end{aligned}$$

so we see that the composition of two isomorphisms is the same thing as matrix multiplication. There is still one more thing we have to check, namely that the function $\varphi \in \mathrm{Aut}(Z_p \times Z_p)$ is in fact an isomorphism. Since we are dealing with finite groups it is enough to make sure that it is injective, which it is if and only if the kernel of $\varphi$ is trivial. The equation

$$(g,h) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (0,0)$$

has a unique solution (g,h)=(0,0) if and only if the matrix is invertible which is the same thing as its determinant $ad - bc \neq 0$.

So we see that $\mathrm{Aut}(Z_p \times Z_p) \cong GL_2(\mathbb{F}_p)$. The same calculations and results arise when we are dealing with $Z_p^n = \underbrace{Z_p \times Z_p \times ... \times Z_p}_{n}$ so we have found that

$$\mathrm{Aut}(Z_p^n) \cong GL_n(\mathbb{F}_p).$$

From [5, p. 418] we know that $GL_n(\mathbb{F}_p)$ is a group of order

$$(p^n - 1)(p^n - p)(p^n - p^2)...(p^n - p^{n-1}).$$

### 1.3.3 Examples

From the previous section we have seen that we will study homomorphisms from one group into the automorphism group of another group, so lets look at some examples of this.

*Example* 1.3.2. Let $\varphi : Z_p \to \mathrm{Aut}(Z_{p^2})$ be a homomorphism. We have that $\mathrm{Aut}(Z_{p^2}) \cong \mathbb{Z}_{p^2}^*$ has order $p(p-1)$. The first isomorphism theorem gives us the following:

$$|\mathrm{im}(\varphi)| = |Z_p|/|\ker(\varphi)| = 1 \text{ or } p.$$

If $|\mathrm{im}(\varphi)| = 1$ then $\varphi$ is trivial and the semi-direct product relating to $\varphi$ is simply the direct product. So lets assume that $|\mathrm{im}(\varphi)| = p$. A subgroup of $\mathbb{Z}_{p^2}^*$ of order $p$ is

$$\{np + 1 : n \in Z_p\}.$$

This can be shown by looking at

$$(np+1)^p = (np)^p + p(np)^{p-1} + ... + p(np) + 1 \equiv 1 \pmod{p^2}$$

and since $p$ is a prime any nontrivial element will be a generator for the group. For instance

$$(np+1)^2 = (np)^2 + 2np + 1 \equiv 2np + 1 \pmod{p^2}.$$

Therefore we can represent $\varphi(k)$ as $(np+1)^k$ for some $n$. The choice of $n$ is not important (as long as it is kept from 0) since we can scale our group action as $(np+1)^{mk}$ for some $m$ depending on $n$. One could also conclude this last fact from Theorem 1.2.7 since we have that $Z_p$ is cyclic and all subgroups of order $p$ of $\mathbb{Z}_{p^2}^*$ are conjugate by each other (from Sylow's theorem).

*Example* 1.3.3. Let $\varphi : Z_p \to \mathrm{Aut}(Z_p \times Z_p)$ be a homomorphism. Just as in the example above we see that we want to look at subgroups of the automorphism group that has order $p$. A subgroup of order $p$ to $\mathrm{Aut}(Z_p \times Z_p) \cong GL_2(\mathbb{F}_p)$ is the group generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ and from Sylow's theorem we can deduce that

any other subgroup of order $p$ is conjugate to this one, since $|GL_2(\mathbb{F}_p)| = p(p^2-1)(p-1)$. Therefore we see that the automorphism $\varphi(k)$ can be represented as multiplication by the matrix $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$.

## 1.4 The groups of order $p^3$

From the fundamental theorem of abelian groups we know that there are three different abelian non-isomorphic groups of order $p^3$, namely $Z_{p^3}$, $Z_{p^2} \times Z_p$ and $Z_p \times Z_p \times Z_p$. Now we will look at the non-abelian groups. From Corollary 1.2.4 we have an example of a group of order $p^3$ that can not be expressed as a semi-direct product for $p = 2$. It will be shown that $p = 2$ is a special case and so we will begin to study this special case of primes $p$ and then move along to the case where $p$ is any odd prime.

### 1.4.1 The special case $p = 2$

**Theorem 1.4.1.** *If $G$ is a non-abelian group of order $2^3 = 8$ then it is isomorphic to either $D_8$ or $Q_8$.*

*Proof.* This proof is mostly based on a similar proof in [4]. There can of course not be any element in $G$ of order 8 since that would imply that the group is abelian. If every element of $G$ has order 2 then $G$ must also be abelian since that implies that for all $a, b \in G$, $abab = (ab)^2 = 1$ and multiplying the left hand side with $a$ and the right hand side with $b$ gives $ba = ab$. So we can conclude that there must exist some element of order 4, say $a$. The subgroup generated by $a$ is of order $4 = 2^{3-1}$ so Theorem 1.1.2 tells us that it must be normal in $G$. Take an element $b \in G \setminus \langle a \rangle$. Since $\langle a \rangle$ is normal we have that

$$bab^{-1} \in \langle a \rangle = \{1, a, a^2, a^3\}.$$

If $bab^{-1} = 1$ then $a$ has order 1, so that can not be. The same thing goes for $bab^{-1} = a^2$ since that implies that $ba^2b^{-1} = a^4 = 1$ which would mean that $a$ has order 2 so that can not be either. Lastly, if $bab^{-1} = a$ then the group is abelian so this is also an impossibility. Now we have two possible cases, either that $b$ has order 2 or 4.

Case 1. $b$ has order 2.
Then we must have that $bab^{-1} = a^3 = a^{-1}$ and so we see that this is generates the group

$$G = \langle a, b : a^4 = 1, b^2 = 1, ba = a^{-1}b \rangle$$

which is isomorphic to $D_8$.

Case 2. $b$ has order 4.
We see that if $\langle a\rangle \cap \langle b\rangle = 1$ then that will imply that $G$ has a order larger than 8 so that can not be. Therefore we can deduce that there must be some other element in $G \setminus \langle a\rangle \cup \langle b\rangle$, call it c, which also must have order 4 and furthermore that $a^2 = b^2 = c^2$. So in this case $G$ is generated by

$$\langle a, b, c : a^4 = b^4 = c^4 = 1, a^2 = b^2 = c^2, ba = a^{-1}b\rangle$$

and this group is isomorphic to $Q_8$. ⨳

*Observation.* The prime 2 is a very special case. In the general case, when $G$ is a $p$-group of order $p^3$ with $p \neq 2$ it is not the case that $G$ has to be abelian only because every element has order $p$ as the case were above.

### 1.4.2 $p$ being any odd prime

**Lemma 1.4.2.** *If $G$ is a non-abelian group of order $p^3$ then its center $Z(G)$ has order $p$.*

*Proof.* Since the center is a subgroup of $G$ it has only a few possible orders, namely 1, $p$, $p^2$ and $p^3$. We know that for $p$-groups the center is never trivial so it can't be 1. Since it is non-abelian it can not be $p^3$ either. From Proposition 1.1.1 we can conclude that the order can not be $p^2$ since that would imply that $|G/Z(G)|$ has order $p$ and would therefore be cyclic. The only choice left is $p$. ⨳

**Lemma 1.4.3.** *If $G$ is a group of order $p^3$ then the commutator subgroup of $G$, $G' = \{[x, y] : x, y \in G\}$, has order $p$ and it is equal to the center of $G$, i.e. $G' = Z(G)$.*

*Proof.* Since the center of $G$ is trivially normal in $G$, i.e. $Z(G) \trianglelefteq G$, and $G/Z(G)$ is abelian (since $G/Z(G)$ is a group of order $p^2$) it follows from theorems in [5] that $G' \leq Z(G)$ and since $G$ is non-abelian $G'$ is non-trivial and therefore the only possibility is $G' = Z(G)$. Since $Z(G)$ has order $p$ it follows that $G'$ has order $p$. ⨳

**Lemma 1.4.4.** *If $G$ is a group and the commutator subgroup of $G$ is the same as the center of $G$, i.e. $G' = Z(G)$, then $(xy)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}}$ for all $x, y \in G$.*

*Proof.* We use induction over $n$. It is of course true for $n = 1$. Suppose it is true for $n = k$, so $(xy)^k = x^k y^k [y, x]^{\frac{k(k-1)}{2}}$. We now show that it holds for $n = k + 1$,

$$\begin{aligned}
x^{k+1}y^{k+1}[y,x]^{\frac{k(k+1)}{2}} &= x^{k+1}y^{k+1}[y,x]^{\frac{k(k-1)}{2}}[y,x]^k \\
&= x^{k+1}y^{k+1}[y,x]^{\frac{k(k-1)}{2}} \underbrace{(y^{-1}x^{-1}yx)(y^{-1}x^{-1}yx)...(y^{-1}x^{-1}yx)}_{k} \\
&= x^k xy[y,x]^{\frac{k(k-1)}{2}} \underbrace{(x^{-1}yx)(x^{-1}yx)...(x^{-1}yx)}_{k} \\
&= x^k xy[y,x]^{\frac{k(k-1)}{2}} x^{-1}y^k x \\
&= x^k[y,x]^{\frac{k(k-1)}{2}} xyx^{-1}(y^{-1}y)y^k x \\
&= x^k[y,x]^{\frac{k(k-1)}{2}}[x^{-1},y^{-1}]y^k yx \\
&= x^k y^k[y,x]^{\frac{k(k-1)}{2}}[x^{-1},y^{-1}]yx \\
&= x^k y^k[y,x]^{\frac{k(k-1)}{2}} xyx^{-1}y^{-1}yx \\
&= x^k y^k[y,x]^{\frac{k(k-1)}{2}} xy \\
&= (xy)^k xy \\
&= (xy)^{k+1}.
\end{aligned}$$

⧛

**Lemma 1.4.5.** *If $G$ is a non-abelian group of order $p^3$ where $p$ is an odd prime and $\varphi : G \to G$ is the mapping $\varphi(x) = x^p$ then the kernel of $\varphi$ is of order $p^2$ or $p^3$.*

*Proof.* First we show that $\varphi$ is a homomorphism. Take $x, y \in G$, we get

$$\begin{aligned}
\varphi(xy) = (xy)^p = [\text{Lemma 1.4.4}] = x^p y^p [y,x]^{\frac{p(p-1)}{2}} = x^p y^p ([y,x]^p)^{\frac{p-1}{2}} = \\
= [\text{Lemma 1.4.3}] = x^p y^p 1^{\frac{p-1}{2}} = x^p y^p = \varphi(x)\varphi(y)
\end{aligned}$$

so $\varphi$ is a homomorphism. By the first isomorphism theorem we have that

$$|G|/|\ker(\varphi)| = |\mathrm{im}(\varphi)|$$

and since $\mathrm{im}(\varphi) \leq Z(G)$ we can deduce that $|\mathrm{im}(\varphi)|$ is either 1 or $p$. Since $G$ has order $p^3$ we must have that $|\ker(\varphi)|$ is equal to either $p^2$ or $p^3$.

⧛

*Observation.* This result does not hold when $p = 2$ since that implies that $\frac{p(p-1)}{2} = p - 1 = 1$, and therefore $[y,x]^{\frac{p(p-1)}{2}} = [y,x]^1 \neq 1$.

**Theorem 1.4.6.** *Every non-abelian group of order $p^3$ where $p$ is an odd prime is isomorphic to either $(Z_p \times Z_p) \rtimes Z_p$ or $Z_{p^2} \rtimes Z_p$.*

*Observation.* The notation might be a bit confusing. Of course $Z_{p^2}$ contains at least one subgroup isomorphic to $Z_p$ and so one could think that the intersections would not be trivial but what we mean when we write $Z_{p^2} \rtimes Z_p$ is two groups $H$ and $K$ that fulfill $H \cap K = 1$ and $H \trianglelefteq G$ and that they in turn are isomorphic to $Z_{p^2}$ and $Z_p$ respectively.

*Proof.* This proof is based on results in [5, p. 183]. Let $G$ be a non-abelian group of order $p^3$. There are two cases, either $G$ contains an element of order $p^2$ or not.

Case 1. There exists some element in $G$ of order $p^2$.
Let $g \in G$ have order $p^2$. From Theorem 1.1.2 we know that $\langle g \rangle$ is normal in $G$. There are $p$ elements in $\langle g \rangle$ that has order $p$ (namely those of the kind $g^k$ where $p$ divides $k$), therefore Lemma 1.4.5 tells us that there is at least one element of order $p$, say $h$, that does not lie in $\langle g \rangle$. $\langle h \rangle$ is a group of order $p$ and $\langle g \rangle$ is a group of order $p^2$ with $\langle g \rangle \cap \langle h \rangle = 1$ so the group $\langle g \rangle \langle h \rangle$ is a group of order $p^3$ and must be equal to $G$. By construction we have that $\langle g \rangle \cap \langle h \rangle = 1$ and since $\langle g \rangle$ is normal in $G$ we can use Theorem 1.2.6 to conclude that

$$G = \langle g \rangle \langle h \rangle \cong \langle g \rangle \rtimes_\varphi \langle h \rangle$$

for some $\varphi$. With $\langle g \rangle \cong Z_{p^2}$ and $\langle h \rangle \cong Z_p$ we know from Theorem 1.2.7 that the choice of $\varphi$ is unimportant (as long as it is kept from the trivial one) and will generate isomorphic groups. Therefore we can conclude that there is only one non-abelian group of order $p^3$ which contains an element of order $p^2$ and it is isomorphic to $Z_{p^2} \rtimes Z_p$.

Case 2. $G$ does not contain an element of order $p^2$.
From Theorem 1.1.2 we know that there exists some normal subgroup $H$ of $G$ that has order $p^2$. Furthermore, since $G$, and therefore also $H$, does not contain an element of order $p^2$ we must have that $H \cong Z_p \times Z_p$. Let now $K$ be generated by some element $k \in G \setminus H$. Since $k$ must have order $p$ we have that $K = \langle k \rangle \cong Z_p$. We had that $H$ is normal in $G$ and by construction we have that $H \cap K = 1$ so Theorem 1.2.6 tells us since $G = HK$ that in this case

$$G \cong H \rtimes_\varphi K \cong (Z_p \times Z_p) \rtimes_\varphi Z_p$$

for some $\varphi$. Since any two elements of $\mathrm{Aut}(Z_p \times Z_p)$ that has order $p$ is conjugate with each other, due to Sylow's theorem (see Example 1.3.3), we have from Theorem 1.2.7 that the choice of $\varphi$ is not important and therefore there is only one non-abelian group of order $p^3$, where every non-identity element has order $p$, up to isomorphism, and that is the group $(Z_p \times Z_p) \rtimes Z_p$ ⨳

*Example* 1.4.7. $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{F}_p \right\} \leq GL_3(\mathbb{F}_p)$ where the operation is matrix multiplication. This group is of order $p^3$ since we have $p$-choices at three

locations and also it is non-abelian since, for example,

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Furthermore, this group has no element of order $p^2$ since:

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & nx & ny + \frac{n(n-1)}{2}xz \\ 0 & 1 & nz \\ 0 & 0 & 1 \end{pmatrix}$$

which is easily shown by induction over $n$. Therefore

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & px & py + \frac{p(p-1)}{2}xz \\ 0 & 1 & pz \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which means that every element in $G$ raised to the power $p$ is the identity. So $G$ is a non-abelian group of order $p^3$ and every non-identity element has order $p$. Hence $G \cong (Z_p \times Z_p) \rtimes Z_p$

From this example we have found a good representation of the non-abelian group $(Z_p \times Z_p) \rtimes Z_p$. Simply by identifying the components of the $3 \times 3$-matrix we can see that

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+fa+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$$

is equivalent to

$$((d,e),f) * ((a,b),c) = ((d,e) + \varphi(f)((a,b)), f+c) = ((d+a, e+fa+b), f+c)$$

where

$$\varphi(f)((a,b)) = (a, fa+b).$$

Notice that the operation $*$ mirrors its arguments in relation to the matrix multiplication. One interesting observation is that

$$\varphi(f)((a,b)) = (a, fa+b) = (a,b) \cdot \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}$$

which we can compare to the result of Example 1.3.3. Since we earlier concluded that any non-abelian group of order $p^3$ has a center of order $p$ we can now find the center of $(Z_p \times Z_p) \rtimes Z_p$ by looking at this matrix representation. For a group of order $p$ every non-identity element is a generator of the group so it is enough to find one element that commutes with every element in the group. From previous calculations we can immediately conclude that

$$\begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in Z(G) \quad , \text{ for all } n \in Z_p$$

which corresponds to $((0,n),0)$. Hence $Z((Z_p \times Z_p) \rtimes Z_p)) \cong \{((0,n),0) : n \in Z_p\}$.

Table 1.1: Non-isomorphic groups of order $p^3$ ($p > 2$)

| Highest order element | Abelian | Non-abelian |
|---|---|---|
| $p^3$ | $Z_{p^3}$ | - |
| $p^2$ | $Z_{p^2} \times Z_p$ | $Z_{p^2} \rtimes Z_p$ |
| $p$ | $Z_p \times Z_p \times Z_p$ | $(Z_p \times Z_p) \rtimes Z_p$ |

*Example* 1.4.8. A representation of the group $Z_{p^2} \rtimes_\varphi Z_p$ might not be as intuitive but one example, from [4], would be

$$G = \{\begin{pmatrix} 1+pa & b \\ 0 & 1 \end{pmatrix} : (1+pa), b \in Z_{p^2}\} \subseteq GL_2(\mathbb{F}_{p^2})$$

where $a$ represents the element of order $p$ and $b$ the element of order $p^2$.

From this example we have a nice representation for $Z_{p^2} \rtimes_\varphi Z_p$, namely $G$. So we can now write the operation

$$(b, a) * (d, c) = (b + \varphi(a)(d), a + c) = (b + (1 + pa) \cdot d, a + c)$$

where $\varphi(a)$ corresponds to multiplication with the element $(1 + pa)$ (compare with the result from Example 1.3.2, with $n = 1$). We can also deduce that the center is

$$Z(G) = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in Z_{p^2} \text{ and } p|n \right\} \cong \{(n, 0) : n \in Z_{p^2} \text{ and } p|n\}.$$

*Observation.* One could wonder why the two groups named in Theorem 1.4.6 are the only non-abelian groups of order $p^3$. For instance, why couldn't we find another one from $G \cong Z_p \rtimes_\varphi Z_{p^2}$? Well, lets take a closer look at $\varphi : Z_{p^2} \to \mathrm{Aut}(Z_p)$. We know that $|\mathrm{Aut}(Z_p)| = p - 1$ since any isomorphism can take any non-identity element on some other non-identity element. From the first isomorphism theorem it is clear that

$$|\mathrm{im}(\varphi)| = 1, p, p^2, p^3$$

but this leaves only one possibility for $\mathrm{Aut}(Z_p) \leq \mathrm{im}(\varphi)$ namely 1. So there is only one homomorphism from $Z_{p^2}$ into $\mathrm{Aut}(Z_p)$ and this must be the trivial one, since $|\ker(\varphi)| = |G|/|\mathrm{im}(\varphi)| = p^3$ so $\ker(\varphi) = G$. Hence the semi-direct product $Z_p \rtimes_\varphi Z_{p^2}$ can in fact only be the direct product $Z_p \times Z_{p^2}$ and this is an abelian group (that we have already covered).

Now we are finished with the groups of order $p^3$ and we have seen that if $p$ is a prime greater than two there are five different groups of order $p^3$ up to isomorphism, and all of them are completely factorizable. The final result can be viewed in Table 1.1.

## 1.5 Automorphisms of $p$-groups, continued

In order to find the structure of the automorphism groups of the non-intuitive $p$-groups, e.g. $Z_{p^2} \rtimes Z_p$, we will go about the same way as in the previous section but also having to take the relations into more consideration since we will be working with non-abelian groups. If $\varphi$ is a automorphism of a group than $\varphi$ has to uphold all of the relations of the group and from that one can deduce much information about the automorphism group. Remembering the notation from Definition 1.3.1 we will use the symbol $\leftrightarrow$ between an automorphism and an element in some other group when we mean that they are isomorphically related.

### 1.5.1 The automorphism group of $Z_{p^2} \rtimes Z_p$

First we will study the automorphism group of $Z_{p^2} \rtimes Z_p$. Two generators of the group are $a = (1, 0)$ and $b = (0, 1)$. From the operation we then get $ba = a^{1+p}b$ and so we have that a presentation of the group can be written

$$Z_{p^2} \rtimes Z_p \cong \langle a, b : a^{p^2} = 1, b^p = 1, ba = a^{p+1}b \rangle.$$

From our relations we can, with elementary calculations, deduce some useful expression

$$b^j a^i = a^{i+jip} b^j,$$
$$(a^i b^j)^n = a^{ni+\frac{(n-1)n}{2}jip} b^{nj}.$$

With these we begin our study of the automorphism group of $Z_{p^2} \rtimes Z_p$. Take some automorphism $\varphi \in \mathrm{Aut}(Z_{p^2} \rtimes Z_p)$, defined by

$$\varphi : \begin{cases} a \mapsto a^i b^j & \text{constraints: } i, k \in Z_{p^2} \\ b \mapsto a^k b^l & \qquad\qquad\quad j, l \in Z_p. \end{cases}$$

If $a \in Z_{p^2} \rtimes Z_p$ has order $p^2$ then $\varphi(a) = a^i b^j$ must also have that order.

$$(a^i b^j)^p = a^{pi+\frac{(p-1)p}{2}jip} b^{pj} = a^{pi} \not\equiv 1 \quad \Leftrightarrow \quad p \nmid i.$$

Hence, we have that $i \not\equiv 0 \pmod p$. Furthermore, if $b$ has order $p$ then $\varphi(b) = a^k b^l$ must also have order $p$ so

$$(a^k b^l)^p = a^{pk+\frac{(p-1)p}{2}klp} b^{pl} = a^{pk} \equiv 1 \quad \Leftrightarrow \quad p|k,$$

therefore we have that $k = pm$ for some $m$. Since this is a non-abelian group we also must have that if $ba = a^{1+p}b$ then $\varphi(b)\varphi(a) = \varphi(a)^{1+p}\varphi(b)$. So

$$\begin{aligned}(a^{pm}b^l)(a^ib^j) &= (a^ib^j)^{1+p}(a^{pm}b^l)\\ \Leftrightarrow a^{pm+i+ilp}b^{l+j} &= a^{i+pm+p(i+pmj)}b^{l+j}\\ \Leftrightarrow a^{ilp} &= a^{ip}\end{aligned}$$

$$\Rightarrow il \equiv i \pmod p$$

and since $i \not\equiv 0 \pmod p$ we conclude that

$$l \equiv 1 \pmod p.$$

In order for $\varphi$ to be a automorphism it has to be bijective which it is if

$$\langle\varphi(b)\rangle \cap \langle\varphi(a)\rangle = 1$$

but this is always true with the constraints we have already deduced. That is because any element in $\langle\varphi(a)\rangle$ of order $p$ is of the form $a^{pr}$ for some $r$ and no element in $\langle\varphi(b)\rangle$ is of that form. So we have that the order of the automorphism group must be

$$|\mathrm{Aut}(Z_{p^2} \rtimes Z_p)| = p^3(p-1)$$

since we have $(p^2-p)$ choices for $i$, $p$ choices for $j$ and $p$ choices for $m$.

Therefore we have that $\varphi \in \mathrm{Aut}(Z_{p^2} \rtimes Z_p)$ is really defined by

$$\varphi : \begin{cases} a \mapsto a^ib^j & \text{constraints: } i \in Z_{p^2} \text{ and } i \not\equiv 0 \pmod p \\ b \mapsto a^{pm}b & \qquad\qquad\quad j, m \in Z_p \end{cases}$$

We can simply write what the automorphism $\varphi$ will map an arbitrary element $g \in Z_{p^2} \rtimes Z_p$ on. Since we already have our generators, $a, b$, of the group we know that $g$ can be expressed as $a^xb^y$ for some $x, y$. Using our relations we get

$$\begin{aligned}\varphi(g) = \varphi(a^xb^y) = \varphi(a)^x\varphi(b)^y = (a^ib^j)^x(a^{pm}b)^y = \\ = (a^{xi+\frac{(x-1)x}{2}jip}b^{xj})(a^{ypm}b^y) = a^{xi+\frac{(x-1)x}{2}jip+ypm}b^{xj+y}.\end{aligned}$$

This will sadly not be enough for us since it will show that we will need to calculate what the powers of $\varphi$ maps $g$ to. If we take another automorphism $\sigma \in \mathrm{Aut}(Z_{p^2} \rtimes Z_p)$, defined by

$$\sigma : \begin{cases} a \mapsto a^{i'}b^{j'} & \text{constraints: } i' \in Z_{p^2} \text{ and } i' \not\equiv 0 \pmod p \\ b \mapsto a^{pm'}b & \qquad\qquad\quad j', m' \in Z_p \end{cases}$$

we can see what multiplication will look like in the automorphism group by calculating

$$\begin{aligned}\sigma \circ \varphi(a) &= \sigma(a^i b^j) = ... = a^{ii'+p\left(\frac{(i-1)ii'j'}{2}+jm'\right)} b^{ij'+j},\\ \sigma \circ \varphi(b) &= \sigma(a^{pm} b) = ... = a^{p(i'm+m')} b.\end{aligned}$$

An automorphism will be fully defined through the triple of the exponents, i.e. $\varphi \leftrightarrow (i,j,k)$. So therefore we can represent the multiplication of two automorphisms as

$$(i',j',m') \cdot (i,j,m) = \left(ii' + p\left(\frac{(i-1)ii'j'}{2} + jm'\right), ij' + j, i'm + m'\right).$$

Now we can calculate the powers of $\varphi \leftrightarrow (i,j,m)$. Thanks to Maple [1] we get:

- $(i,j,m)^2 = \left(i^2 + pj\left(\frac{i^3}{2} - \frac{1}{2}i^2 + m\right), ij + j, im + m\right)$
- $(i,j,m)^3 = \left(i^3 + pj\left(\frac{i^5+i^4}{2} - i^3 + 2im + m\right), i^2j + ij + j, i^2m + im + m\right)$
- $(i,j,m)^4 = \Big(i^4 + pj\left(\frac{i^7+i^6+i^5}{2} - \frac{3}{2}i^4 + 3i^2m + 2im + m\right),$
  $, i^3j + i^2j + ij + j, i^3m + i^2m + im + m\Big)$
- $(i,j,m)^5 = \Big(i^5 + pj\left(\frac{i^9+i^8+i^7+i^6}{2} - 2i^5 + 4i^3m + 3i^2m + 2im + m\right),$
  $, i^4j + i^3j + i^2j + ij + j, i^4m + i^3m + i^2m + im + m\Big)$

The structure of these powers leads us to believe that

$$(i,j,m)^n = \left(i^n + pj\left(\frac{1}{2}i^n \sum_{k=0}^{n-1} i^k - \frac{1}{2}ni^n + m\sum_{k=0}^{n-2}(k+1)i^k\right), j\sum_{k=0}^{n-1} i^k, m\sum_{k=0}^{n-1} i^k\right).$$

Since this is true for $n = 1$ we calculate it raised to the power $n+1$ and get (writing

it as its transpose for typographical reasons)

$$
\begin{aligned}
\begin{pmatrix} i \\ j \\ m \end{pmatrix}^{n+1} &= \begin{pmatrix} i \\ j \\ m \end{pmatrix}^{n} \cdot \begin{pmatrix} i \\ j \\ m \end{pmatrix} \\
&= \begin{pmatrix} i^n + pj\left(\frac{1}{2}i^n \sum_{k=0}^{n-1} i^k - \frac{1}{2}ni^n + m\sum_{k=0}^{n-2}(k+1)i^k\right) \\ j\sum_{k=0}^{n-1} i^k \\ m\sum_{k=0}^{n-1} i^k \end{pmatrix} \cdot \begin{pmatrix} i \\ j \\ m \end{pmatrix} \\
&= \begin{pmatrix} i^{n+1} + pj(\frac{1}{2}i^{n+2}\sum_{k=0}^{n-1} i^k - \frac{1}{2}ni^{n+1} + m(\sum_{k=1}^{n-1} ki^k + \sum_{k=0}^{n-1} i^k)) \\ ij\sum_{k=0}^{n-1} i^k + j \\ i^n m + m\sum_{k=0}^{n-1} i^k \end{pmatrix} \\
&= \begin{pmatrix} i^{n+1} + pj(\frac{1}{2}i^{n+1}\sum_{k=0}^{n} i^k - \frac{1}{2}(n+1)i^{n+1} + m\sum_{k=0}^{n-1}(k+1)i^k) \\ j\sum_{k=0}^{n} i^k \\ m\sum_{k=0}^{n} i^k \end{pmatrix}.
\end{aligned}
$$

Hence, by induction we know it to be true. Now it is an easy, but quite copious, task to calculate $\varphi^n(g)$ by

$$
\begin{aligned}
\varphi^n(g) =& \varphi^n(a)^x\varphi^n(b)^y = \left(a^{i^n+pj\left(\frac{1}{2}i^n\sum_{k=0}^{n-1} i^k - \frac{1}{2}ni^n + m\sum_{k=0}^{n-2}(k+1)i^k\right)} b^{j\sum_{k=0}^{n-1} i^k}\right)^x \left(a^{pm\sum_{k=0}^{n-1} i^k} b\right)^y \\
=& a^{x\left(i^n+pj\left(\frac{1}{2}i^n\sum_{k=0}^{n-1} i^k - \frac{1}{2}ni^n + m\sum_{k=0}^{n-2}(k+1)i^k\right)\right) + \frac{(x-1)x}{2}pi^n j\sum_{k=0}^{n-1} i^k} b^{xj\sum_{k=0}^{n-1} i^k} a^{ypm\sum_{k=0}^{n-1} i^k} b^y \\
=& a^{x\left(i^n+pj\left(\frac{1}{2}i^n\sum_{k=0}^{n-1} i^k - \frac{1}{2}ni^n + m\sum_{k=0}^{n-2}(k+1)i^k\right)\right) + \frac{(x-1)x}{2}pi^n j\sum_{k=0}^{n-1} i^k + ypm\sum_{k=0}^{n-1} i^k} b^{xj\sum_{k=0}^{n-1} i^k + y}.
\end{aligned}
$$

As we will see in the next section we will need to find the elements of order $p$ in this group, i.e. those that fulfill $(i, j, m)^p = (1, 0, 0)$ since that is the identity mapping.

To do this we study

$$(i,j,m)^p = \left( i^p + pj\left(\frac{i^p}{2}\sum_{k=0}^{p-1} i^k + m\sum_{k=0}^{p-2}(k+1)i^k\right), j\sum_{k=0}^{p-1} i^k, m\sum_{k=0}^{p-1} i^k \right).$$

The first coordinate is of the form $i^p + p\alpha$ for some $\alpha$ and since $p$ is a zero divisor in the ring $Z_{p^2}$ (and therefore does not have a multiplicative inverse) we must have that

$$i^p \equiv 1 \pmod{p^2} \text{ and } \alpha \equiv 0 \pmod{p}.$$

That implies that $i = 1 + pr$ for some $r \in Z_p$. Plugging that in gives
(with $(1+pr) \equiv 1 \pmod{p}$)

$$\begin{aligned}(1+pr,j,m)^p &= \left(1 + p^2 r + pj\left(\frac{1}{2}\sum_{k=0}^{p-1} 1 + m\sum_{k=0}^{p-2}(k+1)\right), j\sum_{k=0}^{p-1} 1, m\sum_{k=0}^{p-1} 1\right)\\ &= \left(1 + pj\left(\frac{1}{2}p + m\frac{p(p-1)}{2}\right), jp, mp\right)\\ &= \big(1 + p^2(...), 0, 0\big)\\ &= (1,0,0)\end{aligned}$$

so we do not have any requirements on $j$ and $m$. Therefore, we have found all elements of order $p$ to be of the form $(1+pr,j,m)$ with $r,j,m \in Z_p$ with the exception that $r = j = m = 0$ is not allowed. Now we can finally write what the power of an automorphism of order $p$ maps an arbitrary element $g$ on. Let $\varphi$ be an element of order $p$, i.e. $\varphi \leftrightarrow (1+pr,j,m)$. Then we get

$$\begin{aligned}\varphi^n(g) &= a^{x\left((1+pr)^n + pj\left(\frac{1}{2}\sum_{k=0}^{n-1} 1 - \frac{1}{2}n + m\sum_{k=0}^{n-2}(k+1)\right)\right) + \frac{(x-1)x}{2}pj\sum_{k=0}^{n-1} 1 + ypm\sum_{k=0}^{n-1} 1} b^{xj\sum_{k=0}^{n-1} 1 + y}\\ &= a^{x\left(1 + npr + pj\left(\frac{1}{2}n - \frac{1}{2}n + m\frac{(n-1)n}{2}\right)\right) + \frac{(x-1)x}{2}pjn + ypmn} b^{xjn+y}\\ &= a^{x + p\left(nxr + pjmx\frac{(n-1)n}{2} + \frac{(x-1)x}{2}nj + ynm\right)} b^{xjn+y}.\end{aligned}$$

### 1.5.2 The automorphism group of $Z_{p^2} \times Z_p$

Now we will study the automorphism group of $Z_{p^2} \times Z_p$ which has the presentation

$$Z_{p^2} \times Z_p \cong \langle a,b : a^{p^2} = 1, b^p = 1, ab = ba\rangle.$$

Let $\varphi \in \mathrm{Aut}(Z_{p^2} \times Z_p)$. Since $\varphi$ is an isomorphism it has to map the generators such that the presentation does not change, i.e.

$$\langle a,b : a^{p^2} = 1, b^p = 1, ab = ba\rangle \overset{\varphi}{\mapsto} \langle \varphi(a), \varphi(b) : \varphi(a)^{p^2} = 1, \varphi(b)^p = 1, \varphi(a)\varphi(b) = \varphi(b)\varphi(a)\rangle.$$

Let $\varphi$ be defined by

$$\varphi : \begin{cases} a \mapsto a^i b^j & \text{where} \quad i,k \in Z_{p^2} \\ b \mapsto a^k b^l & \qquad\quad\; j,l \in Z_p, \end{cases}$$

and as always, since $\varphi$ is an automorphism, it has to satisfy the relations of the group. First of all that means that the element $a^i b^j$ must have order $p^2$, not $p$. That gives that

$$(a^i b^j)^p \neq 1 \quad \Rightarrow \quad a^{pi} \neq 1,$$

so $i \not\equiv 0 \pmod{p}$. Secondly, the element $a^k b^l$ must have order $p$

$$(a^k b^l)^p = 1 \quad \Rightarrow \quad a^{pk} = 1.$$

Therefore we have that $k = pm$ for some $m \in Z_p$. The last relation does not yield any further information since any two elements in the group will commute. The only thing left is to make sure that $\varphi$ is a bijection. That will hold true if and only if

$$\langle \varphi(a) \rangle \cap \langle \varphi(b) \rangle = 1.$$

That implies that the elements of order $p$ in $\langle \varphi(a) \rangle$ does not lie in $\langle \varphi(b) \rangle$. There are $p-1$ elements in $Z_{p^2}$ of order $p$ and they are of the form $g^{np}$ where $g$ is a generator of the group and $n \in Z_p$. Our choice of generator is $a^i b^j$ for which we have

$$(a^i b^j)^{np} = a^{inp}, \quad n \in Z_p.$$

From this we can conclude that

$$\langle a^{inp} \rangle \cap \langle a^{pm} b^l \rangle = 1 \qquad \Leftrightarrow \qquad l \not\equiv 0 \pmod{p}.$$

These constraint we have deduced gives the total structure of the automorphism group and every automorphism is defined by these factors. So $\varphi$ must actually be defined by

$$\varphi : \begin{cases} a \mapsto a^i b^j & \text{where} \quad i \in Z_{p^2} \text{ and } i \not\equiv 0 \pmod{p} \\ b \mapsto a^{pm} b^l & \qquad\quad\; m,j,l \in Z_p \text{ and } l \not\equiv 0 \pmod{p}. \end{cases}$$

From this we can calculate the order of the group. There are $(p^2 - p)$ choices for $i$, $p$ choices for $j$ and $m$ and $p-1$ choices for $l$. In total that gives

$$|\mathrm{Aut}(Z_{p^2} \times Z_p)| = (p^3 - p^2)(p^2 - p) = p^3(p-1)^2.$$

Lastly we want to see how the operation in the automorphism group is expressed. Therefore we take another automorphism, $\sigma$, defined by

$$\sigma : \begin{cases} a \mapsto a^{i'} b^{j'} & \text{where} \quad i' \in Z_{p^2} \text{ and } i' \not\equiv 0 \pmod{p} \\ b \mapsto a^{pm'} b^{l'} & \qquad\quad\; m',j',l' \in Z_p \text{ and } l' \not\equiv 0 \pmod{p} \end{cases}$$

and study the composition of $\sigma$ and $\varphi$ as follows

$$\sigma \circ \varphi(a) = \sigma(a^i b^j) = ... = a^{ii'+pjm'} b^{ij'+jl'},$$
$$\sigma \circ \varphi(b) = \sigma(a^{pm} b^l) = ... = a^{p(mi'+lm')} b^{ll'}.$$

As the case were in the previous section we can represent an automorphism by the exponential factors it maps the generators on. We will therefore denote an automorphism, $\varphi$, with

$$\varphi \leftrightarrow \begin{pmatrix} i & j \\ m & l \end{pmatrix}$$

where we collect the $i, j, k, l$ in a 2 by 2 matrix for stylistic effects only. So now we can express our operation in the group by this representation

$$\begin{pmatrix} i' & j' \\ m' & l' \end{pmatrix} \circ \begin{pmatrix} i & j \\ m & l \end{pmatrix} = \begin{pmatrix} ii' + pjm' & ij' + jl' \\ mi' + lm' & ll' \end{pmatrix}.$$

It is not hard to prove that

$$\begin{pmatrix} i & j \\ m & l \end{pmatrix}^n = \begin{pmatrix} i^n + pjm \sum_{k=1}^{n-1} (n-k) i^{n-1-k} l^k & j \sum_{k=0}^{n-1} i^{n-1-k} l^k \\ m \sum_{k=0}^{n-1} i^{n-1-k} l^k & l^n \end{pmatrix}$$

and from this we can find that the elements of order $p$ (with the same methods as with $\mathrm{Aut}(Z_{p^2} \rtimes Z_p)$) and get that $i = 1 + pr$ for some $r \in Z_p$, $l = 1$ and $j, m$ are free. So any element of order $p$ is of the form

$$\begin{pmatrix} i & j \\ m & l \end{pmatrix} = \begin{pmatrix} 1 + pr & j \\ m & 1 \end{pmatrix}$$

where $r, j, m \in Z_p$ with the exception that all of them can not be zero since that gives an element of order 1. Similar to what we did in the previous section we conclude with calculating the mapping of an arbitrary element $g \in Z_{p^2} \times Z_p$ mapped by a power of an automorphism $\varphi \leftrightarrow \begin{pmatrix} i & j \\ m & l \end{pmatrix}$ and get

$$\begin{aligned} \varphi^n(g) &= \varphi^n(a)^x \varphi^n(b)^y = \\ &= (a^{i^n + pjm \sum_{k=1}^{n-1} (n-k) i^{n-1-k} l^k} b^{j \sum_{k=0}^{n-1} i^{n-1-k} l^k})^x (a^{pm \sum_{k=0}^{n-1} i^{n-1-k} l^k} b^{l^n})^y = \\ &= a^{xi^n + pxjm \sum_{k=1}^{n-1} (n-k) i^{n-1-k} l^k + pym \sum_{k=0}^{n-1} i^{n-1-k} l^k} b^{xj \sum_{k=0}^{n-1} i^{n-1-k} l^k + yl^n}. \end{aligned}$$

### 1.5.3 The automorphism group of $(Z_p \times Z_p) \rtimes Z_p$

It will show that we will not need the structure of this group as we progress but we will study some of the most basic structures non the less. By equal calculations as with the previous sections we can deduce that the relations of $(Z_p \times Z_p) \rtimes Z_p$ with the generators $a = ((1,0),0), b = ((0,1),0)$ and $c = ((0,0),1)$ which yields

$$(Z_p \times Z_p) \rtimes Z_p \cong \langle a, b, c : a^p = 1, b^p = 1, c^p = 1, ba = ab, ca = abc, cb = bc \rangle.$$

From this it is straight forward to find the formula for the following expressions

$$c^i a^j = a^j b^{ij} c^i,$$

$$(a^i c^j)^n = a^{ni} b^{ij \frac{n(n-1)}{2}} c^{nj}.$$

Let $\varphi \in \mathrm{Aut}((Z_p \times Z_p) \rtimes Z_p)$ be defined by

$$\varphi : \begin{cases} a \mapsto a^i b^j c^k & \text{where} \quad i,j,k \in Z_p \\ b \mapsto a^l b^m c^n & \qquad\quad l,m,n \in Z_p \\ c \mapsto a^q b^r c^s & \qquad\quad q,r,s \in Z_p \end{cases}$$

Since $\varphi$ will have to uphold the relations we must have that $\varphi(c)\varphi(a) = \varphi(a)\varphi(b)\varphi(c)$ so

$$\begin{aligned} (a^q b^r c^s)(a^i b^j c^k) &= (a^i b^j c^k)(a^l b^m c^n)(a^q b^r c^s) \\ \Leftrightarrow b^{si} &= a^l b^{m+lk+qn+kq} c^n. \end{aligned}$$

Because of the fact that we have chosen the generators so that they can uniquely express every element in the group we must have the demand $l = n = 0$.

$$\begin{aligned} b^{si} &= b^{m+kq} \\ \Rightarrow m &\equiv si - kq \pmod{p} \end{aligned}$$

If $m = 0$ we will have that $\varphi(b)$ does not have order $p$ so we can also say that

$$m \equiv si - kq \not\equiv 0 \pmod{p}.$$

The abelian relations will give redundant information and so we will not discuss those here. Therefore we have that $l = n = 0$ and $m = si - kq \neq 0$ are the only constraints we must place on the homomorphism to satisfy the relations of the group. Now we only have to see when it is bijective. Since we are talking about finite groups it is

enough to show that it is injective and so we can show that the kernel is trivial. Lets take some element in $(Z_p \times Z_p) \rtimes Z_p$, say $a^x b^y c^z$, and suppose it is mapped to zero.

$$\varphi(a^x b^y c^z) = \varphi(a)^x \varphi(b)^y \varphi(c)^z = ... = \\ = a^{xi+qz} b^{y(si-kq)+jx+sz+ki\frac{x(x-1)}{2}+qs\frac{z(z-1)}{2}+qzkx} c^{kx+sz} = 0.$$

This leads us to a system of equations (all calculated over $Z_p$)

$$\begin{cases} xi + qz = 0, \\ kx + sz = 0, \\ y(si - kq) + jx + sz + ki\frac{x(x-1)}{2} + qs\frac{z(z-1)}{2} + qzkx = 0. \end{cases}$$

The first two give rise to

$$z(si - kq) = 0$$

and since we must have $(si - kq) \neq 0$ it follows that $z = 0$. From that we can also deduce that $x = 0$ and finally

$$y(si - kq) = 0 \quad \Rightarrow \quad y = 0.$$

So if $g \in (Z_p \times Z_p) \rtimes Z_p$ and $\varphi(g) = 0$ it must be that $g = 0$, hence the kernel is trivial and $\varphi$ is an automorphism with the constraints we have already deduced. Now it is an easy task to calculate the order of the automorphism group. We have $p$ choices for both $j$ and $r$, furthermore $i, k, q, s$ will in some sense be equivalent to a matrix in $GL_2(\mathbb{F}_p)$ since we have that the determinant of $\begin{pmatrix} i & k \\ q & s \end{pmatrix}$ is kept from zero so that will give us $(p^2 - 1)(p^2 - p)$ choices for those elements and in total we get

$$|\mathrm{Aut}((Z_p \times Z_p) \rtimes Z_p)| = p^3(p - 1)(p^2 - 1).$$

To find the structure of the group we can study the operation in the group, just as we did when looking at $\mathrm{Aut}(Z_{p^2} \rtimes Z_p)$. Take two automorphisms of the group, $\sigma, \omega \in \mathrm{Aut}((Z_p \times Z_p) \rtimes Z_p)$, defined by

$$\sigma : \begin{cases} a \mapsto a^i b^j c^k \\ b \mapsto b^{si-kq} \\ c \mapsto a^q b^r c^s \end{cases} \qquad \omega : \begin{cases} a \mapsto a^{i'} b^{j'} c^{k'} \\ b \mapsto b^{s'i'-k'q'} \\ c \mapsto a^{q'} b^{r'} c^{s'} \end{cases}$$

The composition of the two yields

$$\omega \circ \sigma(a) = \omega(a^i b^j c^k) = ... = a^{ii'+kq'} b^{ij'+j(s'i'-k'q')+kr'+i'k'\frac{i(i-1)}{2}+q's'\frac{k(k-1)}{2}+ikk'q'} c^{ik'+ks'}, \\ \omega \circ \sigma(c) = \omega(a^q b^r c^s) = ... = a^{qi'+sq'} b^{qj'+r(s'i'-k'q')+sr'+i'k'\frac{q(q-1)}{2}+q's'\frac{s(s-1)}{2}+qsk'q'} c^{qk'+ss'}.$$

In the same way as with the elements of $\mathrm{Aut}(Z_{p^2} \rtimes Z_p)$ the elements of this group can be represented by the six exponential components, i.e.

$$\varphi \leftrightarrow \begin{pmatrix} i & j & k \\ q & r & s \end{pmatrix}.$$

Where we write it as a 2 by 3 matrix merely for stylistic reasons. Hence we can express the operation of two automorphisms as

$$\begin{pmatrix} i' & j' & k' \\ q' & r' & s' \end{pmatrix} \circ \begin{pmatrix} i & j & k \\ q & r & s \end{pmatrix} = \\ = \begin{pmatrix} ii' + kq' & ij' + jm' + kr' + i'k'\frac{i(i-1)}{2} + q's'\frac{k(k-1)}{2} + ikk'q' & ik' + ks' \\ qi' + sq' & qj' + rm' + sr' + i'k'\frac{q(q-1)}{2} + q's'\frac{s(s-1)}{2} + qsk'q' & qk' + ss' \end{pmatrix}.$$

## 1.6 The groups of order $p^4$

For any prime $p$, there are 5 abelian groups of order $p^4$ up to isomorphisms, namely

$$Z_{p^4},\ Z_{p^3} \times Z_p,\ Z_{p^2} \times Z_{p^2},\ Z_{p^2} \times Z_p \times Z_p \text{ and } Z_p \times Z_p \times Z_p \times Z_p.$$

Here we will try to structure all of the non-abelian groups as well.

### 1.6.1 The special case $p = 2$

As we have already seen, the prime $p = 2$ is a very special prime and since the calculations are a bit extensive we will be more interested in the general case. From [3] we know that there are 14 non-isomorphic groups of order $2^4 = 16$ and we will not delve further into this special case than so. From [3] we can also see that there are precisely 15 non-isomorphic groups of order $p^4$ when $p$ is not equal to 2. So there are not even the same number of non-isomorphic groups and it is clear that this is really a very special case.

### 1.6.2 $p$ being any odd prime

As stated in the previous section we know that there are 15 different groups of order $p^4$ when $p$ is any odd prime. From the section in which we structured the groups of order $p^3$ we learned that it is most difficult to show when two groups are isomorphic and we will therefore not try to do that here. We will instead henceforth use the result of [3] which tells us the generators and relations for the different groups and we will try to find semi-direct products relating to them. With the information in [3] we formulate the following theorem. Note that the relations are not directly copied

from [3] but have been rewritten to be in a more intuitive form. This has been done by trivial operations such as replacing $b$ with $b^{-1}$.

**Theorem 1.6.1** (Burnside)**.** *If $p$ is a prime greater than two, then there are* 15 *groups of order $p^4$ up to isomorphisms. Five of those are abelian and the non-abelian groups are found in the list below. We enumerate them starting from* (vi) *to remember the five abelian groups.*

(vi) $\langle a, b : a^{p^3} = b^p = 1, ba = a^{1+p^2}b\rangle$

(vii) $\langle a, b, c : a^{p^2} = b^p = c^p = 1, cb = a^p bc, ab = ba, ac = ca\rangle$

(viii) $\langle a, b : a^{p^2} = b^{p^2} = 1, ba = a^{1+p}b\rangle$

(ix) $\langle a, b, c : a^{p^2} = b^p = c^p = 1, ca = a^{1+p}c, ba = ab, cb = bc\rangle$

(x) $\langle a, b, c : a^{p^2} = b^p = c^p = 1, ca = abc, ab = ba, bc = cb\rangle$

(xi) $\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = abc, cb = bc\rangle$

(xii) **if** $p = 3$ $\langle a, b, c : a^{p^2} = b^p = 1, c^p = a^p, ab = ba^{1+p}, ac = cab^{-1}, cb = bc\rangle$

**if** $p > 3$ $\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = a^{1+p}bc, cb = a^p bc\rangle$

(xiii) **if** $p = 3$ $\langle a, b, c : a^{p^2} = b^p = 1, c^p = a^{-p}, ab = ba^{1+p}, ac = cab^{-1}, cb = bc\rangle$

**if** $p > 3$ $\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = a^{1+dp}bc,$
$, cb = a^{dp}bc, d \not\equiv 0, 1 \pmod p\rangle$

(xiv) $\langle a, b, c, d : a^p = b^p = c^p = d^p = 1, dc = acd, bd = db, ad = da,$
$, bc = cb, ac = ca, ab = ba\rangle$

(xv) **if** $p = 3$ $\langle a, b, c : a^{p^2} = b^p = c^p = 1, ab = ba, ac = cab, bc = ca^{-p}b\rangle$

**if** $p > 3$ $\langle a, b, c, d : a^p = b^p = c^p = d^p = 1, dc = bcd, db = abd, ad = da,$
$, bc = cb, ac = ca, ab = ba\rangle$

*Observation.* We see that we get an exception when $p = 3$. Since this a special case we will just as with $p = 2$ neglect this and instead focus on the more general cases. So from here on we will assume $p > 3$ in this chapter.

*Example* 1.6.2. Just as an example we can show why we have the constraint $p > 3$ for the group (xv)

$$\langle a, b, c, d : a^p = b^p = c^p = d^p = 1, ba = ab, ca = ac, da = ad, cb = bc, db = abd, dc = bcd \rangle.$$

We investigate the order of the element $abcd$ and find

$$(abcd)^n = a^{n+\frac{(n-1)n(n+1)}{6}} b^{n+\frac{n(n-1)}{2}} c^n d^n$$

with the proof being an easy exercise in induction. Therefore we have that

$$(abcd)^p = a^{p+\frac{(p-1)p(p+1)}{6}} b^{p+\frac{p(p-1)}{2}} c^p d^p = a^{\frac{(p-1)p(p+1)}{6}} = \begin{cases} a^4 = a \neq 1 & \text{if } p = 3 \\ 1 & \text{else} \end{cases}$$

and so this group has an element of order $p^2$ if $p = 3$ and in this case coincides with some other of the non-abelian groups. Take notice that I did not show the last part of my statement, I merely showed why the special case occurred.

### 1.6.3 The general case $p > 3$

Finding semi-direct products relating to the presentations in [3] can be done by simple experimentation. The result from this study is found below. Notice that we will not let $\varphi$ be a trivial mapping even if we may not stress this at all times. We will in the following text consequently take some generators for the groups we are studying, naming them $a, b, c, ...$ with $a$ having a one in the first component with zeros elsewhere, $b$ having a one in the second component with zeros elsewhere and so on. Furthermore, when we below use the notation of raising an integer to the power of an element in a cyclic group it will be implied that we represent the elements by integers as well.

**Proposition 1.6.3.** *$Z_{p^3} \rtimes_\varphi Z_p$ is isomorphic to* (vi) *for all $\varphi : Z_p \mapsto \mathrm{Aut}(Z_{p^3})$.*

*Proof.* From Section 1.3.1 we have that $\mathrm{Aut}(Z_{p^3}) \cong \mathbb{Z}^*_{p^3}$ which is an abelian group of order $p^2(p-1)$. Therefore there exists a nontrivial $\varphi$ mapping onto a subgroup of $\mathrm{Aut}(Z_{p^3})$ with order $p$. Since the group is cyclic there can only be one subgroup of order $p$ so there is only one choice of $\varphi$ up to the choice of generator. A subgroup of $\mathbb{Z}^*_{p^3}$ of order $p$ is the group generated by $(1 + p^2)$. Hence, from Theorem 1.2.7, we have that $Z_{p^3} \rtimes Z_p$ with operation

$$(x, y) * (x', y') = (x + (1 + p^2)^y x', y + y') = (x + x' + yx'p^2, y + y')$$

is the only group that can be structured in this way up to isomorphism. Now we will find the relations for this group based on some generators. Taking the intuitive choice gives us $a = (1, 0)$ and $b = (0, 1)$. It is clear that $a$ has order $p^3$ and $b$ has order $p$ and also that any element in $Z_{p^3} \rtimes_\varphi Z_p$ can be written on the form $a^i b^j$ for some $i, j$. Furthermore it is easy to find that

$$\begin{aligned} a * b &= (1, 0) * (0, 1) = (1, 1), \\ b * a &= (0, 1) * (1, 0) = (1 + p^2, 1) = (p^2, 0)(1, 1) = a^{p^2+1} * b, \end{aligned}$$

so this group can be written as

$$\langle a, b : a^{p^3} = b^p = 1, ba = a^{1+p^2} b \rangle,$$

which we see is the one numbered (vi) in Theorem 1.6.1. ⧛

**Proposition 1.6.4.** *$(Z_{p^2} \times Z_p) \rtimes_\varphi Z_p$ with $\varphi(z)(x', y') = (x' + pzy', y')$ is isomorphic to* (vii).

*Proof.* From Section 1.5.2 we have that any automorphism $\varphi(z)$ of order $p$ is of the form $\begin{pmatrix} 1 + pr & j \\ m & 1 \end{pmatrix}$ with $r, j, m \in Z_p$ not all zero. One can for example choose

$$\varphi(z) \leftrightarrow \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^z$$

which gives the mapping $\varphi(z)(x', y') = (x' + pzy', y')$ and operation

$$((x, y), z) * ((x', y'), z') = ((x + x' + pzy', y + y'), z + z')$$

We then get the relations

$$\begin{cases} b * a = ((0, 1), 0) * ((1, 0), 0) = ((1, 1), 0) = a * b, \\ c * a = ((0, 0), 1) * ((1, 0), 0) = ((1, 0), 1) = a * c, \\ c * b = ((0, 0), 1) * ((0, 1), 0) = ((p, 1), 1) = a^p * b * z. \end{cases}$$

From the calculations above we get the following presentation of the group

$$\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = ab, ac = ca, cb = a^p bc \rangle,$$

and we see that it is equal to (vii) in Theorem 1.6.1. ⧛

**Proposition 1.6.5.** *$Z_{p^2} \rtimes_\varphi Z_{p^2}$ is isomorphic to* (viii) *for all $\varphi : Z_{p^2} \mapsto \mathrm{Aut}(Z_{p^2})$.*

*Proof.* With the same procedure as above we have that $\mathrm{Aut}(Z_{p^2}) \cong \mathbb{Z}_{p^2}^*$ is a group of order $p(p-1)$. From the first isomorphism theorem we must therefore have that both $\ker(\varphi)$ and $\mathrm{im}(\varphi)$ has order $p$ and so, since by Sylow's theorem, we have that every subgroup of order $p$ is conjugate, Theorem 1.2.7 tells us that there is only one such semi-direct product up to isomorphism regardless of the choice of $\varphi$. One element of order $p$ is $(1+p)$ which constructs the operation

$$(x,y) * (x',y') = (x + (1+p)^y x', y + y') = (x + x' + yx'p, y + y').$$

As above we take generators for the group and try to find relations for these. With $a = (1,0)$ and $b = (0,1)$ it is easy to see that they both have order $p^2$ and that they can generate the whole group. The relation between them is

$$b * a = (0,1) * (1,0) = (1+p, 1) = a^{p+1} * b$$

so this group can be written as

$$\langle a, b : a^{p^2} = b^{p^2} = 1, ba = a^{1+p}b \rangle.$$

This is the same presentation as (viii). ⨳

**Proposition 1.6.6.** $(Z_{p^2} \rtimes Z_p) \times Z_p$ *is isomorphic to* (ix).

*Proof.* That there is only one group written as this up to isomorphisms is clear. The operation in the group can be written (using the results of $Z_{p^2} \rtimes Z_p$) as

$$((x,y),z) * ((x',y'),z') = ((x,y) * (x',y'), z + z') = ((x + x' + yx'p, y + y'), z + z').$$

Furthermore it is very easy to write this group as generators and relations. Simply

$$\langle a, b : a^{p^2} = b^p = 1, ba = a^{1+p}b \rangle \times \langle c : c^p = 1 \rangle = \\ = \langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ac = ca, bc = cb \rangle$$

and so we see that this group is equal to (ix). ⨳

**Proposition 1.6.7.** $(Z_p \times Z_p) \rtimes_\varphi Z_{p^2}$ *is isomorphic to* (x) *for all* $\varphi : Z_{p^2} \mapsto \mathrm{Aut}(Z_p \times Z_p)$.

*Proof.* From Section 1.3.2 we have that $\mathrm{Aut}(Z_p \times Z_p) \cong GL_2(\mathbb{F}_p)$ which has order $p(p^2-1)(p-1)$ and so we have that both $\ker(\varphi)$ and $\mathrm{im}(\varphi)$ has order $p$ and we know, with Sylow's theorem, that every subgroup of order $p$ is conjugate and then by Theorem 1.2.7 we have that there is only one such semi-direct product up to isomorphism. One subgroup of order $p$ of $GL_2(\mathbb{F}_p)$ is the group generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Therefore

we have that there is only one such semi-direct product, up to isomorphism, and it has the operation

$$((x,y),z)*((x',y'),z') = ((x,y)+(x',y')\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^z, z+z') = ((x+x', y+y'+zx'), z+z').$$

Generators for the group are $a = ((1,0),0)$, $b = ((0,1),0)$ and $c = ((0,0),1)$ with $a^p = b^p = c^{p^2} = 1$. The relations then becomes

$$\begin{cases} b*a = ((0,1),0)*((1,0),0) = ((1,1),0) = a*b, \\ \\ c*a = ((0,0),1)*((1,0),0) = ((1,1),1) = a*b*c, \\ \\ c*b = ((0,0),1)*((0,1),0) = ((0,1),1) = b*c, \end{cases}$$

so therefore we have the group

$$\langle a,b,c : a^p = b^p = c^{p^2} = 1, ab = ba, bc = cb, ca = abc\rangle$$

and this is the same presentation as (x). ⧛

**Proposition 1.6.8.** *$(Z_{p^2} \rtimes Z_p) \rtimes_\varphi Z_p$ with $\varphi(z) \leftrightarrow (1,1,0)^z$ is isomorphic to* (xi).

*Proof.* The operation is by definition of the form

$$((x,y),z)*((x',y'),z') = ((x,y)*\varphi(z)(x',y'), z+z').$$

From Section 1.5.1 we know all possible automorphisms, $\sigma$, that $\varphi(z)$ can map to and they are of the form

$$\varphi(z) = \sigma^z \leftrightarrow (1+pr, j, m)^z.$$

From the same section we have seen what $\sigma^z$ maps any element to by the formula

$$\varphi(z)(a^{x'}b^{y'}) = \sigma^z(a^{x'}b^{y'}) = a^{x'+p\left(zxr+pjmx'\frac{(z-1)z}{2}+\frac{(x'-1)x'}{2}zj+y'zm\right)}b^{x'jz+y'}$$

from which we get the operation

$$\begin{aligned} &((x,y),z)*((x',y'),z') = ((x,y)*\varphi(z)(x',y'), z+z') = \\ &= ((x,y)*(x'+p\left(zxr+pjmx'\frac{(z-1)z}{2}+\frac{(x'-1)x'}{2}zj+y'zm\right), x'jz+y'), z+z') = \\ &= ((x+x'+p\left(zxr+pjmx'\frac{(z-1)z}{2}+\frac{(x'-1)x'}{2}zj+y'zm\right)+pyx', y+x'jz+y'), z+z'). \end{aligned}$$

Setting $(i,j,m) = (1,1,0)$ gives us

$$((x,y),z) * ((x',y'),z') = ((x + x' + pz\frac{x'(x'-1)}{2} + pyx', y + y' + x'z), z + z'),$$

and so we deduce the relations

$$\begin{cases} b * a = ((0,1),0) * ((1,0),0) = ((1+p,1),0) = a^{1+p} * b, \\ c * a = ((0,0),1) * ((1,0),0) = ((1,1),1) = a * b * c, \\ c * b = ((0,0),1) * ((0,1),0) = ((0,1),1) = b * c. \end{cases} .$$

The presentation can therefore be written

$$\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = abc, bc = cb \rangle$$

which is equal to the one numbered (xi) in Theorem 1.6.1. ⧖

**Proposition 1.6.9.** *$(Z_{p^2} \rtimes Z_p) \rtimes_\varphi Z_p$ with $\varphi(z) \leftrightarrow (1,1,1)^z$ is isomorphic to* (xii).

*Proof.* If we in the proof of Proposition 1.6.8 instead of $(i,j,m) = (1,1,0)$ put $(i,j,m) = (1,1,1)$ we get

$$((x,y),z)*((x',y'),z') = ((x+x'+px'\frac{z(z-1)}{2}+pz\frac{x'(x'-1)}{2}+py'z+pyx', y+y'+x'z), z+z')$$

and therefore the relations are

$$\begin{cases} b * a = ((0,1),0) * ((1,0),0) = ((1+p,1),0) = a^{1+p} * b, \\ c * a = ((0,0),1) * ((1,0),0) = ((1,1),1) = a * b * c, \\ c * b = ((0,0),1) * ((0,1),0) = ((p,1),1) = a^p * b * c, \end{cases}$$

which gives ut the presentation

$$\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = abc, cb = a^p bc \rangle.$$

This is not equal to any in the list, however we can rewrite this presentation as follows. Set $\alpha = ab$, $\beta = b$ and $\gamma = c$. We can still write any element in the group as a combination of these three. Furthermore it is clear that $\beta^p = b^p = 1$ and $\gamma^p = c^p = 1$. From previous calculations we have that $\alpha^n = (ab)^n = a^{n+p\frac{n(n-1)}{2}}b^n$ so $\alpha^p = a^p$ and $\alpha^{p^2} = 1$. The relations becomes (from the previous relations we see that $a^p$ lies in the center of the group)

$$\begin{cases} \beta\alpha = bab = a^{1+p}bb = \alpha^{1+p}\beta, \\ \gamma\alpha = cab = abcb = aba^p bc = a^{1+p}bbc = \alpha^{1+p}\beta\gamma, \\ \gamma\beta = cb = a^p bc = \alpha^p\beta\gamma. \end{cases}$$

Renaming $\alpha, \beta, \gamma$ with $a, b, c$ we get the presentation

$$\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = a^{1+p}bc, cb = a^p bc\rangle$$

which is the same presentation as (xii) for $p > 3$. ⨳

**Proposition 1.6.10.** *$(Z_{p^2} \rtimes Z_p) \rtimes_\varphi Z_p$ with $\varphi(z) \leftrightarrow (1, 1, d)^z$ where $d \not\equiv 0, 1 \pmod p$ is isomorphic to* (xiii).

*Proof.* From the proof of Proposition 1.6.9 above we can see that if we instead set $(i, j, m) = (1, 1, d)$ with $d \not\equiv 0, 1 \pmod p$ we get

$$((x, y), z)*((x', y'), z') = ((x+x'+px'd\frac{z(z-1)}{2}+pz\frac{x'(x'-1)}{2}+pdy'z+pyx', y+y'+x'z), z+z').$$

Hence the relations will be

$$\begin{cases} b * a = ((0, 1), 0) * ((1, 0), 0) = ((1 + p, 1), 0) = a^{1+p} * b, \\ \\ c * a = ((0, 0), 1) * ((1, 0), 0) = ((1, 1), 1) = a * b * c, \\ \\ c * b = ((0, 0), 1) * ((0, 1), 0) = ((dp, 1), 1) = a^{dp} * b * c, \end{cases}$$

and so, we have the presentation

$$\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = abc, cb = a^{dp}bc\rangle.$$

Similar to what we did above, setting $\alpha = ab$, $\beta = b$ and $\gamma = c$ gives us that the order of $\alpha$ is $p^2$, $\beta$ is $p$ and $\gamma$ is $p$. Furthermore, we get that

$$\begin{cases} \beta\alpha = bab = a^{1+p}bb = \alpha^{1+p}\beta, \\ \gamma\alpha = cab = abcb = aba^{dp}bc = a^{1+dp}bbc = \alpha^{1+p}\beta\gamma, \\ \gamma\beta = cb = a^{dp}bc = \alpha^{dp}\beta\gamma. \end{cases}$$

Again, renaming $\alpha, \beta, \gamma$ with $a, b, c$ when writing the presentation gives us

$$\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = a^{1+dp}bc, cb = a^{dp}bc\rangle$$

which is the same as (xiii) for $p > 3$. ⨳

**Notation.** In order to make a difference between the three semi-direct products above we shall in the future denote the homomorphisms in the semi-direct products for (xi), (xii), (xiii) as $\varphi_1$, $\varphi_2$, $\varphi_3$ respectively.

**Proposition 1.6.11.** *$((Z_p \times Z_p) \rtimes Z_p) \times Z_p$ is isomorphic to* (xiv).

*Proof.* This group can be studied in the same way as the group studied in Proposition 1.6.6. The operation can be written

$$\begin{aligned}(((x,y),z),w)*(((e,f),g),h) &= (((x,y),z)*((x',y'),z'),w+w')\\ &= (((x+x',y+y'+zx'),z+z'),w+w')\end{aligned}$$

and the presentation follows from

$$\begin{aligned}&\langle a,b,c : a^p=b^p=c^p=1, ba=ab, bc=cb, ca=bac\rangle \times \langle d : d^p=1\rangle =\\ &= \langle a,b,c,d : a^p=b^p=c^p=d^p=1, ba=ab, bc=cb, ca=bac, ad=da, bd=db, cd=dc\rangle.\end{aligned}$$

This is the same presentation as (xiv). ⧖

**Proposition 1.6.12.** *$(Z_p \times Z_p \times Z_p) \rtimes_\varphi Z_p$ with*

$$\varphi(w)(x',y',z') = (x'+y'w+z'\frac{w(w-1)}{2}, y'+z'w, z')$$

*is isomorphic to* (xv).

*Proof.* $\varphi : Z_p \mapsto \mathrm{Aut}(Z_p \times Z_p \times Z_p)$. Since $\mathrm{Aut}(Z_p \times Z_p \times Z_p) \cong GL_3(\mathbb{F}_p)$ we can simply choose some matrix with order $p$ as our representation of $\varphi$ and see what presentations we get. With the choice

$$\varphi(w) \leftrightarrow \begin{pmatrix}1&0&0\\1&1&0\\0&1&1\end{pmatrix}^w$$

we get that the automorphism will map a triple $(x',y',z')$ as follows

$$\varphi(w)(x',y',z') = (x',y',z')\begin{pmatrix}1&0&0\\1&1&0\\0&1&1\end{pmatrix}^w = (x'+y'w+z'\frac{w(w-1)}{2}, y'+z'w, z').$$

Then we would have the operation

$$((x,y,z),w)*((x',y',z'),w') = ((x+x'+y'w+z'\frac{w(w-1)}{2}, y+y'+wz', z+z'), w+w')$$

so we get the relations (trivially $a*b=b*a, a*c=c*a, c*b=b*c$)

$$\begin{cases} d*a = ((0,0,0),1)*((1,0,0),0) = ((1,0,0),1) = a*d \\ d*b = ((0,0,0),1)*((0,1,0),0) = ((1,1,0),1) = a*b*d \\ d*c = ((0,0,0),1)*((0,0,1),0) = ((0,1,1),1) = b*c*d \end{cases}.$$

The presentation would then be

$\langle a, b, c, d : a^p = b^p = c^p = d^p = 1, ab = ba, ac = ca, bc = cb, db = abd, dc = bcd, da = ad\rangle$

which is the same as (xv) for $p > 3$. ⧖

We have now found a semi-direct product for all the presentations from [3]. In order to clarify we know summarize our results in the list below.

**The presentations in [3] as semi-direct products**

(vi) $\langle a, b : a^{p^3} = b^p = 1, ba = a^{1+p^2}b\rangle \cong Z_{p^3} \rtimes Z_p$,
with the operation in $Z_{p^3} \rtimes Z_p$ given by

$$(x, y) * (x', y') = (x + x' + yx'p^2, y + y'),$$

cf. Proposition 1.6.3.

(vii) $\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = ab, ca = ac, cb = a^pbc\rangle \cong (Z_{p^2} \times Z_p) \rtimes_\varphi Z_p$
with $\varphi(z)(x', y') = (x' + pzy', y')$ where the operation in $(Z_{p^2} \times Z_p) \rtimes_\varphi Z_p$ is given by

$$((x, y), z) * ((x', y'), z') = ((x + x' + pzy', y + y'), z + z'),$$

cf. Proposition 1.6.4.

(viii) $\langle a, b : a^{p^2} = b^{p^2} = 1, ba = a^{1+p}b\rangle \cong Z_{p^2} \rtimes Z_{p^2}$
with the operation in $Z_{p^2} \rtimes Z_{p^2}$ given by

$$(x, y) * (x', y') = (x + x' + yx'p, y + y'),$$

cf. Proposition 1.6.5.

(ix) $\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = ab, ca = a^{1+p}c, cb = bc\rangle \cong (Z_{p^2} \rtimes Z_p) \times Z_p$
with the operation in $(Z_{p^2} \rtimes Z_p) \times Z_p$ given by

$$((x, y), z) * ((x', y'), z') = ((x + x' + yx'p, y + y'), z + z'),$$

cf. Proposition 1.6.6.

(x) $\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = ab, ca = abc, cb = bc\rangle \cong (Z_p \times Z_p) \rtimes Z_{p^2}$
with the operation in $(Z_p \times Z_p) \rtimes Z_{p^2}$ given by

$$((x, y), z) * ((x', y'), z') = ((x + x', y + y' + zx'), z + z'),$$

cf. Proposition 1.6.7.

(xi) $\langle a,b,c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = abc, cb = bc\rangle \cong (Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_1} Z_p$ with $\varphi_1(z) \leftrightarrow (i,j,m)^z = (1,1,0)^z$ where the operation in $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_1} Z_p$ is given by

$$((x,y),z) * ((x',y'),z') = ((x + x' + pz\frac{x'(x'-1)}{2} + pyx', y + y' + x'z), z + z'),$$

cf. Proposition 1.6.8.

(xii) **if** $p > 3$ $\langle a,b,c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = a^{1+p}bc, cb = a^pbc\rangle \cong$ $\cong (Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_2} Z_p$ with $\varphi_2(z) \leftrightarrow (i,j,m)^z = (1,1,1)^z$ and where the operation in $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_2} Z_p$ is given by

$$\begin{aligned}&((x,y),z) * ((x',y'),z') = \\ &= ((x+x'+px'\frac{z(z-1)}{2}+pz\frac{x'(x'-1)}{2}+py'z+pyx', y+y'+x'z), z+z'),\end{aligned}$$

cf. Proposition 1.6.9.

(xiii) **if** $p > 3$ $\langle a,b,c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = a^{1+dp}bc,$ $, cb = a^{dp}bc, d \not\equiv 0,1 \mod p\rangle \cong (Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_3} Z_p$ with $\varphi_3(z) \leftrightarrow (i,j,m)^z = (1,1,d)^z$ where the operation in $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_3} Z_p$ is given by

$$\begin{aligned}&((x,y),z) * ((x',y'),z') = \\ &= ((x+x'+px'd\frac{z(z-1)}{2}+pz\frac{x'(x'-1)}{2}+pdy'z+pyx', y+y'+x'z), z+z'),\end{aligned}$$

cf. Proposition 1.6.10.

(xiv) $\langle a,b,c,d : a^p = b^p = c^p = d^p = 1, ba = ab, ca = ac, da = ad, cb = bc,$ $, db = bd, dc = acd\rangle \cong ((Z_p \times Z_p) \rtimes Z_p) \times Z_p$ with the operation in $((Z_p \times Z_p) \rtimes Z_p) \times Z_p$ given by

$$(((x,y),z),w) * (((e,f),g),h) = (((x + x', y + y' + zx'), z + z'), w + w'),$$

cf. Proposition 1.6.11.

(xv) **if** $p > 3$ $\langle a,b,c,d : a^p = b^p = c^p = d^p = 1, ba = ab, ca = ac, da = ad,$ $, cb = bc, db = abd, dc = bcd\rangle \cong (Z_p \times Z_p \times Z_p) \rtimes Z_p$ with

$$\varphi(w) \leftrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}^w$$

where the operation in $(Z_p \times Z_p \times Z_p) \rtimes Z_p$ is given by

$$((x,y,z),w) * ((x',y',z'),w') = \\ = ((x+x'+y'w+z'\frac{w(w-1)}{2}, y+y'+wz', z+z'), w+w'),$$

cf. Proposition 1.6.12.

Notice that these do not have to be the only semi-direct products isomorphic to the groups in [3]. We have only showed that there is at least one semi-direct product for every group in the list, not that it is unique. That is actually not even the case as the following example will make clear.

*Example* 1.6.13. Another possibility of a semi-direct product with order $p^4$ would be $(Z_p \times Z_p) \rtimes_\varphi (Z_p \times Z_p)$ with
$\varphi : (Z_p \times Z_p) \mapsto \mathrm{Aut}(Z_p \rtimes Z_p) \cong GL_2(\mathbb{F}_p)$ so lets take a moment to study that. If we choose $\varphi((z,w)) \leftrightarrow \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^z$ we get the the automorphism mapping

$$\varphi((z,w))((x',y')) = (x',y') \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^z = (x'+y'z, y')$$

so therefore we have the operation

$$((x,y),(z,w)) * ((x',y'),(z',w')) = ((x+x'+y'z, y+y'),(z+z',w+w')).$$

With the usual choice of generators we get (trivially $ab = ba, cd = dc$)

$$\begin{cases} c * a = ((0,0),(1,0)) * ((1,0),(0,0)) = ((1,1),(1,0)) = a * c, \\ d * a = ((0,0),(0,1)) * ((1,0),(0,0)) = ((1,0),(0,1)) = a * d, \\ c * b = ((0,0),(1,0)) * ((0,1),(0,0)) = ((1,1),(1,0)) = a * b * c, \\ d * b = ((0,0),(0,1)) * ((0,1),(0,0)) = ((0,1),(0,1)) = b * d, \end{cases}$$

which gives the presentation

$$\langle a,b,c,d : a^p = b^p = c^p = d^p = 1, ba = ab, ca = ac, da = ad, cb = abc, db = bd, dc = cd \rangle.$$

By comparing we see, with the only difference in the presentations being permutations of the generators, that this group is isomorphic to (xiv). That is the same as $((Z_p \times Z_p) \rtimes Z_p) \times Z_p$ was isomorphic to and so we that the factorization of (xiv) into a semi-direct product is not unique.

Table 1.2: Non-isomorphic groups of order $p^4$ ($p > 3$)

| Number | $p$-group | Homomorphism |
|---|---|---|
| (i) | $Z_{p^4}$ | - |
| (ii) | $Z_{p^3} \times Z_p$ | - |
| (iii) | $Z_{p^2} \times Z_{p^2}$ | - |
| (iv) | $Z_{p^2} \times Z_p \times Z_p$ | - |
| (v) | $Z_p \times Z_p \times Z_p \times Z_p$ | - |
| (vi) | $Z_{p^3} \rtimes_\varphi Z_p$ | $\varphi(y) \leftrightarrow (1+p^2)^y$ |
| (vii) | $(Z_{p^2} \times Z_p) \rtimes_\varphi Z_p$ | $\varphi(z) \leftrightarrow \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^z$ |
| (viii) | $Z_{p^2} \rtimes_\varphi Z_{p^2}$ | $\varphi(y) \leftrightarrow (1+p)^y$ |
| (ix) | $(Z_{p^2} \rtimes Z_p) \times Z_p$ | Trivial |
| (x) | $(Z_p \times Z_p) \rtimes_\varphi Z_{p^2}$ | $\varphi(z) \leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^z$ |
| (xi) | $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_1} Z_p$ | $\varphi_1(z) \leftrightarrow (1,1,0)^z$ |
| (xii) | $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_2} Z_p$ | $\varphi_2(z) \leftrightarrow (1,1,1)^z$ |
| (xiii) | $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_3} Z_p$ | $\varphi_3(z) \leftrightarrow (1,1,d)^z$ |
| (xiv) | $((Z_p \times Z_p) \rtimes Z_p) \times Z_p$ | Trivial |
| (xv) | $(Z_p \times Z_p \times Z_p) \rtimes Z_p$ | $\varphi(w) \leftrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}^w$ |

Everything we have deduced from this section can be summarized in the following theorem.

**Theorem 1.6.14.** *If $p$ is a prime greater than three then there are* 15 *non-isomorphic groups of order $p^4$ and all of them are completely factorizable. Furthermore, if $G$ is such a group it is isomorphic to precisely one of the groups found in Table 1.2*

## 1.7 Final notes

### 1.7.1 Methods and generalizations

We have seen that $p$-groups have several nice properties, some of which have been established in Theorem 1.1.2. A group $G$ can be written as a semi-direct product, $H \rtimes K$, if three important conditions are met. First of all, $H$ must be normal in $G$, secondly $H \cap K = 1$ and lastly $G = HK$. In some sense a $p$-group takes one of these requirements out of the equation since we have that there is at least one normal subgroup, $H$, for any possible subgroup order. Therefore we only have to find some

other subgroup, $K$, which is a complement to that one, i.e. $H \cap K = 1$ and $G = HK$. As we have seen it might not always be possible to find such a complement but the "probability" might be a little higher for $p$-groups.

Furthermore, let $G$ be a $p$-group, we have that every subgroup of $G$ is also a $p$-group and especially the kernel of any homomorphism, $\varphi$, taking elements in $G$. From that, and the first isomorphism theorem, one can also deduce that the image of $\varphi$ must also be a $p$-group. This is also an important property since that tells us that if $G \cong H \rtimes_\varphi K$ with $\varphi : K \mapsto \mathrm{Aut}(H)$ we have that $\varphi$ will map onto a $p$-group in the automorphism group. That is a strong restriction we can set and may simplify the procedure.

An important property of the semi-direct product in general can be summarized in the following theorem.

**Theorem 1.7.1.** *If $G \cong H \rtimes_\varphi (K \rtimes_\sigma L)$ then $G \cong (H \rtimes_\alpha K) \rtimes_\beta L$ for some homomorphisms $\alpha$ and $\beta$.*

*Proof.* Denote the operation in $H \rtimes_\varphi (K \rtimes_\sigma L)$ by $*_\varphi$, the operation in $K \rtimes_\sigma L$ as $*_\sigma$, the operation in $H \rtimes_\alpha K$ by $*_\alpha$ and the operation in $(H \rtimes_\alpha K) \rtimes_\beta L$ by $*_\beta$.
Let $\beta : L \mapsto \mathrm{Aut}(H \rtimes_\alpha K)$ be defined by

$$\beta(l) = (\widetilde{\beta}(l), \sigma(l))$$

with which we mean

$$\beta(l)(x, y) = (\widetilde{\beta}(l)(x), \sigma(l)(y))$$

for some $\widetilde{\beta}$. Since $\varphi : (K \rtimes_\sigma L) \mapsto \mathrm{Aut}(H)$ is a homomorphism we have that

$$\varphi((k, l)) = \varphi((k, 0))\varphi((0, l)) = \varphi((1, 0))^k \varphi((0, 1))^l \triangleq \alpha(k)\widetilde{\beta}(l).$$

Hence we see that we can split $\varphi$ into two parts, one depending on $k$ and one depending on $l$ and we choose those as our $\alpha$ and $\widetilde{\beta}$ respectively. Let us now define an isomorphism between $H \rtimes_\varphi (K \rtimes_\sigma L)$ and $(H \rtimes_\alpha K) \rtimes_\beta L$ as

$$\Psi(h, (k, l)) \mapsto ((h, k), l).$$

We have that

$$\begin{aligned}
\Psi\left((h, (k, l)) *_\varphi (h', (k', l'))\right) &= \Psi\left((h \cdot \varphi(k, l)(h'), (k, l) *_\sigma (k', l'))\right) \\
&= \Psi\left((h \cdot \varphi(k, l)(h'), (k \cdot \sigma(l)(k'), l \cdot l'))\right) \\
&= \left((h \cdot \varphi(k, l)(h'), k \cdot \sigma(l)(k')), l \cdot l'\right),
\end{aligned}$$

$$\begin{aligned}
\Psi\left((h,(k,l)) *_\varphi (h',(k',l'))\right) &= \Psi\left((h,(k,l))\right) *_\beta \Psi\left((h',(k',l'))\right) \\
&= ((h,k),l) *_\beta ((h',k'),l') \\
&= ((h,k) *_\alpha \beta(l)(h',k'), l\cdot l') \\
&= \left((h,k) *_\alpha (\widetilde{\beta}(l)(h'), \sigma(l)(k')), l\cdot l'\right) \\
&= \left((h\cdot(\alpha(k)\circ\widetilde{\beta}(l))(h'), k\cdot\sigma(l)(k')), l\cdot l'\right) \\
&= ((h\cdot\varphi(k,l)(h'), k\cdot\sigma(l)(k')), l\cdot l'),
\end{aligned}$$

so this mapping is a homomorphism and since it clearly also is a bijection we have that $\Psi$ is an isomorphism. Hence $H \rtimes_\varphi (K \rtimes_\sigma L) \cong (H \rtimes_\alpha K) \rtimes_\beta L$. ⨳

From this theorem we know that if we can completely factorize a $p$-group into semi-direct products it can always be written as some other $p$-group times some cyclic $p$-group which is quite a strong statement. For example, suppose that we have been able to factorize all $p$-groups of order $p^k$ for all $k < n$ for some $n \in \mathbb{Z}^+$ into semi-direct products. Then we can find all the $p$-groups of order $n$ that can be factorized into semi-direct products by looking at the groups of lower order than $p^n$ taken as a semi-direct product with some cyclic group.

*Example* 1.7.2. Another semi-direct product one could have studied in order to find all the different groups of order $p^4$ was $Z_{p^2} \rtimes_\varphi (Z_p \times Z_p)$ but from the previous theorem we know that this group is isomorphic to $(Z_{p^2} \rtimes Z_p) \rtimes_\sigma Z_p$ for some $\sigma$ and we studied that group instead.

Furthermore we have that a cyclic group is always abelian. This may help us with, for example, determining the center of the group. Let $G \cong H \rtimes_\varphi K$ where $K$ is cyclic. In order to stress the fact that $K$ is abelian we denote the operation in $K$ with "+" and the operation in the not necessarily abelian group $H$ with "$\cdot$". Suppose $(z_1, z_2) \in Z(G)$. Then it has to commute with every element in $G$, especially $(0,k)$ for all $k \in K$

$$\begin{cases}
(z_1,z_2) * (0,k) = (z_1\cdot\varphi(z_2)(0), z_2+k) = (z_1, z_2+k), \\
(0,k) * (z_1,z_2) = (\varphi(k)(z_1), k+z_2) = (\varphi(k)(z_1), z_2+k).
\end{cases}$$

So we must have $z_1 = \varphi(k)(z_1)$ for all $k \in K$ which is the same thing as that the stabilizer of $z_1$ must be the whole of $K$. Now take some element $(h,k) \in H \rtimes_\varphi K$. If $z_1 \in Z(H)$ it must hold that

$$\begin{cases}
(z_1,z_2) * (a,b) = (z_1\cdot\varphi(z_2)(a), z_2+b), \\
(a,b) * (z_1,z_2) = (a\cdot\varphi(b)(z_1), g+z_2) = (a\cdot z_1, z_2+g) = (z_1\cdot a, z_2+g).
\end{cases}$$

That gives us that $\varphi(z_2)(a) = a$ for all $a \in H$. Therefore, $\varphi(z_2)$ must be trivial. So if $z_1 \in Z(H)$, $\varphi(k)(z_1) = z_1$ for all $k \in K$ and $\varphi(z_2) = id$ then we have that $(z_1, z_2)$

lies in the center of $G \cong H \rtimes_\varphi K$, i.e. $(z_1, z_2) \in Z(H \rtimes_\varphi K)$. However we can not be certain that we have found every element in the center. If $z_1 \notin Z(H)$ then we get another, more general, requirement from

$$\begin{cases} (z_1, z_2) * (a, b) = (z_1 \cdot \varphi(z_2)(a), z_2 + b), \\ (a, b) * (z_1, z_2) = (a \cdot \varphi(b)(z_1), g + z_2) = (a \cdot z_1, z_2 + g) = (a \cdot z_1, z_2 + g), \end{cases}$$

which yields $z_1 \cdot \varphi(z_2)(a) = a \cdot z_1$ for all $a \in H$. So in general we can conclude that if $\varphi(k)(z_1) = z_1$ for all $k \in K$ and $z_1 \cdot \varphi(z_2)(a) = a \cdot z_1$ for all $a \in H$ then $(z_1, z_2)$ lies in the center of $H \rtimes_\varphi K$.

As we saw in Example 1.6.13 there can be several ways a group of order $p^4$ can be factorized into semi-direct products, and this will most likely hold true for $p$-groups of order $p^n$ with $n \geq 4$. However, we are yet to see an example of a $p$-group that can be completely factorizable where the cyclic groups in the semi-directs product differs. With that we mean that if $G \cong Z_{p^{i_1}} \rtimes_{\varphi_1} Z_{p^{i_2}} \rtimes_{\varphi_2} ... \rtimes_{\varphi_{n-1}} Z_{p^{i_n}}$ then the semi-direct products is unique in the sense that any other complete factorization of $G$ into semi-direct products will only change the order of the cyclic groups $Z_{p^{i_j}}$ and the homomorphisms $\varphi_j$, not the cyclic groups themselves. From this we state the following:

**Conjecture 1.7.3.** *If a p-group, G, is completely factorizable it will be in a unique way in the sense that if there are two factorizations of G,*

$$G \cong Z_{p^{i_1}} \rtimes_{\varphi_1} Z_{p^{i_2}} \rtimes_{\varphi_2} ... \rtimes_{\varphi_{n-1}} Z_{p^{i_n}} \text{ and}$$

$$G \cong Z_{p^{j_1}} \rtimes_{\widetilde{\varphi}_1} Z_{p^{j_2}} \rtimes_{\widetilde{\varphi}_2} ... \rtimes_{\widetilde{\varphi}_{m-1}} Z_{p^{j_m}},$$

*then $n = m$ and furthermore, disregarding the homomorphisms, the factors, $Z_{p^{j_k}}$, of the second product will only be a permutation of the factors, $Z_{p^{i_k}}$, of the first product.*

# Chapter 2

# Subgroups of $p$-groups

This chapter deals with the subgroup structure of the previously discussed groups. We will also acquire some knowledge of the relation between the different subgroups. The primary approach is, as we will see, based on presentations and almost purely combinatorial.

Throughout the text, $p$ will always be a prime and $G$ will be a group of order $p^n$. As of now, I will also assume that $p > 2$. In every section dealing with a specific group, $G$ will denote the group under discussion.

The central definitions in this chapter are the following:

**Definition 2.0.4.** The number of elements of order $p^k$ in $G$ will be denoted $n_k(G)$. If it is obvious what group is considered, it will be shortened as $n_k = n_k(G)$.

**Definition 2.0.5.** The number of subgroups in $G$ isomorphic with $H$ will be denoted $\mathcal{N}(H, G)$ or in short $\mathcal{N}(H)$ when it is clear what group $G$ we are working with.

Most of our work in this chapter will consist of determining $n_i(G)$ for different $i \in \mathbb{N}$ and $\mathcal{N}(H, G)$ for different $H$, for each of the groups discussed in the previous chapter.

## 2.1 Combinatorial methods

In this section we will present some of the methods that we will use in the subsequent sections where we are determining subgroup structure of the $p$-groups discussed in the previous chapter.

The theory used can be found for example in *Abstract Algebra* by David S. Dummit and Richard M. Foote [5] or *A First Course in Abstract Algebra* by J.B. Fraleigh [6] or any other first-course literature in Abstract Algebra.

### 2.1.1 A method for counting subgroups

It is well known that every group $G$ can be completely described by a presentation. But just as there are different ways of expressing a group $G$ in term of set and operation, there are several different presentations of any given group.

$G$ is isomorphic with a group $G' = \langle a, b, ... : R\rangle$ if and only if we in $G$ can find elements fulfilling all the relations $R$ and those elements generate a group of order $|G| = |G'|$. This can be rephrased in many equivalent ways, but it is always necessary that there exist elements in $G$ satisfying the relations of the presentation. That is also our primary concern, since it is usually the hardest task when showing isomorphism of presentations.

For abelian groups $\langle a, b... : a^{\alpha_1} = b^{\alpha_2} = ... = 1, ab = ba, ac = ca, ab = ba, ...\rangle$ it is then sufficient to show isomorphism by finding elements of the right order that all commute with each other (assuming that we do not choose elements that don't generate a group of the right order), since all the relations are then satisfied.

Similarly, showing that a group $G$ has a group $H$ as a subgroup is equivalent to the problem of finding generators in $G$ such that the relations of $H$ are satisfied. Now we don't need that these generators generate a group of order $|G|$, but merely a group of order $|H|$.

The main theme in this chapter is to determine $\mathcal{N}(H)$. The idea is to use generators and the method is purely combinatorial: count the number of ways of forming subgroups isomorphic with $H$ and then divide by the number of ways of forming the very same subgroup, to prevent so called "double-counting". Rephrased: Count the number of ways of choosing generators for $H$ from the elements of $G$ and then divide by the number of ways of choosing generators for $H$ from the elements of $H$ itself. One advantage with this method is that we will be sure that we have found *every* subgroup isomorphic with $H$ since we have "tried" every possibility.

Remember now that a homomorphism is completely determined by where the generators of the domain-group are mapped. If we also assume that the homomorphism is injective, then we know that the group structure will be preserved. We therefore see that counting generators of $H$ in $G$ is the same as counting injective homomorphisms from $H$ to $G$, but with one important exception. When we are constructing homomorphisms we must choose the set of generators as an ordered set, since permuting structurally similar generators actually gives another homomorphism. I give an example of this for clarification.

*Example* 2.1.1. Let $\varphi$ be an injective homomorphism from $Z_p \times Z_p$ to $Z_p \times Z_p$. If we choose generators $a$ and $b$ in the domain, then the following automorphisms are obviously different:

$$\begin{cases} a \to a \\ b \to b \end{cases}$$

and

$$\begin{cases} a \to b \\ b \to a\,. \end{cases}$$

We see that there is an essential difference in choosing generators of the codomain as $\{a, b\}$ and $\{b, a\}$. We are therefore double-counting whenever we have multiple generators that are interchangeable in the relations of the presentation!

Note now that when choosing a set of generators of $H$ in the original problem, the set is not ordered. It seems as the problem of finding generators for $H$ is not the same as counting homomorphisms; one set is ordered and the other is not. This problem is however easily solved since we will divide the number of injective homomorphisms from $H$ to $G$ with the number of injective homomorphisms from $H$ to $H$. The domain in both cases are $H$, so if we divide by the number of permutations of similar generators, we will divide by the same number in both the numerator and the denominator. The fraction thus stays the same and we conclude that it doesn't matter if we count the sets of generators as an ordered or unordered set, as long as we do the same for both the homomorphisms from $H$ to $G$ and the homomorphisms from $H$ to $H$.

The problem of finding the number of subgroups isomorphic with $H$ in a group $G$ is now reduced to a problem of counting the number of ways of choosing an ordered set of generators for $H$ from the elements of $G$ and also the number of ways of choosing an ordered set of generators for $H$ from the elements of $H$ itself. The latter is merely $|\mathrm{Aut}(H)|$, since we are dealing with finite groups. We have arrived to the main result of this chapter:

**Proposition 2.1.2.**

$$\mathcal{N}(H) = \frac{|\{\varphi \in Hom(H, G) | \varphi \textit{ injective}\}|}{|\mathrm{Aut}(H)|}$$

The hard task now is to determine how to calculate $|\{\varphi \in Hom(H, G) | \varphi \text{ injective}\}|$. As already mentioned, a homomorphism is completely determined by how the generators of the domain-group are mapped. There are now two conditions that must be fulfilled. The first condition accounts for the function to even be a homomorphism at all. The second condition assures that the homomorphism is injective.

- The generators of $H$ must be mapped to elements in $G$ satisfying the relations of $H$.
- The generators of $H$ are *independent*, so they must be mapped to elements in $G$ that are similarly independent.

For a precise description of the theory of presentations, see for example *Presentations of Groups* by D.L. Johnson [7]. It is however sufficient for our needs to just have the concept that a set of elements in a group, $\{g_1, g_2, ..., g_k\} \subset G$ are *independent* in the sense the each generator is not in the span of the others. More precisely, we want

$$g_i \notin \langle g_1, g_2, ..., g_{i-1}, g_{i+1}, ..., g_k \rangle \, .$$

The method just discussed could (and perhaps should) be seen as "choosing" generators in the set of $G$ and $H$ satisfying the two conditions mentioned above.

### 2.1.2 Initial results

*Observation.* Observe again that even though we might write "number of ways of choosing generators", I will always count the number of ways of choosing an *ordered* set of generators. This is crucial to understand to avoid confusion.

**Lemma 2.1.3.** *For p-groups, different subgroups of order p have trivial intersection.*

*Proof.* $H, H' < G \Rightarrow H \cap H' < G$. Lagrange's theorem now says that $|H \cap H'| \Big| |G|$, so $|H \cap H'| = 1$ or $|H \cap H'| = p$. But $|H \cap H'| = p \Rightarrow H = H'$, so $|H \cap H'| = 1$. ⨳

**Theorem 2.1.4.** *For all p-groups, it hold that*

$$\mathcal{N}(Z_{p^k}) = \frac{n_k(G)}{n_k(Z_{p^k})} = \frac{n_k}{p^{k-1}(p-1)} \, .$$

*Proof.* The argument is purely combinatorial. Every subgroup isomorphic with $Z_{p^k}$ is generated by an element of order $p^k$, and every such element in $G$ generates a subgroup isomorphic with $Z_{p^k}$. Furthermore, every element $a \in G$ of order $p^k$ can only generate one subgroup isomorphic with $Z_{p^k}$, namely $\langle a \rangle$. Since there are exactly $n_k(Z_{p^k}) = p^{k-1}(p-1)$ elements in $\langle a \rangle$ of order $p^k$, this subgroup can be generated by $p^{k-1}(p-1)$ different generators. The result follows. ⨳

**Corollary 2.1.5.** *For a p-group $G$, if $n_i = 0$ for $i > k$ $\exists k$, then $\mathcal{N}(Z_{p^i}) = 0$ for $i > k$.*

*Proof.* This follows directly from the preceding theorem. ⨳

**Corollary 2.1.6.** *For a p-group $G$, if $n_i = 0$ for $i > k$ for some $k$, then $\mathcal{N}(H) = 0$ for all subgroups $H < G$ such that $H$ is completely factorizable (recall Definition 1.2.8) with at least one factor of $Z_{p^i}$ for $i > k$.*

*Proof.* From the preceding theorem we know that $G$ has no subgroup isomorphic with $Z_{p^i}$. A subgroup $H$ satisfying the assumptions would though have at least one subgroup isomorphic with $Z_{p^i}$. This is obviously a contradiction. ⨳

*Example* 2.1.7. The group $Z_{p^2} \times Z_{p^2}$ has $n_3 = 0$ and thus it cannot have a subgroup isomorphic with $Z_{p^3}$, since that group has elements of order $p^3$.

**Corollary 2.1.8.** *For all p-groups,*

$$\mathcal{N}(Z_p) = \frac{n_1}{p-1}\,.$$

This can easily be deduced from Theorem 2.1.4, but for instructional reasons I give a direct proof for this.

*Proof.* The argument is combinatorial. First determine the number of ways of choosing a generator, then divide by the number of ways the same subgroup can be generated. The number of ways of choosing generator is of course $n_1$. There are $p-1$ generators in every group of order $p$. The result follows. ⨳

**Corollary 2.1.9.** *If $G \cong Z_p^k$, then*

$$\mathcal{N}(Z_p) = \frac{p^k - 1}{p-1} = p^{k-1} + p^{k-2} + ... + p + 1\,.$$

*Proof.* This follows directly from Corollary 2.1.8 and the fact that $n_1 = p^k - 1$ in this particular group, since all elements except the identity have order $p$ in $G$. ⨳

## 2.2 Subgroups of groups of lower order

In this section we will determine the most important properties of the inner structure of groups of order $p^n$, $n \leq 3$. This includes finding the number of different subgroups and the number of elements of different order. We will also take a look at how we can find subgroups isomorphic to these groups in our subsequent study of the groups of order $p^4$. For that we need to determine $|\mathrm{Aut}(G)|$ for the non-abelian groups we also determine the center $Z(G)$.

We saw in the previous chapter that $p = 2$ must be analyzed separately from the case $p > 2$ when we are investigating groups of order $p^3$. Interestingly enough though, there is no difference for different primes greater than 2. We will focus on the more general case, so throughout this chapter, $p > 2$ is assumed.

Many of the results in this section was derived in Chapter 1, but when they are central for the work being, I will not omit them but present them again with a slightly different approach to the method of proof.

### 2.2.1 $\{id\}$, $Z_p$ and $Z_{p^2}$

These groups are in some sense the building blocks of the groups we will later consider. We will present the relevant properties of these groups here.

#### The trivial group $\{id\}$

According to some definitions, the trivial group $\{id\}$ is a $p$-group. Whether we consider it a $p$-group or not is not relevant to our interests. We will however not count it or describe it when we are determining the subgroup structure of different groups.

#### The cyclic group of order $p$

The only group of order $p$ is the cyclic group $Z_p$. $|\mathrm{Aut}(Z_p)| = p - 1$, since there are $p - 1$ generators in $Z_p$.

There are only two groups of order $p^2$: $Z_p \times Z_p$ and the cyclic group $Z_{p^2}$. Both are abelian. In the next section we will examine $Z_p \times Z_p$, but first we'll take a look at $Z_{p^2}$.

#### The cyclic group of order $p^2$

If we use additive notation, it is clear that the elements of order $p$ in $Z_{p^2}$ are the elements on the form $p\alpha$, for some integer $\alpha \neq 0$, so $n_1 = p-1$. There are $p^2$ elements of $Z_{p^2}$, so $n_2 = (p^2) - (p-1) - 1 = p^2 - p$.

$Z_{p^2}$ has only one subgroup of order $p$. $|\mathrm{Aut}(Z_p)| = p^2 - p$, since that is how many generators $Z_{p^2}$ contains.

### 2.2.2 $Z_p \times Z_p$

$Z_p \times Z_p$ is abelian, so a suitable presentation for $G = Z_p \times Z_p$ is $\langle a, b : a^p = b^p = 1, ab = ba \rangle$.

All nontrivial elements are of order $p$, so $n_1 = p^2 - 1$. According to Corollary 2.1.8, $Z_p \times Z_p$ has $p + 1$ subgroups isomorphic with $Z_p$. With the notation that is used in this document:

$$\mathcal{N}(Z_p) = p + 1\,.$$

The following proposition was stated and proved in Section 1.3.2 , which the reader may want reread. I will though give a slightly different proof which might give the reader some insight about the methods used in this chapter.

**Proposition 2.2.1.**

$$|\mathrm{Aut}(Z_p \times Z_p)| = (p^2-1)(p^2-p) = p(p-1)(p^2-1)$$

*Proof.* There are $p^2-1$ nontrivial elements, so there are obviously $p^2-1$ choices for the first generator, which we can denote $a$. The second generator must not lie in the subgroup generated by $a$, $\langle a \rangle$, since that would break the condition of generators being independent; $\langle a, b \rangle$ would then have order $p$ and not $p^2$ as it should. $G$ is however abelian, so every other element is possible to choose as a second generator. That leaves us with $(p^2-1)-(p-1) = p^2-p$ choices for $b$. The result follows. ⧛

**Theorem 2.2.2.** *If $G$ is a $p$-group, then*

$$\mathcal{N}(Z_p \times Z_p) \leq \frac{n_1(n_1-(p-1))}{p(p-1)(p^2-1)} = \frac{\mathcal{N}(Z_p)(\mathcal{N}(Z_p)-1)}{p(p+1)}\,.$$

*Equality holds if and only if all elements in $G$ of order $p$ commute with every other element of order $p$.*

*Proof.* Assume that all elements of order $p$ commute with each other. Let $a, b \in G$ be elements of order $p$. Since all elements of order $p$ commute with each other, $ab = ba$ is automatically fulfilled. The only remaining condition is then that $\langle a \rangle \cap \langle b \rangle = 1$. We have $n_1$ choices for the first generator and then $n_1-(p-1)$ for the second. Dividing with the number of ways of forming the same subgroup from different generators, we arrive at

$$\mathcal{N}(Z_p \times Z_p) = \frac{n_1(n_1-(p-1))}{|\mathrm{Aut}(Z_p \times Z_p)|} = \frac{n_1(n_1-(p-1))}{p(p-1)(p^2-1)}\,.$$

The last equality follows directly from $\mathcal{N}(Z_p) = \frac{n_1}{p-1}$:

$$\frac{n_1(n_1-(p-1))}{p(p+1)(p-1)^2} = \frac{\left(\frac{n_1}{p-1}\right)\left(\frac{n_1-(p-1)}{p-1}\right)}{p(p+1)} = \frac{\mathcal{N}(Z_p)(\mathcal{N}(Z_p)-1)}{p(p+1)}\,.$$

However, if not all elements of order $p$ in $G$ commute, then we get less choices for generators since we also need to impose the condition $ab = ba$. The denominator with $|\mathrm{Aut}(Z_p \times Z_p)|$ does not change though, of course. This goes with the idea that this is the number of ways of choosing generators of $H$ *within* $H$ itself, which is independent of $G$ and its structure. ⧛

### 2.2.3 $Z_{p^3}$

If we use additive notation, the elements of order $p$ in $Z_{p^3}$ are the elements on the form $p^2\alpha$ with $\alpha \neq 0$. There are thus $p-1$ elements of order $p$. Similarly, the elements of order $p^2$ are the elements on the form $p\beta$ that are not of order $p$ or 1. We thus have $p^2-(p-1)-1 = p^2-p$ different values for $\beta$. The elements of order $p^3$ are the elements that are not of lower order, so we have $n_3 = p^3 - (p^2-p) - (p-1) - 1 = p^3 - p^2$. We arrive at

$$\begin{cases} n_3 = p^3 - p^2 \\ n_2 = p^2 - p \\ n_1 = p - 1\,. \end{cases}$$

From Theorem 2.1.4 and Theorem 2.2.2 we get $\mathcal{N}(Z_{p^2}) = \mathcal{N}(Z_p) = 1$ and $\mathcal{N}(Z_p \times Z_p) = 0$.

There are $p^3 - p^2$ choices for a generator of $Z_{p^3}$, and hence $|\mathrm{Aut}(Z_{p^3})| = p^3 - p^2 = p^2(p-1)$.

### 2.2.4 $Z_{p^2} \times Z_p$

Since $Z_{p^2} \times Z_p$ is abelian, this group has the presentation $\langle a, b : a^{p^2} = b^p = 1, ba = ab\rangle$.

Using additive notation with the first component modulo $p^2$ and the second component modulo $p$, we observe that $g = (x, y) \in G$ has order $p$ exactly when $x$ is a multiple of $p$. That means that we have $p$ choices for $x$ and $p$ choices for $y$ if we want $g$ to have order $p$. We can however not have $x = y = 0$ since $g$ would then be the identity element. We conclude that $n_1 = p^2 - 1$ and it then follows that $n_2 = p^3 - p^2$. The elements of order $p$ (or less) have the form $(p\alpha, y)$.

Now we have elements of both order $p^2$ and $p$, so we might get subgroups isomorphic both to $Z_{p^2}$ and $Z_p \times Z_p$. By Corollary 2.1.8 we get

$$\mathcal{N}(Z_p) = \frac{p^2 - 1}{p - 1} = p + 1\,.$$

From Theorem 2.2.2 we obtain

$$\mathcal{N}(Z_p \times Z_p) = 1\,.$$

From Theorem 2.1.4 we get

$$\mathcal{N}(Z_{p^2}) = \frac{p^3 - p^2}{p^2 - p} = p\,.$$

**Proposition 2.2.3.**

$$|\mathrm{Aut}(Z_{p^2} \times Z_p)| = (p^3 - p^2)(p^2 - p) = p^3(p-1)^2$$

*Proof.* All elements in $G$ commute, so the only condition on $a$ and $b$ is that they intersect trivially. For $a$ there are $p^3 - p^2$ choices. For $b$ there are $(p^2-1) - (p-1) = p^2 - p$ options, since there are $p-1$ elements of order $p$ in $\langle a \rangle$. The result follows. ⨳

In summary for $Z_{p^2} \times Z_p$:

$$\begin{cases} n_2 = p^3 - p^2 \\ n_1 = p^2 - 1 \\ \mathcal{N}(Z_p) = p + 1 \\ \mathcal{N}(Z_{p^2}) = p \\ \mathcal{N}(Z_p \times Z_p) = 1 \\ |\mathrm{Aut}(Z_{p^2} \times Z_p)| = p^3(p-1)^2 \,. \end{cases}$$

**Theorem 2.2.4.** *For all p-groups it hold that*

$$\mathcal{N}(Z_{p^2} \times Z_p) \leq \frac{n_2(n_1 - (p-1)}{p^3(p-1)^2} = \frac{\mathcal{N}(Z_{p^2})(\mathcal{N}(Z_p) - 1)}{p^2} \,.$$

*Equality holds if and only if all elements of order $p^2$ commute with all elements of order $p$.*

*Proof.* Assume that all elements of order $p^2$ commute with all elements of order $p$. Let $a$ have order $p^2$ and $b$ order $p$. By assumption, $ab = ba$, so the only condition on $a$ and $b$ (except their orders) is that their intersection is trivial. We can choose $a$ arbitrarily, which gives us $n_2$ options. Now we need that $b \notin \langle a \rangle$. There are $p-1$ elements of order $p$ in $\langle a \rangle$, so we are left with $n_1 - (p-1)$ choices. The result follows from Proposition 2.1.2, since $|\mathrm{Aut}(Z_{p^2} \times Z_p)| = p^3(p-1)^2$.
The last equality follows directly from using Theorem 2.1.4 and Corollary 2.1.8

This is obviously an upper bound for $\mathcal{N}(Z_{p^2} \times Z_p)$; in the case that not all elements in $G$ of order $p^2$ commutes with all elements of order $p$ we get less choices of $b$ for a given $a$ (or vice versa), while the denominator stays the same. ⨳

### 2.2.5 $Z_p \times Z_p \times Z_p$

A presentation of this group is $\langle a, b, c : a^p = b^p = c^p = 1, ba = ab, ca = ac, cb = bc \rangle$.

Every nontrivial element is of order $p$, so

$$\begin{cases} n_3 = n_2 = 0 \\ n_1 = p^3 - 1 \,. \end{cases}$$

According to Corollary 2.1.8,

$$\mathcal{N}(Z_p) = \frac{p^3-1}{p-1} = p^2+p+1\,.$$

Since $n_2 = 0$, $N(Z_{p^2}) = 0$. Theorem 2.2.2 gives that

$$\mathcal{N}(Z_p^2) = \frac{(p^2+p+1)(p^2+p)}{(p+1)p} = p^2+p+1\,.$$

The next proposition was proved in the previous chapter, but we will here see a slightly different method that illustrates the methods used in this chapter.

**Proposition 2.2.5.**

$$|\mathrm{Aut}(Z_p \times Z_p \times Z_p)| = p^3(p-1)(p^2-1)(p^3-1)$$

*Proof.* $G$ is commutative, so the only conditions are that $b \notin \langle a\rangle$ and $c \notin \langle a,b\rangle$. We have $p^3-1$ choices for $a$ and $(p^3-1)-(p-1) = p^3-p$ choices for $b$. $c$ may not lie in $\langle a,b\rangle$, which is a group of order $p^2$. There are thus $(p^3-1)-(p^2-1) = p^3-p^2$ options for $c$. In total: $|\mathrm{Aut}(Z_p\times Z_p\times Z_p)| = (p^3-1)(p^3-p)(p^3-p^2) = p^3(p-1)(p^2-1)(p^3-1)$. ⨳

In conclusion, for $Z_p \times Z_p \times Z_p$ it holds that:

$$\begin{cases} n_1 = p^3-1 \\ N(Z_p) = p^2+p+1 \\ N(Z_p\times Z_p) = p^2+p+1 \\ |\mathrm{Aut}(Z_p \times Z_p \times Z_p)| = p^3(p-1)(p^2-1)(p^3-1)\,. \end{cases}$$

For information on $\mathcal{N}(Z_p \times Z_p \times Z_p)$ in a general $p$-group, see Theorem 2.2.18.

### 2.2.6 $(Z_p \times Z_p) \rtimes Z_p$

From the previous chapter we know that the operation is

$$((x,y),z)((x',y'),z') = ((x+x', y+y'+zx'), z+z')$$

with every component modulo $p$. One presentation is

$$\langle a,b,c : a^p = b^p = c^p = 1, ba = ab, ca = abc, cb = bc\rangle\,.$$

**Lemma 2.2.6.** *For $g = ((x,y),z) \in (Z_p \times Z_p) \rtimes Z_p$ with the operation above, it holds that*

$$g^n = ((nx, ny + \frac{n(n-1)xz}{2}), nz)\,.$$

*Proof.* Proof by induction. $g^1 = ((x, y), z)$, so it holds for $n = 1$. Assume the formula holds for $n$.

$$\begin{aligned} g^{n+1} &= g^n g \\ &= ((nx, ny + \frac{n(n-1)xz}{2}), nz)((x, y), z) \\ &= ((nx + n, ny + \frac{n(n-1)xz}{2} + y + (nz)x), nz + z) \\ &= (((n+1)x, (n+1) + \frac{(n^2-n)xz}{2} + \frac{2nxz}{2}), (n+1)z) \\ &= (((n+1)x, (n+1)y + \frac{(n+1)nxz}{2}), (n+1)z) \end{aligned}$$

The result follows by induction. ⨳

**Proposition 2.2.7.** *For $(Z_p \times Z_p) \rtimes Z_p$ it holds that*

$$\begin{cases} n_2 = 0 \\ n_1 = p^3 - 1 \end{cases}$$

*Proof.* Notice that

$$g^p = ((px, py + \frac{p(p-1)xz}{2}), pz) = ((0, 0), 0)\,.$$

This means that all nontrivial elements have order $p$. ⨳

From Theorem 2.1.4:

$$\begin{cases} \mathcal{N}(Z_{p^2}) = 0 \\ \mathcal{N}(Z_p) = p^2 + p + 1\,. \end{cases}$$

*Observation.* In order to determine $\mathcal{N}(Z_p \times Z_p)$ we cannot use Theorem 2.2.2, since not all elements of order $p$ commute. If we choose two elements arbitrarily, we could actually accidently generate the whole group. An example of this is $H = \langle((1, 0), 0), ((0, 0), 1)\rangle$. H will obviously consist of elements $((x, 0), z) = a^x c^z$, but we will also have $ca = ((1, 1), 1) \in H$, so $H$ has at least order $p^2+1$ and thus $p^3$, implying that $H = G$.

**Lemma 2.2.8.** *$g, g' \in G = (Z_p \times Z_p) \rtimes Z_p$ (with the operation defined above) commute if and only if $xz' \equiv x'z \pmod p$.*

*Proof.* From the operation:

$$gg' = ((x + x', y + y' + zx'), z + z')$$

and

$$g'g = ((x + x', y + y' + z'x), z + z')$$

We see that equality in the second component holds if and only if $xz' \equiv x'z \pmod{p}$. ⨳

**Proposition 2.2.9.** *The center of $(Z_p \times Z_p) \rtimes Z_p$ with the operation defined above is*

$$Z(G) = \langle((0,1),0)\rangle \cong Z_p\,.$$

*Proof.* Assume $g \in Z(G)$. Then we must have $xz' \equiv x'z \pmod{p}$ for arbitrarily chosen $x', z'$. This can clearly only be achieved if $x = z = 0$. $y$ is however arbitrary. ⨳

**Lemma 2.2.10.** *Let $g, h \in G = (Z_p \times Z_p) \rtimes Z_p$ and $\langle g\rangle \neq \langle h\rangle$. If $gh = hg$, then $Z(G) < \langle g, h\rangle$.*

*Proof.* (Credit to Mats Boij for the line of the proof.)

Take an element $a \in \langle g, h\rangle$. If $a \in Z(G)$, then we are finished. Assume instead that $a \notin Z(G)$. The centralizer of $a$, $C_G(a) = \{g \in G | ga = ag\}$, cannot have order $p^3$ since we assumed that $a \notin Z(G)$. It cannot have order $p$ either, since it commutes with at least one other element than its powers, namely $h$ from the assumptions. $C_G(a)$ must then have order $p^2$ and be isomorphic with $Z_p \times Z_p$. Since also $h \in C_G(a)$, we can conclude that $C_G(a) = \langle g, h\rangle$ (Which is itself an interesting result!). We also know that $Z(G) < C_G(a) \quad \forall a \in G$, which proves the lemma. ⨳

**Proposition 2.2.11.** *In $(Z_p \times Z_p) \rtimes Z_p$ it holds that*

$$N(Z_p \times Z_p) = p + 1\,.$$

*Proof.* Since we cannot use Theorem 2.2.2, we must find another approach. Again, all subgroups isomorphic with $Z_p \times Z_p$ can be generated by two elements of order $p$. Call them $g, h$, $\langle g\rangle \neq \langle h\rangle$. $Z_p \times Z_p$ is abelian, so $gh = hg$ by necessity. If $gh = hg$, then $|\langle g, h\rangle| = p^2$ by previous argument, so it will indeed generate a subgroup of the right order. Furthermore, all elements in $G$ have order $p$, so it must indeed be isomorphic with $Z_p \times Z_p$.

Lemma 2.2.10 implies that $Z(G) < \langle g, h\rangle$. We can then ignore the choices of generators $g$ and $h$ where neither $\langle g\rangle = Z(G)$ or $\langle h\rangle = Z(G)$ since every sought subgroup can be expressed as $H = \langle f, g\rangle$, with $f \in Z(G)$. The number of ways of forming different combinations of $\langle f, g\rangle$ will now be the $\mathcal{N}(Z_p) - 1$ choices for $\langle g\rangle$. These will coincide exactly $\mathcal{N}(Z_p, Z_p^2) - 1 = (p + 1) - 1 = p$ times. We have covered all possibilities, so

$$\mathcal{N}(Z_p^2) = \frac{(p^2 + p + 1) - 1}{(p + 1) - 1} = p + 1\,.$$

⨳

For the sake of completeness, here is again the order of the automorphism group of $(Z_p \times Z_p) \rtimes Z_p$:

$$|\mathrm{Aut}((Z_p \times Z_p) \rtimes Z_p)| = p^3(p-1)(p^2-1)\,.$$

The proof can be found in Section 1.5.3.

In summary for $(Z_p \times Z_p) \rtimes Z_p$:

$$\begin{cases} n_1 = p^3 - 1 \\ N(Z_p) = p^2 + p + 1 \\ N(Z_p^2) = p + 1\,. \end{cases}$$

### 2.2.7 $Z_{p^2} \rtimes Z_p$

This group has the presentation

$$\langle a, b : a^{p^2} = b^p = 1, ba = a^p b\rangle$$

and the operation

$$(x, y)(x', y') = (x + x' + pyx', y + y')$$

with the first component modulo $p^2$ and the second component modulo $p$.

**Lemma 2.2.12.** *For $g = (x, y) \in Z_{p^2} \rtimes Z_p$ with the operation above, it holds that*

$$g^n = (nx + \frac{pn(n-1)xy}{2}, ny), .$$

*Proof.* Proof by induction. It holds for $g^1 = (x, y)$. Assume that it holds for $g^n$.

$$\begin{aligned} g^{n+1} &= g^n g \\ &= (nx + \frac{pn(n-1)xy}{2}, ny)(x, y) \\ &= (nx + \frac{pn(n-1)xy}{2} + x + p(ny)x, ny + y) \\ &= ((n+1)x + \frac{p(n^2-n)xy}{2} + \frac{2pnxy}{2}, (n+1)y) \\ &= ((n+1)x + \frac{p(n+1)nxy}{2}, (n+1)y) \end{aligned}$$

The result follows by induction. ⧛

**Proposition 2.2.13.** *For $Z_{p^2} \rtimes Z_p$ it holds that*

$$\begin{cases} n_2 = p^3 - p^2 \\ n_1 = p^2 - 1\,. \end{cases}$$

*Proof.* Using the previous result, we get

$$g^p = (px + \frac{pp(p-1)xy}{2}, py) = (px, 0)\,.$$

Evidently, we have elements of order $p^2$ exactly when $x$ is not a multiple of $p$, and thus $p^2 - p$ choices for $x$. We can however choose $y$ arbitrarily, so we arrive at $n_2 = (p^2 - p)p = p^3 - p^2$.

Since also

$$g^{p^2} = (p^2x + \frac{pp^2(p^2-1)xy}{2}, p^2y) = (0, 0)\,,$$

There are no elements of order $p^3$, so $n_2 = p^3 - p^2$. ⨳

**Proposition 2.2.14.** *The elements in $G = Z_{p^2} \rtimes Z_p$ of order $p$ forms an abelian subgroup.*

*Proof.* The elements in $G$ of order $p$ are the elements on the form $(p\alpha, y)$. We have that

$$(p\alpha, y)(p\alpha', y') = (p\alpha + p\alpha' + pyp\alpha', y + y') = (p\alpha + p\alpha', y + y')\,.$$

The product is then of order $p$, implying that the elements of order $p$ form a subgroup. We also see that all these elements commute, so it is abelian. ⨳

**Proposition 2.2.15.** *The center of $G = Z_{p^2} \rtimes Z_p$ with the operation defined above is*

$$Z(G) = \langle (p, 0) \rangle \cong Z_p\,.$$

*Proof.* Let $(x, y) \in Z(G)$ and let $(x', y') \in G$ be arbitrary. We get the product

$$(x, y)(x', y') = (x + x' + pyx', y + y')\,.$$

We see that they commute if and only if $yx' \equiv y'x \pmod{p}$. If $x'$ and $y'$ are arbitrary, we must then obviously have $x \equiv 0 \pmod{p}$, or equivalently $x = p\alpha$ and $y = 0$. ⨳

For $Z_{p^2} \rtimes Z_p$, by using Corollary 2.1.8,Theorem 2.2.2 and Theorem 2.1.4 we get:

$$\begin{cases} n_2 = p^3 - p^2 \\ n_1 = p^2 - 1 \\ \mathcal{N}(Z_p) = p + 1 \\ \mathcal{N}(Z_p^2) = 1 \\ \mathcal{N}(Z_{p^2}) = p\,. \end{cases}$$

For the sake of completeness:

$$|\mathrm{Aut}(Z_{p^2} \rtimes Z_p)| = p^3(p-1)$$

The proof is given in Section 1.5.1.

In summary for $Z_{p^2} \rtimes Z_p$:

$$\begin{cases} n_2 = p^3 - p^2 \\ n_1 = p^2 - 1 \\ \mathcal{N}(Z_p) = p + 1 \\ \mathcal{N}(Z_{p^2}) = p \\ \mathcal{N}(Z_p \times Z_p) = 1 \\ |\mathrm{Aut}(Z_{p^2} \rtimes Z_p)| = p^3(p-1)\,. \end{cases}$$

*Result* 2.2.16. When determining $\mathcal{N}(Z_{p^2} \rtimes Z_p)$ in an arbitrary $p$-group, the condition of independent generators is redundant.

*Proof.* $ba = a^{1+p}b$ implies that $ba \neq ab$, but $\langle a \rangle$ is cyclic and therefore all elements in it commute. The conclusion is that $b \notin \langle a \rangle$, since we would otherwise reach a contradiction. ⨳

### 2.2.8 General Theorems

When we soon turn our attention towards the groups of order $p^4$, we will see that they can have subgroups of order $p^3$. It is therefore time to state some more general results that will help us to describe these groups.

**Lemma 2.2.17.**

$$|\mathrm{Aut}(Z_p^k)| = \prod_{i=0}^{k-1} \left(p^k - p^i\right)$$

This is stated in Chapter 1, but I will present a combinatorial proof.

*Proof.* All generators have the same order, and we are working with an abelian group, so the only condition is that of independence of generators.

For the first generator, $g_1$, there are $p^k - 1$ choices, since $n_1(Z_p^k) = p^k - 1$. The second generator, $g_2$, must not lie in $\langle g_1 \rangle$, so there are $(p^k - 1) - (p - 1) = p^k - p$ choices for $g_2$. For the third generator, $g_3$, to not lie in the span of $g_1$ and $g_2$, we must exclude $p^2 - 1$ choices, because $\langle g_1, g_2 \rangle$ is a group isomorphic with $Z_p \times Z_p$ and then has order $p^2$.

We observe that for the $(i+1)$:th generator, we need to exclude $p^i - 1$ options, namely the options in $\langle g_1, g_2, ..., g_i \rangle$. The result follows. ⨳

**Theorem 2.2.18.** *For p-groups, it hold that*

$$\mathcal{N}(Z_p^k) \leq \frac{\prod_{i=0}^{k-1} (n_1 - (p^i - 1))}{\prod_{i=0}^{k-1} (p^k - p^i)}\,.$$

*Equality holds if and only if all elements of $G$ of order $p$ commute with every other element of order $p$.*

*Proof.* Assume that all elements in $G$ of order $p$ commute. Then, by choosing elements of order $p$ we need only worry about the condition of independence. We have $n_1$ choices for the first generator $g_1$. For the second choice we must exclude all elements of order $p$ in $\langle g_1 \rangle$, of which there are $p-1$. That accounts to $n_1-(p-1)$ choices. For the third generator, $g_3$, the condition is that $g_3 \notin \langle g_1, g_2 \rangle$, so there are $n_1-(p^2-1)$ options.

For the $(i+1)$:th generator the condition is that $g_{i+1} \notin \langle g_1, g_2, ..., g_i \rangle$. Hence there are $n_1-(p^i-1)$ choices for $g_{i+1}$.

The equality then follows from Proposition 2.1.2 and Lemma 2.2.17.

Assume now instead that not all elements of order $p$ commute. That gives us further restrictions on the possible choices of generators. The denominator is however independent of $G$. ⧖

**Corollary 2.2.19.** *For abelian $p$-groups, it hold that*

$$\mathcal{N}(Z_p^k) = \frac{\prod_{i=0}^{k-1}(n_1-(p^i-1))}{\prod_{i=0}^{k-1}(p^k-p^i)}.$$

**Corollary 2.2.20.** *If $G$ is a $p$-group in which all elements of order $p$ commute and $n_1 = p^k-1$, then it holds that $\mathcal{N}(Z_p^k) = 1$. and $\mathcal{N}(Z_p^l) = 0$ for $l > k$.*

*Proof.* This follows trivially from Theorem 2.2.18. Using the theorem and remembering that $n_1 = p^k-1$, we get

$$\mathcal{N}(Z_p^k) = \frac{\prod_{i=0}^{k-1}(n_1-(p^i-1))}{\prod_{i=0}^{k-1}(p^k-p^i))} = \frac{\prod_{i=0}^{k-1}\left((p^k-1)-(p^i-1)\right)}{\prod_{i=0}^{k-1}(p^k-p^i))} = 1$$

Similarly, if $l > k$:

$$\mathcal{N}(Z_p^l) = \frac{\prod_{i=0}^{l-1}(n_1-(p^i-1))}{\prod_{i=0}^{l-1}(p^l-p^i))} = \frac{\prod_{i=0}^{l-1}\left(p^k-p^i\right)}{\prod_{i=0}^{l-1}(p^l-p^i))}$$

The numerator will here be zero since the factor corresponding to $i = k \leq l-1$ is zero. The denominator never gets a factor equal to zero since the product stops at $i = l-1$. ⧖

**Theorem 2.2.21.** *If $G$ is a completely factorizable $p$-group (see Definition 1.2.8) of order $p^4$ with $n_1 = p^k-1$, then $G$ contains no subgroups consisting of more than $k$ factors of semidirect products.*

*Proof.* We have seen that for every group $H$ of order $p^3$ or less it holds that $H$ consists of semidirect products with $l$ factors if and only if $n_1(H) = p^l - 1$. Then clearly if $l > k$, we have more elements of order $p$ in the subgroup $H$ than in the group $G$. But that is impossible! ↯

*Example* 2.2.22. $Z_{p^2} \times Z_{p^2}$ is a completely factorizable group with two factors. It has $p^2 - 1$ elements of order $p$. It contains no subgroup isomorphic with $Z_p \times Z_p \times Z_p$, since that subgroup would then have $p^3 - 1$ elements of order $p$.

## 2.3 Subgroups of groups of order $p^4$

The purpose of this section is to list the number of different subgroups as well as the number of elements of different order for the groups of order $p^4$. We will also find the center of each group and often gain some knowledge of what the inner structures of the groups are like.

The procedure will in many aspects be straight-forward and rely heavily on the results of Chapter 1 and the results about the smaller $p$-groups just presented.

Also in this section will we assume that $p > 2$, but as we noticed in the preceding chapter, a few of the groups collapse nontrivially when $p = 3$. I will therefore in those cases even assume that $p > 3$, which when I do will be stated explicitly.

### 2.3.1 The abelian groups of order $p^4$

The procedure is more or less mechanical and the results hold for all primes, even $p = 2$. For $\mathcal{N}(Z_{p^i})$, use Theorem 2.1.4. For $\mathcal{N}(Z_p^i)$, use Theorem 2.2.18. For $\mathcal{N}(Z_{p^2} \times Z_p)$, use Theorem 2.2.4. We can of course not have non-abelian subgroups in an abelian group, so $\mathcal{N}(Z_{p^2} \rtimes Z_p) = \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 0$.

| | $Z_{p^4}$ | $Z_{p^3} \times Z_p$ | $Z_{p^2} \times Z_{p^2}$ | $Z_{p^2} \times Z_p \times Z_p$ | $Z_p \times Z_p \times Z_p \times Z_p$ |
|---|---|---|---|---|---|
| $n_4$ | $p^4 - p^3$ | 0 | 0 | 0 | 0 |
| $n_3$ | $p^3 - p^2$ | $p^4 - p^3$ | 0 | 0 | 0 |
| $n_2$ | $p^2 - p$ | $p^3 - p^2$ | $p^4 - p^2$ | $p^4 - p^3$ | 0 |
| $n_1$ | $p - 1$ | $p^2 - 1$ | $p^2 - 1$ | $p^3 - 1$ | $p^4 - 1$ |
| $\mathcal{N}(Z_p)$ | 1 | $p + 1$ | $p + 1$ | $p^2 + p + 1$ | $p^3 + p^2 + p + 1$ |
| $\mathcal{N}(Z_{p^2})$ | 1 | $p$ | $p^2 + p$ | $p^2$ | 0 |
| $\mathcal{N}(Z_p \times Z_p)$ | 0 | 1 | 1 | $p^2 + p + 1$ | $p^4 + p^3 + 2p^2 + p + 1$ |
| $\mathcal{N}(Z_{p^3})$ | 1 | $p$ | 0 | 1 | 0 |
| $\mathcal{N}(Z_{p^2} \times Z_p)$ | 0 | 1 | 1 | $p^2 + p + 1$ | 0 |
| $\mathcal{N}(Z_p \times Z_p \times Z_p)$ | 0 | 0 | 0 | 1 | $p^3 + p^2 + p + 1$ |

### 2.3.2 The general method

As we will see later in this section, the descriptions for the different nonabelian subgroups of order $p^4$ will be presented in a very similar manner (and order). The procedure for *each* group is roughly as such:

- We will first give one possible presentation and one possible operation for the group under discussion. These are provided from the previous chapter. Note that there are many possible defining operations and presentations for every single group, I just choose convenient ones for ease of calculation and illustration. For the sake of brevity, I will not note this in every single case below.
- Starting from the operation we can easily determine $g^n$ and then the number of elements of the different orders by simply computing $g^p$, $g^{p^2}$ et cetera.
- From Theorem 2.1.4 we directly get $\mathcal{N}(Z_{p^k})$ and most importantly $\mathcal{N}(Z)$.
- Theorem 2.2.21 and Corollary 2.1.6 can tell us that some groups definitely not are subgroups of the group under discussion.
- If the product of elements of order $p$ also is of order $p$, then we know that they form a subgroup. That is very valuable information.
- By computing the condition for commuting elements we can find $Z(G)$ and sometimes also other useful information.
- The number of different abelian subgroups follows from Theorem 2.2.18, Theorem 2.1.4 and Theorem 2.2.4. If not all elements of order $p$ commute, it is often necessary to use the condition for commuting elements.
- Lastly, if there are any remaining subgroups to treat with, they are dealt with.

### 2.3.3 (vi) $Z_{p^3} \rtimes Z_p$

As noted in the previous chapter, this group is isomorphic with

$$\langle a, b : a^{p^3} = b^p = 1, ba = a^{1+p^2}b \rangle$$

with operation

$$(x, y)(x', y') = (x + x' + p^2yx', y + y') .$$

The first component is modulo $p^3$ and the second modulo $p$.

**Lemma 2.3.1.** *For $g = (x, y) \in Z_{p^3} \rtimes Z_p$ with the operation above, it holds that*

$$g^n = (nx + \frac{p^2n(n-1)xy}{2}, ny) .$$

*Proof.* Proof by induction. It holds for $g^1 = (x, y)$. Assume that it holds for $g^n$.

$$\begin{aligned} g^{n+1} &= g^n g \\ &= (nx + \frac{p^2 n(n-1)xy}{2}, ny)(x, y) \\ &= (nx + \frac{p^2 n(n-1)xy}{2} + x + p^2(ny)x, ny + y) \\ &= ((n+1)x + \frac{p^2(n^2-n)xy}{2} + \frac{2p^2 nxy}{2}, (n+1)y) \\ &= ((n+1)x + \frac{p^2(n+1)nxy}{2}, (n+1)y) \end{aligned}$$

The result follows by induction. ⧖

**Proposition 2.3.2.** *For $Z_{p^3} \rtimes Z_p$ it holds that*

$$\begin{cases} n_3 = p^4 - p^3 \\ n_2 = p^3 - p^2 \\ n_1 = p^2 - 1\,. \end{cases}$$

*Proof.* A few quick calculations give that

$$(x, y)^{p^3} = (p^3 x + \frac{p^2 p^3(p^3-1)xy}{2}, p^3 y) = (0, 0) = id\,,$$

$$(x, y)^{p^2} = (p^2 x + \frac{p^2 p^2(p^2-1)xy}{2}, p^2 y) = (p^2 x, 0)\,,$$

and finally

$$(x, y)^p = (px + \frac{p^2 p(p-1)xy}{2}, py) = (px, 0)\,.$$

The first equation shows that there are no elements of order $p^4$. From the last equation we see that the elements of order $p$ or less are the elements where $x$ is a multiple of $p^2$, $y$ arbitrary. That gives us $p^2$ elements, but including the identity. $n_1 = p^2 - 1$.

$g$ has order $p^2$ or less if $x$ is a multiple of $p$, $y$ arbitrary. There are $p^3$ such elements. Subtracting the $p^2$ elements of lower order yields $n_2 = p^3 - p^2$. It follows that $n_3 = p^4 - p^3$. ⧖

From Theorem 2.1.4 and its corollaries we receive:

$$\begin{cases} \mathcal{N}(Z_p) = p + 1 \\ \mathcal{N}(Z_{p^2}) = p \\ \mathcal{N}(Z_{p^3}) = p\,. \end{cases}$$

**Proposition 2.3.3.** *For $Z_{p^3} \rtimes Z_p$ it holds that*

$$\begin{cases} \mathcal{N}(Z_p \times Z_p) = 1 \\ \mathcal{N}(Z_p^2 \times Z_p) = 1\,. \end{cases}$$

*Proof.* Consider the product of two elements of order $p$:

$$(p^2\alpha, y)(p^2\alpha', y') = (p^2\alpha + p^2\alpha' + p^2 y p^2\alpha', y + y') = (p^2\alpha + p^2\alpha', y + y')\,.$$

They obviously commute with each other.

Consider now the product of an element of order $p^2$ and an element of order $p$:

$$(p^2\alpha, y)(p\alpha', y') = (p^2\alpha + p\alpha' + p^2 y p\alpha', y + y') = (p^2\alpha + p\alpha')\,,$$

$$(p\alpha', y')(p^2\alpha, y) = (p^2\alpha + p\alpha' + p^2 y' p^2\alpha, y + y') = (p^2\alpha + p\alpha')\,.$$

We see that they commute. The result follows from Theorem 2.2.18 and Theorem 2.2.4. ⨳

**Proposition 2.3.4.** *The center of $G = Z_{p^3} \rtimes Z_p$ is*

$$Z(G) = \langle (p, 0) \rangle \cong Z_{p^2}\,.$$

*Proof.* From the operation we see that

$$gg' = g'g \Leftrightarrow yx' \equiv y'x \pmod{p}\,.$$

If we let $g'$ be arbitrary, we see that $gg' = g'g$ only if $g = (p\alpha, 0)$. ⨳

Directly from Theorem 2.2.21:

$$\mathcal{N}(Z_p \times Z_p \times Z_p) = \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 0\,.$$

**Proposition 2.3.5.** *For $Z_{p^3} \rtimes Z_p$ it holds that*

$$\mathcal{N}(Z_{p^2} \rtimes Z_p) = 0\,.$$

*Proof.* All elements of order $p^2$ commute with all elements of order $p$, and this is then true for every subset of $G$. $Z_{p^2} \rtimes Z_p$ however contains elements with these properties, so we can have no such subgroup in $G$. ⨳

In summary for $Z_{p^3} \rtimes Z_p$:

$$\begin{cases} n_3 = p^4 - p^3 \\ n_2 = p^3 - p^2 \\ n_1 = p^2 - 1 \\ \mathcal{N}(Z_p) = p + 1 \\ \mathcal{N}(Z_{p^2}) = p \\ \mathcal{N}(Z_p \times Z_p) = 1 \\ \mathcal{N}(Z_{p^3}) = p \\ \mathcal{N}(Z_{p^2} \times Z_p) = 1 \\ \mathcal{N}(Z_p \times Z_p \times Z_p) = 0 \\ \mathcal{N}(Z_{p^2} \rtimes Z_p) = 0 \\ \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 0\,. \end{cases}$$

### 2.3.4 (vii) $(Z_{p^2} \times Z_p) \rtimes Z_p$

From the previous chapter we know that this group is isomorphic with

$$\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = ab, ca = ac, cb = a^p bc \rangle\,.$$

We have the operation

$$((x, y), z)((x', y'), z') = ((x + x' + pzy', y + y'), z + z')$$

with the first component modulo $p^2$ and the second and third component modulo $p$.

**Lemma 2.3.6.** *For $g = ((x, y), z) \in (Z_{p^2} \times Z_p) \rtimes Z_p$ with the operation above, it holds that*

$$g^n = ((nx + \frac{pn(n-1)yz}{2}, ny), nz)\,.$$

*Proof.* Proof by induction. It holds for $g^1 = (x, y)$. Assume that it holds for $g^n$.

$$\begin{aligned} g^{n+1} &= g^n g \\ &= ((nx + \frac{pn(n-1)yz}{2}, ny), nz)((x, y), z) \\ &= ((nx + \frac{pn(n-1)yz}{2} + x + p(nz)y, ny + y), nz + z) \\ &= (((n+1)x + \frac{p(n^2-n)yz}{2} + \frac{2pnyz}{2}, (n+1)y), (n+1)z) \\ &= (((n+1)x + \frac{p(n+1)nyz}{2}, (n+1)y), (n+1)z) \end{aligned}$$

The result follows by induction. ∎

**Proposition 2.3.7.** *For $(Z_{p^2} \times Z_p) \rtimes Z_p$ it holds that*

$$\begin{cases} n_2 = p^4 - p^3 \\ n_1 = p^3 - 1\,. \end{cases}$$

*Proof.* Since

$$g^p = ((x,y),z)^p = ((px + \frac{pp(p-1)yz}{2}, py), pz) = ((px,0),0)\,,$$

we see that $g$ is of order $p$ or less only if $x$ is a multiple of $x$. We can allow $y$ and $z$ to be arbitrary, so $n_1 = p^3 - 1$. (Remember that $x$ is modulo $p^2$ and $y, z$ modulo $p$.)

Similarly,

$$g^{p^2} = ((x,y),z)^{p^2} = ((p^2x + \frac{pp^2(p^2-1)yz}{2}, p^2y), p^2z) = ((0,0),0)$$

shows that there are no elements of higher order than $p^2$, so $n_2 = p^4 - p^3$. ⧖

From Theorem 2.1.4 and its corollaries we receive:

$$\begin{cases} \mathcal{N}(Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_{p^2}) = p^2 \\ \mathcal{N}(Z_{p^3}) = 0\,. \end{cases}$$

**Proposition 2.3.8.** *The center of $G = (Z_{p^2} \times Z_p) \rtimes Z_p$ with the operation defined above is*

$$Z(G) = \langle((1,0),0)\rangle \cong Z_{p^2}\,.$$

*Proof.* From the operation we get that

$$gg' = g'g \Leftrightarrow zy' \equiv z'y \pmod{p}\,.$$

Thus if we let $g'$ be arbitrary, we must have $y = z = 0$. ⧖

**Proposition 2.3.9.** *Let $G$ be the group $(Z_{p^2} \times Z_p) \rtimes Z_p$. The product of elements of $G$ of order $p$ has order $p$. The product of an element of order $p^2$ and an element of order $p$ has order $p^2$.*

*Proof.* It follows directly from

$$((p\alpha,y),z)((p\alpha',y'),z') = ((p\alpha + p\alpha' + pzy', y + y'), z + z')$$

and

$$((p\alpha,y),z)((x',y'),z') = ((p\alpha + x' + pzy', y + y'), z + z')\,.$$

⧖

Notice that this means that the element of order $p$ form a subgroup of order $p^3$, since it is closed under multiplication. All elements of order $p$ does not commute however, so

$$\begin{cases} \mathcal{N}(Z_p \times Z_p \times Z_p) = 0 \\ \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 1\,. \end{cases}$$

The last assertion is confirmed by choosing $a = ((0,1),0), b = ((p,0),0), c = ((0,0),1)$ for generators of $(Z_p \times Z_p) \rtimes Z_p$ .

If we consider just the subgroup with elements of order $p$, $(Z_p \times Z_p) \rtimes Z_p$, then it is obvious that every smaller subgroup in $G$ with elements of just order $p$ will be a subgroup of this subgroup isomorphic with $(Z_p \times Z_p) \rtimes Z_p$. We can draw the conclusion that

$$\mathcal{N}(Z_p \times Z_p) = \mathcal{N}(Z_p \times Z_p, (Z_p \times Z_p) \rtimes Z_p) = p + 1\,.$$

**Proposition 2.3.10.** *For $(Z_{p^2} \times Z_p) \rtimes Z_p$ it holds that*

$$\mathcal{N}(Z_{p^2} \times Z_p) = p + 1\,.$$

*Proof.* Assume $a = ((x,y),z)$ has order $p^2$. Then $a^p = ((px,0),0)$, so the only subgroup of $\langle a \rangle$ isomorphic with $Z_p$ is $\langle((p,0),0)\rangle$. This fact is very convenient, since we then now that for every choice of $a$, $b$ is not allowed to be in the center because they would then coincide. (Notice that $\langle((p,0),0)\rangle < Z(G)$.) We can then first choose $b$ with the only condition that $b \notin Z(G)$ and then choose $a$ with the only condition that $ab = ba$. We then solve the problem of coinciding generators.

We have $p^3 - p$ choices for $b$, since it must not be in the center.

For $a$, we see that we can choose $x$ arbitrary, we just need that $x \not\equiv 0 \pmod p$ for the order of $a$. We thus have $p^2 - p$ choices for $x$ alone. To repeat myself, the only condition now is that $ab = ba \Leftrightarrow zy' \equiv z'y \pmod p$. We now have three different cases to examine.

$y' = 0, z' \neq 0 \Rightarrow y = 0$ and $z$ can be chosen arbitrarily.

$z' = 0, y' \neq 0 \Rightarrow z = 0$ and $y$ can be chosen arbitrarily.

$y', z' \neq 0$. Choose $y$ and $z$ is determined by $zy' \equiv z'y \pmod p$ or vice versa.

We see that in either case, we have $p$ choices for $y$ and $z$ combined. Bringing all this together and revoking Theorem 2.2.4:

$$\mathcal{N}(Z_{p^2} \times Z_p) = \frac{(p^3 - p)(p^2 - p)p}{p^3(p-1)^2} = \frac{p^3(p-1)(p^2-1)}{p^3(p-1)^2} = p + 1\,.$$

⨳

**Proposition 2.3.11.** *For $(Z_{p^2} \times Z_p) \rtimes Z_p$ it holds that*

$$\mathcal{N}(Z_{p^2} \rtimes Z_p) = p^2 - 1\,.$$

*Proof.* Let $a = ((x, y), z), b = ((p\alpha', y'), z')$.

$$\begin{cases} ba = ((x + p\alpha' + pz'y, y + y'), z + z') \\ a^{1+p}b = ((x + px + 0, y + 0), z + 0)((p\alpha', y'), z') = ((x + px + p\alpha' + pz'y, y + y'), z + z') \end{cases}$$

The condition from the relation is then that

$$z'y \equiv x + zy' \pmod{p}.$$

We see directly that $b$ cannot lie in the center, because that would imply $x \equiv 0 \pmod{p}$, contradicting the order of $a$. That solves the problem of coinciding generators automatically. We also see that also $a$ cannot be in the center, for the same reason.

First choose $a$. We cannot have $y = z = 0$, and we must have $x \not\equiv 0 \pmod{p}$. In total $(p^2 - p)(p^2 - 1)$ possibilities for $a$. (This can also be realized by taking the elements of the center from the total: $(p^4 - p^3) - (p^2 - p) = p^4 - p^3 - p^2 + p = (p^2 - p)(p^2 - 1)$.)

When choosing $b$, we quickly realize that $\alpha'$ is arbitrary ($p$ choices). Again we have three different cases to investigate.

$y = 0, z \neq 0 \Rightarrow y'$ is completely determined by $y' \equiv \frac{-x}{z} \pmod{p}$ since we are working in the field $Z_p$. Notice that $y' \not\equiv 0 \pmod{p}$ for the same reason, since $x \equiv 0 \pmod{p}$.

The same thing happens for $z = 0, y \neq 0$.

$y, z \neq 0$. Choose $y'$ and $z'$ is determined by $z' \equiv (x + zy')/y \pmod{p}$ or vice versa. Again, this is possible because we are working in a field. Notice here that $y' = z' = 0$ is not an option, so again we have $p$ choices.

In total for $b$: $p^2$ choices. $|\mathrm{Aut}(Z_{p^2} \rtimes Z_p)| = p^3(p - 1)$, so

$$\mathcal{N}(Z_{p^2} \rtimes Z_p) = \frac{(p^2 - p)(p^2 - 1)p^2}{p^3(p - 1)} = p^2 - 1.$$

In summary for $(Z_{p^2} \times Z_p) \rtimes Z_p$:

$$\begin{cases} n_2 = p^4 - p^3 \\ n_1 = p^3 - 1 \\ \mathcal{N}(Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_{p^2}) = p^2 \\ \mathcal{N}(Z_p \times Z_p) = p + 1 \\ \mathcal{N}(Z_{p^3}) = 0 \\ \mathcal{N}(Z_{p^2} \times Z_p) = p + 1 \\ \mathcal{N}(Z_p \times Z_p \times Z_p) = 0 \\ \mathcal{N}(Z_{p^2} \rtimes Z_p) = p^2 - 1 \\ \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 1\,. \end{cases}$$

### 2.3.5 (viii) $Z_{p^2} \rtimes Z_{p^2}$

This group is isomorphic with

$$\langle a, b : a^{p^2} = b^{p^2} = 1, ba = a^{1+p}b \rangle$$

with the operation

$$(x, y)(x', y') = (x + x' + pyx', y + y')\,.$$

Both components modulo $p^2$.

**Lemma 2.3.12.** *For $g = (x, y) \in Z_{p^2} \rtimes Z_{p^2}$ with the operation above, it holds that*

$$g^n = (nx + \frac{pn(n-1)xy}{2}, ny)\,.$$

*Proof.* Proof by induction. It holds for $g^1 = (x, y)$. Assume that it holds for $g^n$.

$$\begin{aligned} g^{n+1} &= g^n g \\ &= (nx + \frac{pn(n-1)xy}{2}, ny)(x, y) \\ &= (nx + \frac{pn(n-1)xy}{2} + x + p(ny)x, ny + y) \\ &= ((n+1)x + \frac{p(n^2-n)xy}{2} + \frac{2pnxy}{2}, (n+1)y) \\ &= ((n+1)x + \frac{p(n+1)nxy}{2}, (n+1)y) \end{aligned}$$

The result follows by induction. ∎

**Proposition 2.3.13.** *For $Z_{p^2} \rtimes Z_{p^2}$ it holds that*

$$\begin{cases} n_2 = p^4 - p^2 \\ n_1 = p^2 - 1\,. \end{cases}$$

*Proof.* Since

$$g^p = (x,y)^p = (px + \frac{pp(p-1)xy}{2}, py) = (px, py)\,,$$

we see that $g$ has order less or equal to $p$ only if both $x$ and $y$ are multiples of $p$. That gives us a total of $p^2$ elements since both components are calculated modulo $p^2$. $n_1 = p^2 - 1$. Also, since

$$g^{p^2} = (x,y)^{p^2} = (p^2x + \frac{pp^2(p^2-1)xy}{2}, p^2y) = (0,0)\,,$$

there are obviously no elements of higher order than $p^2$, and thus $n_2 = p^4 - p^2$. ⨳

From Theorem 2.1.4 and its corollaries we get:

$$\begin{cases} \mathcal{N}(Z_p) = p+1 \\ \mathcal{N}(Z_{p^2}) = p^2 + p \\ \mathcal{N}(Z_{p^3}) = 0\,. \end{cases}$$

**Proposition 2.3.14.** *For $Z_{p^2} \rtimes Z_{p^2}$ it holds that*

$$\mathcal{N}(Z_p \times Z_p) = 1\,.$$

*Proof.* Take two elements of order $p$ and multiply them:

$$(p\alpha, p\beta)(p\alpha', p\beta') = (p\alpha + p\alpha' + pp\beta p\alpha', p\beta + p\beta') = (p\alpha + p\alpha', p\beta + p\beta')\,.$$

We see that all elements of order $p$ commute. The result follows from Theorem 2.2.18. ⨳

From Theorem 2.2.21 we get

$$\mathcal{N}(Z_p \times Z_p \times Z_p) = \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 0\,.$$

**Proposition 2.3.15.** *The center of $G = Z_{p^2} \rtimes Z_{p^2}$ with the operation defined above is*

$$Z(G) = \langle (p,0), (0,p) \rangle \cong Z_p \times Z_p\,.$$

*Proof.* From the operation we get that

$$gg' = g'g \Leftrightarrow yx' \equiv y'x \pmod{p}\,.$$

Let $g' \in G$ be arbitrary. It then follows that we must have $x, y \equiv 0 \pmod{p}$, so the elements on the form $g = (p\alpha, p\beta)$ commute with all other elements. We see that $Z(G)$ consists exactly of the elements of order $p$. ⨳

**Proposition 2.3.16.** *In $Z_{p^2} \rtimes Z_{p^2}$ it holds that*

$$\begin{cases} \mathcal{N}(Z_{p^2} \times Z_p) = p+1 \\ \mathcal{N}(Z_{p^2} \rtimes Z_p) = 0\,. \end{cases}$$

*Proof.* The first assertion follows directly from the preceding proposition and Theorem 2.2.4. The second assertion follows from the fact that if all elements of order $p$ commute in $G$, then it must also be true in all of its subgroups. ⧖

In summary for $Z_{p^2} \rtimes Z_{p^2}$:

$$\begin{cases} n_2 = p^4 - p^2 \\ n_1 = p^2 - 1 \\ \mathcal{N}(Z_p) = p+1 \\ \mathcal{N}(Z_{p^2}) = p^2 + p \\ \mathcal{N}(Z_p \times Z_p) = 1 \\ \mathcal{N}(Z_{p^3}) = 0 \\ \mathcal{N}(Z_{p^2} \times Z_p) = p+1 \\ \mathcal{N}(Z_p \times Z_p \times Z_p) = 0 \\ \mathcal{N}(Z_{p^2} \rtimes Z_p) = 0 \\ \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 0\,. \end{cases}$$

### 2.3.6 (ix) $(Z_{p^2} \rtimes Z_p) \times Z_p$

We know from the previous chapter that this group is isomorphic with

$$\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = ac, cb = bc \rangle$$

and that is has the operation

$$((x,y),z)((x',y'),z') = ((x + x' + pyx', y + y'), z + z')\,.$$

First component modulo $p^2$, second and third component modulo $p$.

**Lemma 2.3.17.** *For $g = ((x,y),z) \in (Z_{p^2} \rtimes Z_p) \times Z_p$ with the operation above, it holds that*

$$g^n = ((nx + \frac{pn(n-1)xy}{2}, ny), nz)\,.$$

*Proof.* Proof by induction. It holds for $g^1 = ((x, y), z)$. Assume that it holds for $g^n$.

$$\begin{aligned} g^{n+1} &= g^n g \\ &= ((nx + \frac{pn(n-1)xy}{2}, ny), nz)((x, y), z) \\ &= ((nx + \frac{pn(n-1)xy}{2} + x + p(ny)x, ny + y), nz + z) \\ &= (((n+1)x + \frac{p(n^2-n)xy}{2} + \frac{2pnxy}{2}, (n+1)y), (n+1)z) \\ &= (((n+1)x + \frac{p(n+1)nxy}{2}, (n+1)y), (n+1)z) \end{aligned}$$

The result follows by induction. ⨳

**Proposition 2.3.18.** *For $(Z_{p^2} \rtimes Z_p) \times Z_p$ it holds that*

$$\begin{cases} n_2 = p^4 - p^3 \\ n_1 = p^3 - 1\,. \end{cases}$$

*Proof.* First we notice that

$$g^p = ((x, y), z)^p = ((px + \frac{pp(p-1)xy}{2}, py), pz) = ((px, 0), 0)\,.$$

This is equal to $((0, 0), 0)$ exactly when $x$ is a multiple of $p$, so as before we have $n_1 = p^3 - 1$. We have no elements of order $p^3$ since

$$g^{p^2} = ((x, y), z)^{p^2} = ((p^2x + \frac{pp^2(p^2-1)xy}{2}, p^2y), p^2z) = ((0, 0), 0)\,.$$

Thus $n_2 = p^4 - p^3$. ⨳

Just as usual, from Theorem 2.1.4:

$$\begin{cases} \mathcal{N}(Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_{p^2}) = p^2\mathcal{N}(Z_{p^3}) = 0\,. \end{cases}$$

**Proposition 2.3.19.** *The center of $G = (Z_{p^2} \rtimes Z_p) \times Z_p$ with the operation defined above is*

$$Z(G) = \langle((p, 0), 0), ((0, 0), 1)\rangle \cong Z_p \times Z_p\,.$$

*Proof.* We see from the operation that

$$gg' = g'g \Leftrightarrow yx' \equiv y'x \pmod{p}$$

For an arbitrary $g'$ we then need that $x = p\alpha$ and $y = 0$. $z$ is though arbitrary. The result follows. ⨳

**Proposition 2.3.20.** *In* $(Z_{p^2} \rtimes Z_p) \times Z_p$ *it holds that*

$$\begin{cases} \mathcal{N}(Z_p \times Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_p \times Z_p \times Z_p) = 1 \\ \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 0\,. \end{cases}$$

*Proof.* I will first show that all elements of order $p$ commute with all other elements of order $p$:

$$((p\alpha, y), z)((p\alpha', y'), z') = ((p\alpha + p\alpha' + p^2 y\alpha', y + y'), z + z') = ((p\alpha + p\alpha', y + y'), z + z')\,.$$

Now Theorem 2.2.18 implies that

$$\mathcal{N}(Z_p \times Z_p) = \frac{(p^2 + p + 1)(p^2 + p)}{p^2 + p} = p^2 + p + 1$$

and also

$$\mathcal{N}(Z_p \times Z_p \times Z_p) = 1\,.$$

Finally, since all elements of order $p$ commutes, $\mathcal{N}((Z_p \times Z_p) \rtimes Z_p)$ must be zero. ⨳

**Proposition 2.3.21.** *For* $(Z_{p^2} \rtimes Z_p) \times Z_p$ *it holds that*

$$\mathcal{N}(Z_{p^2} \times Z_p) = p\,.$$

*Proof.* We want to examine when elements of order $p^2$ commute with elements of order $p$. A few quick calculations show that

$$((x, y, ), z)((p\alpha', y'), z') = ((x + p\alpha' + pyp\alpha', y + y'), z + z') = ((x + p\alpha', y + y'), z + z')$$

and

$$((p\alpha', y'), z')((x, y), z) = ((x + p\alpha' + py'x, y + y'), z + z')\,.$$

Thus they commute only if $y'x \equiv 0 \pmod{p}$. But if $x$ was a multiple of $p$, then would $((x, y), z)$ not be an element of order $p^2$, so we must have $y' = 0$. The conclusion is that the generator of order $p$ must necessarily lie in the center. We must though exclude the elements in $\langle((p, 0), 0)\rangle$, since we would otherwise break the condition of independence of generators.

We thus have $p^2 - p$ choices for the generator of order $p$ and can choose the generator of order $p^2$ freely: $p^4 - p^3$ choices.

We conclude that

$$\mathcal{N}(Z_{p^2} \times Z_p) = \frac{(p^4 - p^3)(p^2 - p)}{p^3(p - 1)^2} = p\,.$$

⨳

**Proposition 2.3.22.** *For $(Z_{p^2} \rtimes Z_p) \times Z_p$ it holds that*

$$\mathcal{N}(Z_{p^2} \rtimes Z_p) = p^2 \,.$$

*Proof.* Let $a = ((x, y), z), b = ((p\alpha', y'), z')$.

$$ba = ((x + p\alpha' + py'x, y + y'), z + z')$$

and

$$a^{1+p}b = ((x + p\alpha' + px, y + y'), z + z') \,,$$

hence the relation is satisfied only if $y'x \equiv x \pmod{p}$. Because of the order of $a$, $x \not\equiv 0 \pmod{p}$, and then $y' = 1$. We get that $b = ((p\alpha', 1), z')$.

We have $p^4 - p^3$ choices for $a$ and $p^2$ choices for $b$. Note that it cannot happen that $\langle b \rangle = \langle ((p, 0), 0) \rangle$, which was actually guaranteed by Result 2.2.16.

We then get

$$\mathcal{N}(Z_{p^2} \rtimes Z_p) = \frac{(p^4 - p^3)p^2}{p^3(p-1)} = p^2 \,.$$

⨵

In summary for $(Z_{p^2} \rtimes Z_p) \times Z_p$:

$$\begin{cases} n_2 = p^4 - p^3 \\ n_1 = p^3 - 1 \\ \mathcal{N}(Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_{p^2}) = p^2 \\ \mathcal{N}(Z_p \times Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_{p^3}) = 0 \\ \mathcal{N}(Z_{p^2} \times Z_p) = p \\ \mathcal{N}(Z_p \times Z_p \times Z_p) = 1 \\ \mathcal{N}(Z_{p^2} \rtimes Z_p) = p^2 \\ \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 0 \,. \end{cases}$$

### 2.3.7 (x) $(Z_p \times Z_p) \rtimes Z_{p^2}$

This group is isomorphic with

$$\langle a, b, c : a^p = b^p = c^{p^2} = 1, ba = ab, ca = abc, cb = bc \rangle$$

with the operation

$$((x, y), z)((x', y'), z') = ((x + x', y + y' + zx'), z + z')$$

with first and second component modulo $p$ and the third component modulo $p^2$.

**Lemma 2.3.23.** *For $g = ((x, y), z) \in (Z_p \times Z_p) \rtimes Z_{p^2}$ with the operation above, it holds that*

$$g^n = ((nx, ny + \frac{n(n-1)xz}{2}), nz)\,.$$

*Proof.* Proof by induction. It holds for $g^1 = (x, y)$. Assume that it holds for $g^n$.

$$\begin{aligned} g^{n+1} &= g^n g \\ &= ((nx, ny + \frac{n(n-1)xz}{2}), nz)((x, y), z) \\ &= ((nx + x, ny + \frac{n(n-1)xz}{2} + y + (nz)x), nz + z) \\ &= (((n+1)x, (n+1)y + \frac{n(n-1)xz}{2} + \frac{2nxz}{2}), (n+1)z) \\ &= (((n+1)x, (n+1)y + \frac{(n+1)nxz}{2}), (n+1)z) \end{aligned}$$

The result follows by induction. ⨳

**Proposition 2.3.24.** *For $(Z_p \times Z_p) \rtimes Z_{p^2}$ it holds that*

$$\begin{cases} n_2 = p^4 - p^3 \\ n_1 = p^3 - 1\,. \end{cases}$$

*Proof.* We see that

$$g^p = ((px, py + \frac{p(p-1)xz}{2}), pz) = ((0, 0), pz)$$

and

$$g^{p^2} = ((p^2x, p^2y + \frac{p^2(p^2-1)xz}{2}), p^2z) = ((0, 0), 0)\,.$$

Thus $g$ has order $p$ only if $z$ is a multiple of $p$. We then have $p$ choices for each component, and $n_1 = p^3 - 1$. No element has order $p^3$, so $n_2 = p^4 - p^3$. ⨳

From Theorem 2.1.4 and its corollaries:

$$\begin{cases} \mathcal{N}(Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_{p^2}) = p^2 \\ \mathcal{N}(Z_{p^3}) = 0\,. \end{cases}$$

**Proposition 2.3.25.** *The center of $G = (Z_p \times Z_p) \rtimes Z_{p^2}$ with the operation defined above is*

$$Z(G) = \langle((0, 1), 0), ((0, 0), p)\rangle \cong Z_p \times Z_p\,.$$

*Proof.* From the operation we get that

$$gg' = g'g \Leftrightarrow zx' \equiv z'x \pmod{p}.$$

If we let $g'$ be arbitrary, we must have $x = 0$ and $z = p\gamma$. ⨳

**Proposition 2.3.26.**

$$\begin{cases} \mathcal{N}(Z_p \times Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_p \times Z_p \times Z_p) = 1 \\ \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 0\,. \end{cases}$$

*Proof.* I will first show that all elements of order $p$ commute with all other elements of order $p$:

$$((x,y),p\gamma)((x',y'),p\gamma') = ((x+x', y+y'+p\gamma z'), p\gamma + p\gamma') = ((x+x', y+y'), p\gamma + p\gamma')\,.$$

Now Theorem 2.2.18 implies that

$$\mathcal{N}(Z_p \times Z_p) = \frac{(p^2+p+1)(p^2+p)}{p^2+p} = p^2 + p + 1$$

and also

$$\mathcal{N}(Z_p \times Z_p \times Z_p) = 1\,.$$

We also arrive at

$$\mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 0\,.$$

⨳

**Proposition 2.3.27.** *For $(Z_p \times Z_p) \rtimes Z_{p^2}$ it holds that*

$$\mathcal{N}(Z_{p^2} \times Z_p) = p\,.$$

*Proof.* We want to examine when elements of order $p^2$ commute with elements of order $p$.

We have that

$$((x,y),z)((x',y'),p\gamma') = ((x+x', y+y'+zx'), z+p\gamma') = ((x+x', y+y'+zx'), z+p\gamma')$$

and

$$((x',y'),p\gamma')((x,y),z) = ((x+x', y+y'+p\gamma' x), z+p\gamma') = ((x+x', y+y'), z+p\gamma')\,.$$

Thus they commute only if $z'x \equiv 0 \pmod{p}$. But if $z$ was a multiple of $p$, then would $((x,y),z)$ not be an element of order $p^2$, so we must have $x' = 0$. Furthermore, $((x,y),z)^p = ((0,0),pz)$, so we must exclude the elements in $\langle((0,0),p)\rangle$ from the

choices of generator of order $p$, since we would otherwise break the condition of independence of generators. That leaves us with $p^2 - p$ generators of order $p$. We can though choose the generator of order $p^2$ freely, since the other generator is in the center and then automatically fulfilling the relation. We conclude that

$$N(Z_{p^2} \times Z_p) = \frac{(p^4 - p^3)(p^2 - p)}{p^3(p-1)^2} = p\,.$$

⁒

**Proposition 2.3.28.** *In $(Z_p \times Z_p) \rtimes Z_{p^2}$ it holds that*

$$\mathcal{N}(Z_{p^2} \rtimes Z_p) = 0\,.$$

*Proof.* We are searching for elements fulfilling

$$a^{p^2} = b^p = 1, ba = a^{1+p}b\,.$$

Take one element of order $p^2$ and one element of order $p$ and set them as $a$ and $b$. We want them to satisfy $ba = a^{1+p}b$. First:

$$ba = ((x', y'), p\gamma')((x, y), z) = ((x+x', y+y'+p\gamma' x), z+p\gamma') = ((x+x', y+y'), z+p\gamma')\,.$$

Continuing with the right side of the relation:

$$\begin{aligned} a^{1+p}b = &= ((x, y, ), z)^{1+p}((x', y'), p\gamma') \\ &= (((1+p)x, (1+p)y + \frac{(1+p)(1+p-1)xz}{2}), (1+p)z)((x', y', p\gamma') \\ &= ((x, y), z + pz)((x', y'), p\gamma') \\ &= ((x + x', y + y' + zx' + pzx'), z + pz + p\gamma') \\ &= ((x + x', y + y' + zx'), z + p\gamma' + pz)\,. \end{aligned}$$

Equality in the third component can only hold if $z \equiv 0 \bmod p$, but that is impossible since that would imply that $a = ((x, y), z)$ is an element of order $p$ ! We can therefore not find elements in $G$ satisfying the relations of $Z_{p^2} \rtimes Z_p$. ⁒

In summary for $(Z_p \times Z_p) \rtimes Z_{p^2}$:

$$\begin{cases} n_2 = p^4 - p^3 \\ n_1 = p^3 - 1 \\ \mathcal{N}(Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_{p^2}) = p^2 \\ \mathcal{N}(Z_p \times Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_{p^3}) = 0 \\ \mathcal{N}(Z_{p^2} \times Z_p) = p \\ \mathcal{N}(Z_p \times Z_p \times Z_p) = 1 \\ \mathcal{N}(Z_{p^2} \rtimes Z_p) = 0 \\ \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 0\,. \end{cases}$$

### 2.3.8 (xi) $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_1} Z_p$

This group is isomorphic with

$$\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = abc, cb = bc \rangle .$$

The operation becomes

$$((x, y), z)((x', y'), z') = ((x + x' + \frac{pzx'(x' - 1)}{2} + pyx', y + y' + zx'), z + z') .$$

First component is modulo $p^2$, the second and third components are modulo $p$.

**Lemma 2.3.29.** *For $g = ((x, y), z) \in (Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_1} Z_p$ with the operation above, it holds that*

$$g^n = ((nx+\frac{pn(n-1)x(x-1)z}{4}+\frac{pn(n-1)xy}{2}+\frac{p(n-2)(n-1)nx^2z}{6}, ny+\frac{n(n-1)xz}{2}), nz) .$$

*Proof.* Proof by induction, it is exactly similar to the analogue in the previous groups. ⧖

**Proposition 2.3.30.** *In $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_1} Z_p$ it holds that*

$$\begin{cases} n_2 = p^4 - p^3 \\ n_1 = p^3 - 1 . \end{cases}$$

*Proof.* We see that

$$\begin{aligned} g^p = & ((px + \tfrac{pp(p-1)x(x-1)z}{4} + \tfrac{pp(p-1)xy}{2} + \tfrac{p(p-2)(p-1)px^2z}{6}, py + \tfrac{p(p-1)xz}{2}), pz) \\ = & ((px, 0, 0) \end{aligned}$$

so $g$ has order $p$ only if $x$ is a multiple of $p$. As before, $n_1 = p^3 - 1$ $g^{p^2} = ((0, 0), 0)$, so $n_2 = p^4 - p^3$. ⧖

Thanks to Theorem 2.1.4 we get

$$\begin{cases} \mathcal{N}(Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_{p^2}) = p^2 \\ \mathcal{N}(Z_{p^3}) = 0 . \end{cases}$$

**Proposition 2.3.31.** *For $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_1} Z_p$ it holds that*

$$\begin{cases} \mathcal{N}(Z_p \times Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_p \times Z_p \times Z_p) = 1 \\ \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 0 . \end{cases}$$

*Proof.* We multiply two elements of order $p$:

$$\begin{array}{rcl}((p\alpha,y),z)((p\alpha',y'),z') = & ((p\alpha+p\alpha'+\frac{pzp\alpha'(p\alpha'-1)}{2}+pyp\alpha',y+y'+zp\alpha'),z+z') = \\ = & ((p\alpha+p\alpha',y+y'),z+z')\end{array}.$$

All elements of order $p$ commute and the product of elements of order $p$ is of order $p$. The results follow from Theorem 2.2.18 and the fact that not all elements of order $p$ commute in $(Z_p \times Z_p) \rtimes Z_p$. ⧛

**Lemma 2.3.32.** *For every $g \in G = (Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_1} Z_p$ of order $p^2$, it holds that $Z(G) < \langle g \rangle$.*

**Proposition 2.3.33.** *For $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_1} Z_p$ with the operation defined above it holds that*

$$\mathcal{N}(Z_{p^2} \times Z_p) = 0$$

*and*

$$Z(G) = \langle((p,0),0)\rangle \cong Z_p\,.$$

*Proof.* By multiplying an element of order $p$ with an element of order $p^2$ we get

$$((p\alpha',y'),z')((x,y),z) = ((x+p\alpha'+\frac{pz'x(x-1)}{2}+py'x, y+y'+zx'),z+z')$$

and

$$\begin{array}{rcl}((x,y),z)((p\alpha',y'),z') = & ((x+p\alpha'+\frac{pzp\alpha'(p\alpha'-1)}{2}+pyp\alpha',y+y'+zp\alpha'),z+z') \\ = & ((x+p\alpha',y+y'),z+z')\,.\end{array}$$

If these elements are to commute, they must satisfy

$$\begin{cases}\frac{z'x(x-1)}{2}+y'x \equiv 0 \pmod p \\ z'x \equiv 0 \pmod p\,.\end{cases}$$

But since $x \not\equiv 0 \pmod p$, we must have $z' = 0$. The first equation then becomes $y'x \equiv 0 \pmod p$. By the same argument, we must have $y' = 0$. So the only elements of order $p$ that commute with all (or any, for that matter) elements of order $p^2$, are the elements on the form $((p\alpha',0),0)$.

All elements of order $p$ commute with each other, so we have found the center: $Z(G) = \langle((p,0),0)\rangle \cong Z_p$. This also means that the only possible choices of generator of order $p$ are the generators of $Z(G)$, but because of the preceding lemma, the generators would then not be independent; $\langle b\rangle < \langle a\rangle$! Therefore, $N(Z_{p^2} \times Z_p) = 0$. ⧛

**Proposition 2.3.34.** *In $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_1} Z_p$ it holds that*

$$N(Z_{p^2} \rtimes Z_p) = p\,.$$

*Proof.* We want to find elements $a, b$ fulfilling $a^{p^2} = b^p = 1, ba = a^{p+1}b$. The left side of the last relation is

$$ba = ((p\alpha', y'), z')((x, y), z) = ((x + p\alpha' + \frac{pz'x(x-1)}{2} + py'x, y + y' + z'x), z + z')\,.$$

We then have that

$$\begin{aligned} a^{1+p} = &\ ((x + px + \tfrac{p(1+p)px(x-1)z}{4} + \tfrac{p(1+p)pxy}{2} + \tfrac{p(p-1)p(1+p)x^2z}{6}, y + \tfrac{(1+p)pxz}{2}), z) \\ = &\ ((x + px, y), z)\,, \end{aligned}$$

which leads to

$$\begin{aligned} a^{1+p}b = &\ ((x + px, y), z)((p\alpha', y'), z') \\ = &\ ((x + p\alpha' + px + \tfrac{pzp\alpha'(p\alpha'-1}{2}, y + y' + zp\alpha'), z + z') \\ = &\ ((x + p\alpha' + px, y + y'), z + z')\,. \end{aligned}$$

The conditions for $a$ and $b$ are then

$$\begin{cases} \frac{z'x(x-1)}{2} + y'x \equiv x \pmod p \\ z'x \equiv 0 \pmod p\,. \end{cases}$$

But since $((x, y), z)$ is of order $p^2$, $x \not\equiv 0 \pmod p$ must hold. We can see that that implies $z' = 0$. Inserting this in the first condition, we get $y'x \equiv x \pmod p$. Again, $x \not\equiv 0 \pmod p$ and so $y' = 1$. We conclude that the generator of order $p^2$ is arbitrary, but the element of order $p$ must be on the form $((p\alpha', 1), 0)$. There are therefore $p^4 - p^3$ choices for $a$ and $p$ choices for $b$. $|\mathrm{Aut}(Z_{p^2} \rtimes Z_p)| = p^3(p-1)$ now gives us the result

$$\mathcal{N}(Z_{p^2} \rtimes Z_p) = \frac{(p^4 - p^3)p}{p^3(p-1)} = p\,.$$

⨱

In summary for $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_1} Z_p$:

$$\begin{cases} n_2 = p^4 - p^3 \\ n_1 = p^3 - 1 \\ \mathcal{N}(Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_{p^2}) = p^2 \\ \mathcal{N}(Z_p \times Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_{p^3}) = 0 \\ \mathcal{N}(Z_{p^2} \times Z_p) = 0 \\ \mathcal{N}(Z_p \times Z_p \times Z_p) = 1 \\ \mathcal{N}(Z_{p^2} \rtimes Z_p) = p \\ \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 0 \end{cases}$$

### 2.3.9 (xii) $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_2} Z_p$, $p > 3$

*Observation.* We must assume that $p > 3$ in this case, since it collapses nontrivially for $p \leq 3$.

This group is isomorphic with

$$\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = a^{1+p}bc, cb = a^p bc \rangle$$

with the operation

$$gg' = ((x + x' + \frac{pz(z-1)x'}{2} + \frac{pzx'(x'-1)}{2} + pzy' + pyx', y + y' + zx'), z + z')$$

or, equally,

$$gg' = ((x + x' + \frac{pz^2x'}{2} + \frac{pzx'^2}{2} + pzy' + pyx' - pzx', y + y' + zx'), z + z') \,.$$

The first component is modulo $p^2$ and the second and third are both modulo $p$.

**Lemma 2.3.35.** *For $g = ((x, y), z) \in (Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_2} Z_p$ with the operation above, it holds that*

$$g^n = \begin{pmatrix} nx + \frac{pn(n-1)(2n-1)xz^2}{12} + \frac{pn(n-1)(n-2)x^2z}{6} + \frac{pn(n-1)}{4}(2yz + 2xy - 2xz + x^2z) \\ ny + \frac{n(n-1)xz}{2} \\ nz \end{pmatrix} .$$

*Proof.* Proof by induction. There is no difficulty in this proof, the verification is in the line of the previous analogue results for the other groups. ⧛

**Proposition 2.3.36.** *For $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_2} Z_p$ it holds that*

$$\begin{cases} n_2 = p^4 - p^3 \\ n_1 = p^3 - 1 \,. \end{cases}$$

*Proof.* $g^p = ((px, 0, 0)$, so $g$ has order $p$ only if $x$ is a multiple of $p$. As before, $n_1 = p^3 - 1$ $g^{p^2} = ((0, 0), 0)$, so $n_2 = p^4 - p^3$. ⧛

From Theorem 2.1.4 we get

$$\begin{cases} \mathcal{N}(Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_{p^2}) = p^2 \\ \mathcal{N}(Z_{p^3}) = 0 \,. \end{cases}$$

**Proposition 2.3.37.** *The center of $G = (Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_2} Z_p$ with the operation defined above is*

$$Z(G) = \langle ((p, 0), 0) \rangle \cong Z_p \,.$$

*Proof.* Taking a look at the second component in the operation, we see that $zx' \equiv z'x \pmod{p}$ must be satisfied for two commuting elements. If this is to be satisfied for an arbitrary $g' = ((x', y'), z')$, then we must have $x = p\alpha$ and $z = 0$. Turning to the first component, we see that the only terms remaining form the requirement $z'y \equiv yx' \pmod{p}$. This holds for arbitrary $x', z'$ only if $y = 0$. ⧖

**Proposition 2.3.38.** *In $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_2} Z_p$, the product of two elements of order $p$ has order $p$ and it commutes if and only if $zy' \equiv z'y \pmod{p}$.*

*Proof.* By multiplying two elements of order $p$ we get

$$((p\alpha, x), z)((p\alpha', y'), z') = ((p\alpha + p\alpha' + pzy', y + y'), z + z')\,.$$

The result follows by inspection of the first component. ⧖

**Proposition 2.3.39.** *For $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_2} Z_p$ it holds that*

$$\begin{cases} \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 1 \\ \mathcal{N}((Z_p \times Z_p) \times Z_p) = 0 \\ \mathcal{N}(Z_p \times Z_p) = p + 1\,. \end{cases}$$

*Proof.* The previous proposition implies that $G$ has a subgroup consisting of the elements of order $p$, and that not all elements in it commutes. We find that this subgroup, let us call it $H$, is nonabelian, and since there is only one nonabelian group of order $\leq p^3$ with all elements having order $p$, we conclude that $H \cong (Z_p \times Z_p) \rtimes Z_p$. There are only $p^3 - 1$ elements of order $p$ however, so

$$\mathcal{N}((Z_p \times Z_p) \times Z_p) = 0\,.$$

Every smaller subgroup consisting of elements of order $p$ must be a subgroup of $H$, since it contains *all* the elements of order $p$. Proposition 2.2.11 gives the last result. ⧖

**Lemma 2.3.40.** *For every $g \in G = (Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_2} Z_p$ of order $p^2$, it holds that $Z(G) < \langle g \rangle$.*

**Proposition 2.3.41.** *In $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_2} Z_p$ it holds that*

$$\mathcal{N}(Z_{p^2} \times Z_p) = 1\,.$$

*Proof.* Let $g = ((x, y), z), g' = ((p\alpha', y'), z')$. We see that

$$gg' = ((x + p\alpha' + pzy', y + y'), z + z')$$

and also

$$g'g = ((x + p\alpha' + \frac{pz'^2x}{2} + \frac{pz'x^2}{2} + pz'y + py'x - pz'x, y + y' + z'x), z + z')\,.$$

Equality in the second component implies that

$$z'x \equiv 0 \pmod{p}\,.$$

We want $g$ to be of order $p^2$, so $x \not\equiv 0 \pmod{p}$, and thus $z' = 0$. Now taking a look at the first component, we get

$$y'x \equiv zy' \pmod{p} \Leftrightarrow y'(x - z) \equiv 0 \pmod{p},\,.$$

Assume first that $x - z \not\equiv 0 \pmod{p}$. That would imply $y' = 0$. Thus the only elements that such elements of order $p^2$ commute with are in the center, $g' \in Z(G)$. But from Lemma 2.3.40 we see that such elements of order $p^2$ cannot form subgroups isomorphic with $\mathcal{N}(Z_{p^2} \times Z_p)$.

Assume then that $x \equiv z \pmod{p}$. $y'$ is then arbitrary with the exception that $y' \neq 0$, since that would again lead to the previous situation. We have $p^2 - p$ choices for $x$ and $p$ choices for $y$. $z$ is completely determined by the choice of $x$. We have $p$ choices for $\alpha'$ and $p - 1$ choices for $y'$. This totals to $(p^2 - p)p \cdot p(p - 1) = p^3(p - 1)^2$. $|\mathrm{Aut}(Z_{p^2} \times Z_p)| = p^3(p - 1)^2$, so

$$\mathcal{N}(Z_{p^2} \times Z_p) = \frac{p^3(p-1)^2}{p^3(p-1)^2} = 1\,.$$

⨳

**Proposition 2.3.42.** *For $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_2} Z_p$ it holds that*

$$\mathcal{N}(Z_{p^2} \rtimes Z_p) = p - 1\,.$$

*Proof.* Let $a = ((x, y), z), b = ((p\alpha', y'), z')$. The calculations are then

$$ba = ((x + p\alpha' + \frac{pz'(z'-1)x}{2} + \frac{pz'x(x-1)}{2} + pz'y + py'x, y + y' + z'x), z + z')\,,$$

$$a^{1+p}b = ((x + px, y), z)((p\alpha', y'), z') = ((x + p\alpha' + px + pzy', y + y'), z + z')\,.$$

The condition for the second component is then that $z'x \equiv 0 \pmod{p}$.

$x \not\equiv 0 \pmod{p} \Rightarrow z' = 0$. The condition for the first component is then reduced to

$$y'x \equiv x + zy' \pmod{p}\,.$$

We see that we must have $y' \not\equiv 0 \pmod{p}$. That leaves us with $p$ choices for $\alpha'$ and $p-1$ choices for $y'$. $\langle a \rangle$ and $\langle b \rangle$ can never coincide, so we can choose $a$ with $y'x \equiv x+zy' \pmod{p}$ as the only restriction. We get $p^2-p$ choices for $x$ and $p$ choices for $y$. Now $z$ is fully determined by the condition. In total we have $(p^2-p)p \cdot p(p-1)$ choices for $a$ and $b$. We thus get the result

$$\mathcal{N}(Z_{p^2} \rtimes Z_p) = \frac{p^3(p-1)^2}{p^3(p-1)} = p-1\,.$$

⨳

In summary for $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_2} Z_p$:

$$\begin{cases} n_4 = 0 \\ n_3 = 0 \\ n_2 = p^4 - p^3 \\ n_1 = p^3 - 1 \\ \mathcal{N}(Z_p) = p^2 + p + 1 \\ \mathcal{N}(Z_{p^2}) = p^2 \\ \mathcal{N}(Z_p \times Z_p) = p+1 \\ \mathcal{N}(Z_{p^3}) = 0 \\ \mathcal{N}(Z_{p^2} \times Z_p) = 1 \\ \mathcal{N}(Z_p \times Z_p \times Z_p) = 0 \\ \mathcal{N}(Z_{p^2} \rtimes Z_p) = p-1 \\ \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 1\,. \end{cases}$$

### 2.3.10 (xiii) $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_3} Z_p$, $p > 3$

Again, it is necessary to assume $p > 3$. As was showed in the preceding chapter, if we let $d \not\equiv 0, 1 \pmod{p}$, then we have the presentation

$$\langle a, b, c : a^{p^2} = b^p = c^p = 1, ba = a^{1+p}b, ca = a^{1+dp}bc, cb = a^{dp}bc \rangle$$

and the operation

$$gg' = ((x + x' + \frac{pdz(z-1)x'}{2} + \frac{pzx'(x'-1)}{2} + pdzy' + pyx', y + y' + zx'), z + z')\,,$$

with the first component modulo $p^2$ and the second and third component modulo $p$.

**Lemma 2.3.43.** *For $g = ((x,y),z) \in (Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_3} Z_p$ with the operation above, it holds that*

$$g^n = \begin{pmatrix} nx + \frac{pn(n-1)(2n-1)dxz^2}{12} + \frac{pn(n-1)(n-2)x^2z}{6} + \frac{pn(n-1)}{4}(2dyz + 2xy - (d+1)xz + x^2z) \\ ny + \frac{n(n-1)xz}{2} \\ nz \end{pmatrix}.$$

*Proof.* The proof follows the same procedure as the previous analogue results for the other groups and is left out for readability and brevity. ⨳

**Proposition 2.3.44.** *For* $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_3} Z_p$ *it holds that*

$$\begin{cases} n_2 = p^4 - p^3 \\ n_1 = p^3 - 1\,. \end{cases}$$

*Proof.* $g^p = ((px, 0, 0)$, so $g$ has order $p$ only if $x$ is a multiple of $p$. As before, $n_1 = p^3 - 1$ $g^{p^2} = ((0,0),0)$, so $n_2 = p^4 - p^3$. ⨳

**Proposition 2.3.45.** *The center of* $G = (Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_3} Z_p$ *with the operation defined above is*

$$Z(G) = \langle((p,0),0)\rangle \cong Z_p\,.$$

*Proof.* This is indeed very similar to the previous group. Taking a look at the second component, we see that $zx' \equiv z'x \pmod p$ must be satisfied for two commuting elements. If this is to be satisfied for an arbitrary $g' = ((x', y'), z')$, then we must have $x = p\alpha$ and $z = 0$. Turning to the first component, we see that the only terms remaining form the requirement $dz'y \equiv yx' \pmod p \Leftrightarrow y(dz' - x') \equiv 0 \pmod p$. This holds for arbitrary $x', z'$ only if $y = 0$. ⨳

**Proposition 2.3.46.** *In* $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_3} Z_p$*, the product of two elements of order* $p$ *has order* $p$*. They commute if and only if* $zy' \equiv z'y \pmod p$*.*

*Proof.* We first see that

$$((p\alpha, x), z)((p\alpha', y'), z') = ((p\alpha + p\alpha' + pdzy', y + y'), z + z')\,.$$

It then holds that

$$gg' = g'g \Leftrightarrow dzy' \equiv dz'y \pmod p\,.$$

By assumption, $d \not\equiv 0 \pmod p$. We are working in the field $Z_p$, so the result follows. ⨳

**Proposition 2.3.47.** *For* $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_3} Z_p$ *it holds that*

$$\begin{cases} \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 1 \\ \mathcal{N}((Z_p \times Z_p) \times Z_p) = 0 \\ \mathcal{N}(Z_p \times Z_p) = p + 1\,. \end{cases}$$

*Proof.* The previous proposition implies that $G$ has a subgroup consisting of the elements of order $p$, and that not all elements in it commute. We find that this subgroup, let us call it $H$, is nonabelian, and since there is only one nonabelian group

of order $\leq p^3$, we conclude that $H \cong ((Z_p \times Z_p) \rtimes Z_p)$. There are only $p^3 - 1$ elements of order $p$ however, so

$$\mathcal{N}((Z_p \times Z_p) \times Z_p) = 0\,.$$

Every smaller subgroup consisting of elements of order $p$ must be a subgroup of $H$, since it contains *all* the elements of order $p$. Proposition 2.2.11 gives the result. ⁒

**Lemma 2.3.48.** *For every $g \in G = (Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_3} Z_p$ of order $p^2$, it holds that $Z(G) < \langle g \rangle$.*

**Proposition 2.3.49.** *In $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_3} Z_p$ it holds that*

$$\mathcal{N}(Z_{p^2} \times Z_p) = 1\,.$$

*Proof.* This is following the line of the proof in the previous section.

Let $a = ((x, y, ), z), b = ((p\alpha', y'), z')$. We get that

$$ba = ((x + p\alpha' + \frac{pdz'(z'-1)x}{2} + \frac{pz'x(x-1)}{2} + pdz'y + py'x, y + y + z'x), z + z')$$

and also

$$ab = ((x + p\alpha' + pdzy', y + y'), z + z')\,.$$

Equality in the second component can only hold if $z' = 0$. The condition for equality in the first component is then reduced to $y'(x - dz) \equiv 0 \pmod{p}$, but we cannot allow $y' = 0$ since that would imply $\langle b \rangle < \langle a \rangle$. The condition becomes $x \equiv dz \pmod{p}$. We have $p$ choices for $\alpha'$ and $p - 1$ choices for $y'$. We have solved the problem of coinciding generators, so the only restriction for $a$ is $x \equiv dz \pmod{p}$. That leaves us with $p^2 - p$ choices for $x$ and $p$ choices for $y$. $z$ will be determined by the choice of $x$. In total: $p^2(p-1) \cdot p(p-1)$. The result then follows:

$$\mathcal{N}(Z_{p^2} \times Z_p) = \frac{p^3(p-1)^2}{p^3(p-1)^2} = 1\,.$$

⁒

**Proposition 2.3.50.** *In $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_3} Z_p$ it holds that*

$$\mathcal{N}(Z_{p^2} \rtimes Z_p) = p - 1\,.$$

*Proof.* Let $a = ((x, y), z), b = ((p\alpha', y'), z')$. We want them to satisfy $ba = a^{1+p}b$, so we calculate

$$ba = ((x + p\alpha' + \frac{pdz'(z'-1)x}{2} + \frac{pz'x(x-1)}{2} + pdz'y + py'x, y + y' + z'x), z + z')$$

and

$$a^{1+p}b = ((x+px,y),z)((p\alpha',y'),z') = ((x+p\alpha'+px+pdzy',y+y'),z+z')\,.$$

The condition for the second component is then that $z'x \equiv 0 \pmod{p}$. $x \not\equiv 0 \pmod{p} \Rightarrow z' = 0$. The condition for the first component is then reduced to

$$y'x \equiv x + dzy' \pmod{p}\,.$$

We see that we must have $y' \not\equiv 0 \pmod{p}$. That leaves us with $p$ choices for $\alpha'$ and $p-1$ choices for $y'$. $\langle a\rangle$ and $\langle b\rangle$ can never coincide, so we can choose $a$ with $y'x \equiv x+dzy' \pmod{p}$ as the only restriction. We get $p^2-p$ choices for $x$ and $p$ choices for $y$. Now $z$ is fully determined by the condition. In total we have $(p^2-p)p\cdot p(p-1)$ choices for $a$ and $b$. We conclude that

$$\mathcal{N}(Z_{p^2} \rtimes Z_p) = \frac{p^3(p-1)^2}{p^3(p-1)} = p-1\,.$$

In summary for $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_3} Z_p$:

$$\begin{cases} n_4 = 0 \\ n_3 = 0 \\ n_2 = p^4 - p^3 \\ n_1 = p^3 - 1 \\ \mathcal{N}(Z_p) = p^2+p+1 \\ \mathcal{N}(Z_{p^2}) = p^2 \\ \mathcal{N}(Z_p \times Z_p) = p+1 \\ \mathcal{N}(Z_{p^3}) = 0 \\ \mathcal{N}(Z_{p^2} \times Z_p) = 1 \\ \mathcal{N}(Z_p \times Z_p \times Z_p) = 0 \\ \mathcal{N}(Z_{p^2} \rtimes Z_p) = p-1 \\ \mathcal{N}((Z_p \times Z_p) \rtimes Z_p) = 1\,. \end{cases}$$

*Observation.* There is no difference in structure between group (xii) and (xiii) that I have found.

### 2.3.11 (xiv) $((Z_p \times Z_p) \rtimes Z_p) \times Z_p$

In the previous chapter, it was shown that this group is isomorphic with

$$\langle a,b,c,d : a^p = b^p = c^p = d^p = 1, dc = acd, bd = db, ad = da, bc = cb, ac = ca, ab = ba\rangle$$

with operation

$$(((x,y),z),w)(((x',y'),z'),w') = (((x+x,y+y'+zx'),z+z'),w+w')\,.$$

All components are modulo $p$.

**Lemma 2.3.51.** *For $g = (((x,y),z),w) \in ((Z_p \times Z_p) \rtimes Z_p) \times Z_p$ with the operation above, it holds that*

$$g^n = (((nx, ny + \frac{n(n-1)xz}{2}), nz), nw)\,.$$

*Proof.* Proof by induction. It holds for $g^1 = (((x,y),z),w)$. Assume that it holds for $g^n$.

$$\begin{aligned}
g^{n+1} &= g^n g \\
&= (((nx, ny + \frac{n(n-1)xz}{2}), nz), nw)(((x,y),z),w) \\
&= (((nx+x, ny + \frac{n(n-1)xz}{2} + y + (nz)x), nz+z), nw+w) \\
&= ((((n+1)x, (n+1)y + \frac{(n^2-n)xz}{2} + \frac{2nxz)}{2}, (n+1)z), (n+1)w) \\
&= ((((n+1)x, (n+1)y + \frac{(n+1)nxz}{2}), (n+1)z), (n+1)w)
\end{aligned}$$

The result follows by induction. ⨳

**Proposition 2.3.52.** *For $((Z_p \times Z_p) \rtimes Z_p) \times Z_p$ it holds that*

$$n_1 = p^4 - 1\,.$$

*Proof.* For any $g \in G$ we have $g^p = (((0,0),0),0)$. ⨳

**Proposition 2.3.53.** *The center of $G = ((Z_p \times Z_p) \rtimes Z_p) \times Z_p$ with the operation defined above is*

$$Z(G) = \langle (((0,1),0),0), (((0,0),0),1) \rangle \cong Z_p \times Z_p\,.$$

*Proof.* By inspection of the operation, we see that the condition for commuting is $xz' = x'z$. If we let $g' = (((x',y'),z'),w')$ be arbitrary, we see that we must have $x = z = 0$. The elements commuting with all other elements are thus on the form $(((0,y),0),w)$. The result follows immediately. ⨳

**Proposition 2.3.54.** *For any $g \in G = ((Z_p \times Z_p) \rtimes Z_p) \times Z_p$ (with the operation defined above) such that $g \notin Z(G)$,*

$$C(g) = Z(G) \times \langle g \rangle \cong Z_p \times Z_p \times Z_p\,.$$

*Proof.* By definition, this arbitrary $g$ commutes with all elements in $Z(G)$. $g$ can however not commute with any other elements than the elements in $Z(G)$ and $\langle g \rangle$, because then $|C(g)| > p^3$. That would force $|C(g)| = p^4$, but by assumption $g \notin Z(G)$ so we reach a contradiction.

$g$ also commutes with its powers, so $|C(g)| > p^2$, completing the proof. ⨳

This means that elements not lying in the center commute with $p^3$ elements.
From Corollary 2.1.8 and Corollary 2.1.6:

$$\begin{cases} \mathcal{N}(Z_p) = p^3 + p^2 + p + 1 \\ \mathcal{N}(Z_{p^2}) = \mathcal{N}(Z_{p^3}) = 0 \\ \mathcal{N}(Z_{p^2} \times Z_p) = \mathcal{N}(Z_{p^2} \rtimes Z_p) = 0\,. \end{cases}$$

In summary for $((Z_p \times Z_p) \rtimes Z_p) \times Z_p$:

$$\begin{cases} n_1 = p^4 - 1 \\ \mathcal{N}(Z_p) = p^3 + p^2 + p + 1 \\ \mathcal{N}(Z_{p^2}) = 0 \\ \mathcal{N}(Z_{p^3}) = 0 \\ \mathcal{N}(Z_{p^2} \times Z_p) = 0 \\ \mathcal{N}(Z_{p^2} \rtimes Z_p) = 0\,. \end{cases}$$

*Observation.* It remains to determine $\mathcal{N}(Z_p \times Z_p)$, $\mathcal{N}(Z_p \times Z_p \times Z_p)$ and $\mathcal{N}((Z_p \times Z_p) \rtimes Z_p)$ for this group.

### 2.3.12 (xv) $(Z_p \times Z_p \times Z_p) \rtimes Z_p$, $p > 3$

Again, it is crucial that $p > 3$ for the results to hold.

This group is isomorphic with

$$\langle a, b, c, d : a^p = b^p = c^p = d^p = 1, ba = ab, ca = ac, da = ad, cb = bc, db = abd, dc = bcd \rangle$$

with operation

$$((x, y, z), w)((x', y', z'), w') = ((x + x' + wy' + \frac{w(w-1)z'}{2}, y + y' + wz', z + z'), w + w')$$

and all components modulo $p$.

**Lemma 2.3.55.** *For $g = (((x, y), z), w) \in (Z_p \times Z_p \times Z_p) \rtimes Z_p$ with the operation above, it holds that*

$$g^n = ((nx + \frac{n(n-1)yw}{2} + \frac{n(n-1)w(w-1)z}{4} + \frac{n(n-1)(n-2)(zw^2}{6}, ny + \frac{n(n-1)zw}{2}, nz), nw)$$

*Proof.* I omit the proof for brevity. There is no essential difference to this proof and the similar ones that I have already done for the other groups. ⧖

**Proposition 2.3.56.** *For $(Z_p \times Z_p \times Z_p) \rtimes Z_p$ it holds that*

$$n_1 = p^4 - 1\,.$$

*Proof.* A quick calculation shows that

$$\begin{aligned} g^p = &\ ((px + \tfrac{p(p-1)yw}{2} + \tfrac{p(p-1)w(w-1)z}{4} + \tfrac{p(p-1)(p-2)zw^2}{6}, py + \tfrac{p(p-1)zw}{2}, pz), pw) \\ = &\ ((0,0,0),0)\,. \end{aligned}$$

⧖

**Proposition 2.3.57.** *The center of $(Z_p \times Z_p \times Z_p) \rtimes Z_p$ with $p > 3$ and the operation defined above is*

$$Z(G) = \langle((1,0,0),0)\rangle \cong Z_p\,.$$

*Proof.* By looking at the operation, we see that

$$gg' = g'g \Leftrightarrow \begin{cases} wz' = w'z \\ wy' + \frac{w(w-1)z'}{2} = w'y + \frac{w'(w'-1)z}{2} \end{cases}\,.$$

The first equation can only be satisfied for every $g' = ((x', y', z'), w') \in G$ if $w = z = 0$. The second equation becomes $w'y = 0$, which is only satisfied for arbitrary $w'$ if $y = 0$. ⧖

Note that you can see that $\langle((1,0,0),0)\rangle \leq Z(G)$ from the presentation.

From Corollary 2.1.8 and Corollary 2.1.6 we get

$$\mathcal{N}(Z_p) = p^3 + p^2 + p + 1$$

and

$$\mathcal{N}(Z_{p^2}) = \mathcal{N}(Z_{p^3}) = \mathcal{N}(Z_{p^2} \times Z_p) = \mathcal{N}(Z_{p^2} \rtimes Z_p) = 0\,.$$

In summary for $(Z_p \times Z_p \times Z_p) \rtimes Z_p$:

$$\begin{cases} n_1 = p^4 - 1 \\ \mathcal{N}(Z_p) = p^3 + p^2 + p + 1 \\ \mathcal{N}(Z_{p^2}) = 0 \\ \mathcal{N}(Z_{p^3}) = 0 \\ \mathcal{N}(Z_{p^2} \times Z_p) = 0 \\ \mathcal{N}(Z_{p^2} \rtimes Z_p) = 0\,. \end{cases}$$

*Observation.* It remains to determine $\mathcal{N}(Z_p \times Z_p)$, $\mathcal{N}(Z_p \times Z_p \times Z_p)$ and $\mathcal{N}((Z_p \times Z_p) \rtimes Z_p)$ for this group.

## 2.4 Starting points for further studies

Throughout this text we have seen that some results seem to hold for all $p$-groups (at least of low order with sufficiently big $p$). It thus seems plausible that a few general results hold. For example that the $n_i$ are independent of everything but $p$ and the factors of the semidirect product, at least for completely factorazible $p$-groups. This is a result that would most probably prove Conjecture 1.7.3.

Another thing we have noticed is that it seems like the product of elements of order $p$ is itself of order $p$. Again, it seems plausible that this holds for completely factorizable $p$-groups when $p$ is sufficiently big.

We also have a few natural starting points such as the study of the groups of order $p^5$ and higher and also the study of what exactly happens when $p = 2$ or $p = 3$ for the groups that collapse for these values of $p$.

In summary, here are some suggestions for starting points for further studies listed:

- Determine $\mathcal{N}(Z_p \times Z_p)$, $\mathcal{N}(Z_p \times Z_p \times Z_p)$ and $\mathcal{N}((Z_p \times Z_p) \rtimes Z_p)$ for the groups denoted (xiv) and (xv).
- For the further studies of the groups of order $p^n$ with $n > 4$ it is needed to determine $|\mathrm{Aut}(G)|$ for all the groups of order $p^4$.
- Continue with the study of the groups of order $p^5$.
- Examine what happens when $p = 2$ and $p = 3$ for the groups that break down for these values of $p$.
- A proof or rejecting of Conjecture 1.7.3 is of high importance.
- We saw that for all the groups of order $p^4$, (with $p > 3$ when needed) it is true that $a, b \in G$ of order $p$ implies $(ab)^p = 1$. Is this generally true? Will it hold for the groups of order $p^5$ when $p$ is big enough?
- Some of the groups studied suffer from clumsy operations and/or presentations. Finding alternatives might make some of the work more intuitive.

# Chapter 3

# Representations of $p$-groups

In this chapter we will look at $p$-groups using representation theory. We will study the irreducible characters of the non-abelian $p$-groups of order $p^3$ and $p^4$ and present their character tables. In the process of finding these characters the conjugacy classes of the groups will also be calculated. But first we will give an introduction to the theory which covers the basics and proves the theorems that will be used later.

## 3.1 Short introduction to representation theory

This introduction will follow ideas and proofs presented in the book *Linear representations of finite groups* written by Jean-Pierre Serre (see [8]).

### 3.1.1 Definitions and basics

A *representation* $\rho$ is defined as a homomorphism from a group $G$ into $\mathrm{GL}(V)$ where $V$ is a finite dimensional vector space over $\mathbb{C}$ and the *degree* of a representation is defined to be the dimension of the space $V$. We will use the notation $\rho_g$ to describe the linear map associated to $g$ by $\rho$.

Two representations, $(V, \rho)$ and $(W, \sigma)$, of the same group are called *isomorphic* if there exists a linear isomorphism from $V$ to $W$ with the property that $f \circ \rho_g = \sigma_g \circ f$ for any $g \in G$.

*Example* 3.1.1. Let $V$ be the vector space spanned by $(e_g)_{g \in G}$ and let $\rho$ act on the set of basis vectors as $\rho_h e_g = e_{hg}$. Then $\rho$ is a representation and it is called the *regular representation.*

These representations will usually be studied through their *subrepresentations* which are defined as a subspace $W$ of $V$ which is stable under the action of $\rho(g)$, that is we have

$$\rho(g)W \subseteq W \ \ \forall\, g \in G.$$

A representation which has no proper non-trivial subrepresentations will be called an *irreducible* representation and we have a theorem regarding decomposing representations.

**Theorem 3.1.2.** *Every representation can be written as a direct sum of irreducible representations.*

For the proof of this we will need the following lemma.

**Lemma 3.1.3.** *If $\rho : G \to \mathrm{GL}(V)$ is a representation, then for every subspace $W$ of $V$ stable under $G$ there exists a complement which also is stable under $G$.*

*Proof.* Here we will use a trick from Serre's book, see Theorem 1.1 in [8]. Let $p$ be the projection of $V$ onto $W$ and define

$$p^0 = \frac{1}{|G|} \sum_{g \in G} \rho_g \circ p \circ \rho_g^{-1},$$

which also is a projection onto $W$ since $\rho_g W \subseteq W$ for all $g \in G$, and thus has a complement $W^0$ in $V$. But we also have that $p^0 \circ \rho_g = \rho_g \circ p^0$ since

$$\begin{aligned} \rho_h \circ p^0 \circ \rho_h^{-1} &= \rho_h \circ (\frac{1}{|G|} \sum_{g \in G} \rho_g \circ p \circ \rho_g^{-1}) \circ \rho_h^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} \rho_h \circ \rho_g \circ p \circ \rho_g^{-1} \circ \rho_h^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} \rho_g \circ p \circ \rho_g^{-1} \\ &= p^0. \end{aligned}$$

Therefore if we take $x \in W^0$ we get $p^0 x = 0$ and $\rho_g \circ p^0 x = 0$ so we have $p^0 \circ \rho_g x = 0$ thus $\rho_g x \in W^0$ and

$$\rho_g W^0 \subseteq W^0$$

which shows that $W^0$ is stable under $G$. ⨳

*Proof of theorem 3.1.2.* Let $\rho : G \to \mathrm{GL}(V)$. We will show this using induction on the degree of the representation. If $n = 1$ then it is irreducible, so assume that the theorem is true for all degrees less than $n$. If the representation is irreducible there is nothing to prove, otherwise there exists a proper non-trivial subrepresentation which implies the existence of a subspace $W$ which is stable under $G$. Then by lemma 3.1.3 we get the existence of a complement such that $V = W \bigoplus W'$, that is we have $V$ as a direct sum of representations of degree strictly less than $n$ and so by induction we are done. ⨳

**Lemma 3.1.4** (Schur's lemma)**.** *Let $(V, \rho)$ and $(W, \sigma)$ be two irreducible representations of a group $G$. Let also $f : V \to W$ be a linear function with the property $f \circ \rho_g = \sigma_g \circ f$.*

*(i) If $V$ and $W$ are non-isomorphic then $f = 0$.*

*(ii) If $V$ and $W$ isomorphic then $f$ will be multiplication by a scalar.*

*Proof.* For *(i)* we observe that $f(V)$ is a subspace of $W$ since linear maps takes subspaces into subspaces. We observe that $f(V)$ is stable under $\sigma$ since for any $g \in G$

$$\sigma_g f(V) = (\sigma_g \circ f)(V) = (f \circ \rho_g)(V)$$

now we use that $\rho_g V \subseteq V$ and get $\sigma_g f(V) \subseteq f(V)$. Because of irreducibility we can conclude that either $f(V)$ is 0 or $W$, now assume that $f(V) = W$ but that would imply that $V$ and $W$ are isomorphic, thus $f = 0$.

To prove *(ii)* we assume that $V = W$ and $\rho = \sigma$, then there exists an eigenvalue $\lambda$. So let $f' = f - \lambda$ and note that $f' \circ \rho_g = \rho_g \circ f'$ since for $x \in V$ and $g \in G$

$$(f' \circ \rho_g)x = f'\rho_g x = f\rho_g x - \lambda\rho_g x = \rho_g f x - \rho_g \lambda x = (\rho_g \circ f')x.$$

But $\ker f'$ is a stable subspace under $\rho$ since for $x \in \ker f'$

$$f'(\rho_g x) = \rho_g(f'x) = \rho_g 0 = 0$$

and so $\rho_g \ker f' \subseteq \ker f'$. Note also that since $\lambda$ has at least one eigenvector we get $\ker f' \neq 0$. Therefore $\ker f' = V$ because $\rho$ is irreducible and thus $f = \lambda$. ⨳

### 3.1.2 Characters

If $\rho$ is a representation of $G$ then the *character* $\chi$ of $\rho$ (usually denoted $\chi_\rho$) is defined for $g \in G$ as

$$\chi_\rho(g) = \mathrm{Tr}(\rho(g))$$

where Tr is the trace. With a little abuse of language we will call a character of an irreducible representation an *irreducible character*.

**Theorem 3.1.5.** *If $\chi$ is the character of a representation $\rho$ of degree $n$ then $\chi$ has the following properties*

*(i)* $\chi(1) = n$

*(ii)* $\chi(hgh^{-1}) = \chi(g)\ \forall\ h, g \in G.$

*(iii)* $\chi(g^{-1}) = \overline{\chi(g)}\ \forall\ g \in G.$

*Proof.* Note that since $\rho$ is a homomorphism 1 must map to the identity element of $\mathrm{GL}(V)$ which is the identity matrix $I_n$ of size $n$. Then $\chi(1) = \mathrm{Tr}(I_n)$, but we have $\mathrm{Tr}(I_n) = n$ thus proving *(i)*.

The second property is trivial since we know that the trace is similarity invariant (see any book in linear algebra for proof).

The third property follows from the fact that eigenvalues of $\rho_g$ are roots of unity and the fact that the character $\chi(g)$ is the sum of the eigenvalues. We also note that if $\lambda$ is an eigenvalue of $\rho_g$ then $\lambda^{-1}$ is an eigenvalue of $\rho_{g^{-1}}$ and that $\overline{\lambda} = \lambda^{-1}$, then

$$\overline{\chi(g)} = \sum \overline{\lambda_i} = \sum \lambda_i^{-1} = \chi(g^{-1}).$$

⁂

Another valuable property of these characters is that they respect the direct product.

**Theorem 3.1.6.** *Let $(V, \rho)$ and $(W, \sigma)$ be two representations of $G$ and let also $\varphi$ and $\psi$ be their characters. Then the character $\chi$ of $V \oplus W$ is $\chi = \varphi + \psi$.*

See Proposition 2.2 in [8] for proof.

The second property of Theorem 3.1.5 can also be stated by saying that a function $f : G \to \mathbb{C}$ should be constant on the conjugacy classes of $G$ and such a function will be called a *class function*. If we consider the vector space of all class functions we can define an inner product as

$$(\varphi, \psi) = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\psi(g)}.$$

We now want to prove one of the most useful theorems regarding characters.

**Theorem 3.1.7** (The orthogonality relations)**.**

*(i) Let $\chi$ be a character of a representation $(V, \rho)$, then $\chi$ is irreducible if and only if $(\chi, \chi) = 1$.*

*(ii) If $\varphi$ and $\psi$ are characters of two non-isomorphic irreducible representations then $(\varphi, \psi) = 0$.*

The proof will be split up into three propositions and throughout their proofs we will use Corollary 2.1 from Serre's book, see [8].

**Lemma 3.1.8.** *Let $(V, \rho)$ and $(W, \sigma)$ be two irreducible representations of a group $G$ and let $h : V \to W$ be linear and define*

$$h^0 = \frac{1}{|G|} \sum_{t \in G} \sigma_t^{-1} h \rho_t.$$

*Then*

*(i) if $\rho$ and $\sigma$ are non-isomorphic then $h^0 = 0$*

*(ii) if $V = W$ and $\rho = \sigma$ then $h^0 = \frac{1}{n}\mathrm{Tr}(h)$, where $n = \dim V$.*

*Proof.* Note that for any $s \in G$ $h^0 \circ \rho_s = \sigma_s \circ h^0$ since

$$\begin{aligned}\sigma_s^{-1} \circ h^0 \circ \rho_s &= \frac{1}{|G|}\sum_{t\in G} \sigma_s^{-1}\sigma_t^{-1} h \rho_t \rho_s \\ &= \frac{1}{|G|}\sum_{t\in G} \sigma_{(ts)^{-1}} h \rho_{ts} \\ &= h^0.\end{aligned}$$

Now we can use Schur's lemma 3.1.4 and get for *(i)* that $h^0 = 0$ since $h = 0$. For *(ii)* we get that $h^0 = \lambda$ and since

$$\mathrm{Tr}(h^0) = \frac{1}{|G|}\sum_{t\in G} \mathrm{Tr}(\sigma_t^{-1} h \rho_t) = \mathrm{Tr}(h)$$

and since $\mathrm{Tr}(\lambda) = n\lambda$ we conclude that $h^0 = \frac{1}{n}\mathrm{Tr}(h)$. ⨵

**Proposition 3.1.9.** *Let $\chi$ be a character of a representation $(V, \rho)$, then $(\chi, \chi) = 1$ if $\chi$ is irreducible.*

*Proof.* Let $\chi$ be given in matrix-from by $\rho_g = (r_{ij}(g))$. Then $\chi(g) = \sum r_{ii}(g)$ and

$$(\chi, \chi) = \frac{1}{|G|}\sum_{g\in G} \chi(g)\overline{\chi(g)} = \frac{1}{|G|}\sum_{g\in G, i', j'} r_{i'i'}(g) r_{j'j'}(g^{-1}).$$

Now we redefine $h^0$ from Lemma 3.1.8 to be in matrix-form given by $(h^0_{ij})$, with $h = (h_{ij}), \rho_g = (r_{ij}(g))$ and $\sigma_g = (s_{ij}(g))$ we get

$$h^0_{ij} = \frac{1}{|G|}\sum_{t, i', j'} s_{ii'}(t^{-1}) h_{i'j'} r_{j'j}(t).$$

If we then apply *(ii)* of the lemma to $\rho_g$ we get that

$$h^0 = \frac{1}{n}\mathrm{Tr}(h)$$

and in matrix-form this is

$$h^0_{ij} = \frac{\delta_{ij}}{n}\sum_{i', j'} \delta_{i'j'} h_{i'j'}.$$

When we equate these expressions we get

$$\frac{1}{|G|}\sum_{t,i',j'} s_{ii'}(t^{-1})h_{i'j'}r_{j'j}(t) = \frac{\delta_{ij}}{n}\sum_{i',j'}\delta_{i'j'}h_{i'j'}$$

which is a system relating coefficients of $h_{ij}$ thus we can express them separately as

$$\frac{1}{|G|}\sum_{t} s_{ii'}(t^{-1})r_{j'j}(t) = \frac{1}{n}\delta_{ij}\delta_{i'j'}.$$

Now apply this last formula with $s_{ij} = r_{ij}$

$$\frac{1}{|G|}\sum_{t} r_{ii'}(t^{-1})r_{j'j}(t) = \frac{1}{n}\delta_{ij}\delta_{i'j'}$$

and so we can continue to calculate $(\chi, \chi)$

$$\begin{aligned}(\chi,\chi) &= \frac{1}{|G|}\sum_{g\in G,i',j'} r_{i'i'}(g)r_{j'j'}(g^{-1}) \\ &= \frac{1}{n}\sum_{i',j'}\delta_{i'j'}\delta_{i'j'} \\ &= 1.\end{aligned}$$

⁒

**Proposition 3.1.10.** *If $\varphi$ and $\psi$ are characters of two non-isomorphic irreducible representations then $(\varphi, \psi) = 0$.*

*Proof.* Let $\rho_g = (r_{ij}(g))$ and $\sigma_g = (s_{ij}(g))$ be the irreducible representations with characters $\varphi$ and $\psi$.

We again use $h^0$ from Lemma 3.1.8 in matrix-form as

$$h^0_{ij} = \frac{1}{|G|}\sum_{t,i',j'} s_{ii'}(t^{-1})h_{i'j'}r_{j'j}(t)$$

but this time the lemma gives that $h^0_{ij} = 0$ for our non-isomorphic representations and hence gives the system of equations

$$\frac{1}{|G|}\sum_{t} s_{ii'}(t^{-1})r_{j'j}(t) = 0.$$

When we then calculate $(\varphi, \psi)$ we get

$$(\varphi,\psi) = \frac{1}{|G|}\sum_{g\in G,i',j'} r_{i'i'}(g)s_{j'j'}(g^{-1}) = 0.$$

⁒

**Proposition 3.1.11.** *Let $\chi$ be a character of a representation $(V, \rho)$, then $\chi$ is irreducible if $(\chi, \chi) = 1$.*

*Proof.* We use Theorem 3.1.2 and write the representation $V$ as a direct sum of irreducible representations $W_i$

$$V = \bigoplus_i m_i W_i,$$

where $m_i$ is the multiplicity and $W_i$ is non-isomorphic to $W_j$ if $i \neq j$. But then it is clear from Theorem 3.1.6 that $\chi = \sum_i \chi_i$ where $\chi_i$ is the characters of $W_i$, so that

$$(\chi, \chi) = (\sum_i \chi_i, \sum_j \chi_j) = \sum_{i,j} (\chi_i, \chi_j) = \sum m_k^2.$$

The assumption $(\chi, \chi) = 1$ then gives that the $\chi$ must be irreducible since the multiplicities $m_k$ are a positive integers. ⨳

And thus we are done with the proof of Theorem 3.1.7.

We now turn our attention to the space of class functions on $G$ and we will prove that it has a basis related to the irreducible characters and its dimension is related to the conjugacy classes of $G$.

**Theorem 3.1.12.** *The characters of the irreducible representations of $G$ form an orthonormal basis for the space of class functions on $G$.*

*Proof.* Again the discussion will follow a proof by Serre (see Theorem 2.6 in [8]).

It is already clear that the irreducible characters $\chi_1, \ldots, \chi_h$ form a orthonormal set, so we only need to show that they span the space of class functions on $G$. So assume that we have a class function $f$ that is orthogonal to $\chi_i$ and thus outside the span of the characters.

We intend to show that $f = 0$ by applying Schur's lemma 3.1.4 to the function $\rho_f$ defined for any irreducible representation $\rho : G \to \mathrm{GL}(V)$ by

$$\rho_f = \sum_{g \in G} f(g) \rho_g.$$

Then $\rho_f$ is a linear function from $V$ to $V$, and for any $h \in G$

$$\begin{aligned} \rho_h^{-1} \rho_f \rho_h &= \sum_{g \in G} f(g) \rho_{h^{-1}} \rho_g \rho_h \\ &= \sum_{u = h^{-1} g h \in G} f(huh^{-1}) \rho_u \\ &= \sum_{u \in G} f(u) \rho_u \\ &= \rho_f \end{aligned}$$

and so we have satisfied the assumptions of Schur's lemma and get that $\rho_f = \lambda$. So we take the trace of this equality and get

$$n\lambda = \mathrm{Tr}(\rho_f) = \sum_{g\in G} f(g)\mathrm{Tr}(\rho_g) = \sum_{g\in G} f(g)\chi(g) = g(f,\chi)$$

but since $f$ is orthogonal to all the irreducible characters we get that $(f,\chi) = 0$ and thus $\lambda = 0$. We conclude that $\rho_f = 0$ for all irreducible representations, but we can always decompose a reducible representation and thus $\rho_f = 0$ for any representation.

Now choose the regular representation (see Example 3.1.1) and look at how $\rho_f$ acts on $e_1$

$$\rho_f e_1 = \sum_{g\in G} f(g)\rho_g e_1 = \sum_{g\in G} f(g)e_g$$

but $\rho_f = 0$ which implies $\sum_{g\in G} f(g)e_g = 0$ which means that $f(g) = 0$ for all $g$. So we conclude $f = 0$ which is what we wanted to show. ⧖

**Theorem 3.1.13.** *The numbers of irreducible characters are the same as the number of conjugacy classes of $G$.*

*Proof.* The class functions are determined by their values on the conjugacy classes of $G$ thus as a complex vector space they have a dimension equal to the number of classes. But we showed in the previous theorem that the irreducible characters form a basis for the same vector space, thus the number of classes and number of irreducible characters are the same. ⧖

We also have a restriction on the degrees of the irreducible representations and how they relate to the size of $G$.

**Theorem 3.1.14.** *Let $n_i$ be the degrees of the irreducible representations of $G$ then*

$$|G| = \sum_i n_i^2.$$

*Proof.* We make use of the regular representation from Example 3.1.1 and note that if we let $r$ be its character then $r(1) = |G|$ and $r(g) = 0$ if $g \neq 1$ since $\rho_g e_i \neq e_i$ if $g \neq 1$.

Now if we expand the character $r$ as a linear combination of the irreducible characters, $r(g) = \sum (r,\chi_i)\chi_i(g)$, we get the coefficients as

$$(r,\chi_i) = \frac{1}{|G|}\sum_{g\in G} r(g)\overline{\chi_i(g)} = \frac{|G|}{|G|}\overline{\chi_i(1)} = n_i$$

where $n_i$ is the degree of the character $\chi_i$. If we then evaluate $r(1)$ we get that

$$r(1) = \sum_i (r,\chi_i)\chi_i(1) = \sum_i n_i^2$$

but $r(1) = |G|$ and we are done. ⧖

### 3.1.3 Induced representations

Let $H \leq G$ and let $\theta : H \to \mathrm{GL}(W)$ be a representation of $H$. Let also $R$ be the set of representatives of the left cosets of $H$ in $G$. We say that a representation $\rho : G \to \mathrm{GL}(V)$ is *induced* from the representation $\theta$ of $H$ if we can write $V$ as a direct sum of copies of $W$, that is

$$V = \bigoplus_{r \in R} \rho_r W.$$

One can think of this representation as letting $\theta$ act on $W$ and identifying $\theta$ with the restriction of $\rho_H$ to $H$. In that case the subspace $W$ becomes stable under $\rho$ and thus the spaces $\rho_s W$ will also be stable under $H$ and only depends on the coset to which $s$ belongs. Then the action of $G$ on this set of subspaces $\rho_r W$ will be the same as that of the action of $G$ on the set of cosets.

We cannot a priori assume the existence and uniqueness of this representation (at least not if we define it this way, see chapter 16 in [2] for another definition using group algebras and tensor products), this is proved in Theorem 11 in [8].

If we know the character of $\theta$ we can compute the character of the induced representation $\rho$ as in Theorem 12 in [8]

**Theorem 3.1.15.**

$$\chi_\rho(g) = \frac{1}{|H|} \sum_{t \in G, t^{-1}gt \in H} \chi_\theta(t^{-1}gt).$$

**Corollary 3.1.16.**

$$\chi_\rho(1) = |G : H| \chi_\theta(1)$$

*Proof.* Just evaluate the formula in the previous theorem for 1

$$\chi_\rho(1) = \frac{1}{|H|} \sum_{t \in G, t^{-1}1t \in H} \chi_\theta(t^{-1}1t) = \frac{1}{|H|} \sum_{t \in G} \chi_\theta(1) = |G : H| \chi_\theta(1).$$

⁂

## 3.2 Preliminaries

We will need to know the representations of some small abelian $p$-groups, namely those of $Z_p$ and $Z_p \times Z_p$. To find these we will use the following theorem.

**Theorem 3.2.1.** *If $G$ is an abelian group then every irreducible representation will be of degree 1 and the converse is also true.*

*Proof.* Since $G$ is abelian we know that it has $|G|$ conjugacy classes. Which by Theorem 3.1.13 is gives that $G$ has $|G|$ irreducible characters, but we also have by Theorem 3.1.14 that

$$|G| = n_1^2 + \ldots + n_{|G|}^2,$$

which clearly only can be satisfied when $n_i = 1$ for all $i$. The converse is clear from Theorem 3.1.13. ⨳

### 3.2.1 Characters of $Z_p$

We proceed as in Example 5.1 in [8] and begin by noting that since $Z_p$ is abelian every irreducible representation will be of degree 1 (Theorem 3.2.1). Thus the characters of these representations will be of the type $\chi(g) = w$ for some $w \in \mathbb{C}$. Noting that $g^p = 1$ we see that $w^p = 1$, so $w$ is a $p$-th root of unity, that is $w = e^{\frac{2\pi i}{p}\alpha}$ for $\alpha = 0, \ldots, p-1$. Thus we get the irreducible characters defined for $x \in Z_p$

$$\chi_\alpha(x) = e^{\frac{2\pi i}{p}\alpha x}.$$

### 3.2.2 Characters of $Z_p \times Z_p$

This is treated in Example 15.2 in [2] as follows.

We first observe that the conjugacy classes of a direct product is the product of a class in each of the factors, thus we have in our case $p^2$ conjugacy classes. This can be shown as in the example in [2] by noting that an element $(x, y)$ in a direct product is conjugate to $(x', y')$ if and only if $x$ and $x'$ are conjugate and likewise for $y$ and $y'$.

We make the assumption that the characters will be

$$\tau_{\alpha\beta}(x, y) = \chi_\alpha(x)\chi_\beta(y)$$

where $\chi_\alpha$ and $\chi_\beta$ are irreducible characters of $Z_p$. We now want to verify that these functions indeed are $p^2$ irreducible characters by using Theorem 3.1.7. Then by Theorem 3.1.13 we know that there are no other irreducible characters and we are

done.

$$\begin{aligned}
(\tau_{\alpha\beta}, \tau_{\alpha'\beta'}) &= \frac{1}{|G|}\sum_{g\in G}\tau_{\alpha\beta}(g)\overline{\tau_{\alpha'\beta'}(g)} \\
&= \frac{1}{p^2}\sum_{x,y\in Z_p}\chi_\alpha(x)\chi_\beta(y)\overline{\chi_{\alpha'}(x)\chi_{\beta'}(y)} \\
&= \frac{1}{p^2}\sum_{x,y\in Z_p} e^{\frac{2\pi i}{p}\alpha x} e^{\frac{2\pi i}{p}\beta y} e^{-\frac{2\pi i}{p}\alpha' x} e^{-\frac{2\pi i}{p}\beta' y} \\
&= \frac{1}{p^2}\sum_{x\in Z_p} e^{\frac{2\pi i}{p}(\alpha-\alpha')x}\sum_{y\in Z_p} e^{\frac{2\pi i}{p}(\beta-\beta')y} \\
&= \frac{1}{p^2} p\delta_{\alpha\alpha'} p\delta_{\beta\beta'} \\
&= \delta_{\alpha\alpha'}\delta_{\beta\beta'}
\end{aligned}$$

Here we have used that the sum over all the $p$-th roots of unity is zero and thus we have found all of the characters.

## 3.3 Characters of $p$-groups of order $p^3$

Throughout this section $\lambda$ will denote an arbitrary non-trivial $p$-th root of unity.

### 3.3.1 Characters of $(Z_p \times Z_p) \rtimes Z_p$

Let $G = (Z_p \times Z_p) \rtimes Z_p$. To motivate our search for the the irreducible characters we make use of Theorem 16 in [8] which is stated to hold for supersolvable groups, but since $p$-groups are supersolvable we can state the theorem as

**Theorem 3.3.1.** *Let $G$ be a $p$-group. Then each irreducible representation of $G$ is induced by a representation of degree 1 of a subgroup of $G$.*

So since we know the irreducible characters of both $Z_p$ and $Z_p \times Z_p$ we can look at the induced characters of these subgroups, but we are only interested in the case $Z_p \times Z_p$ since the degree of an induced representation is related to $H$ as in Corollary 3.1.16 and so we want $|G : H| = p$.

To continue we need to find the conjugacy classes of $G$, and this is done best by considering the matrix presentation of $G$ which is introduced in Example 1.4.7. So if we have $g = ((x, y), z) \in G$, it was shown that $g$ is equivalent to the matrix

$$\begin{pmatrix} 1 & z & y \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix},$$

and that multiplication in $G$ is with this presentation just matrix multiplication which gives the formula

$$((x,y),z)) * ((x',y'),z') = ((x+x', y+y'+x'z), z+z').$$

So now it is not hard to find the conjugates of $g$ by $h$, let $h = ((u,v),w)$ so we have that $h^{-1}gh$ is

$$\begin{pmatrix} 1 & -w & wu-v \\ 0 & 1 & -u \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & z & y \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & w & v \\ 0 & 1 & u \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & z & y+zu-xw \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}.$$

If not both $x$ and $z$ are zero we see that we get $p$ conjugates and if $x = z = 0$ we see that $g$ is in the center of $G$. And so we can conclude that the representatives of the non-trivial conjugacy classes are $((x,0),z)$ and that we have $p^2 - 1$ different classes of this type. We also get that $Z(G) = \{((0,y),0) \mid y \in Z_p\}$.

**Induced characters of $(Z_p \times Z_p) \rtimes Z_p$ by $Z_p \times Z_p$**

Let $G = (Z_p \times Z_p) \rtimes Z_p$ and $H = \{((x,y),0)\} \cong Z_p \times Z_p$ so that $|G : H| = p$. To calculate the induced characters $\chi$ we use Theorem 3.1.15 and let $\tau_{\varepsilon\zeta}(x,y) = \lambda^{\varepsilon x}\lambda^{\zeta y}$ be the characters of $H$, then

$$\chi((x,y),z) = \frac{1}{|H|} \sum_{t \in G, t^{-1}gt \in H} \tau_{\varepsilon\zeta}(t^{-1}gt).$$

With the definition of $H$ we get that

$$\chi((x,y),z) = \frac{1}{p^2} \sum_{\substack{((u,v),w) \in G \\ ((x,y+zu-xw),z) \in H}} \lambda^{\varepsilon x}\lambda^{\zeta(y+zu-xw)},$$

but since $H$ is of the form $\{((x,y),0)\}$ we see that $\chi = 0$ if $z \neq 0$ and note also that the summand does not depend on $v$, thus

$$\chi((x,y),0) = \frac{p^2}{p^2} \sum_w \lambda^{\varepsilon x}\lambda^{\zeta(y-xw)} = \lambda^{\varepsilon x}\lambda^{\zeta y} \sum_w \lambda^{-\zeta w x}.$$

The sum $\sum_w \lambda^{-\zeta x w}$ is a sum of all roots of unity and will vanish when $\zeta x \neq 0$, but $\zeta$ is arbitrary and this implies that $\chi$ vanishes whenever $x \neq 0$. Note now that $\chi(g)$ is zero whenever $g \notin Z(G)$, so we finally have our induced character $\chi$ which takes its non-zero values on the center as

$$\chi_\zeta((0,y),0) = p\lambda^{\zeta y}.$$

We also want to verify that these characters are irreducible by calculating

$$\begin{aligned}(\chi_\zeta, \chi_{\zeta'}) &= \frac{1}{|G|}\sum_{g\in G}\chi_\zeta(g)\overline{\chi_{\zeta'}(g)} \\ &= \frac{1}{p^3}\sum_y p\lambda^{\zeta y}p\lambda^{-\zeta' y} \\ &= \frac{p^2}{p^3}\sum_y \lambda^{(\zeta-\zeta')y} \\ &= \delta_{\zeta\zeta'}\end{aligned}$$

where the last equality is again due to the fact that we sum over all roots of unity and so if we use Theorem 3.1.7 we get that $\chi_\zeta$ are irreducible, non-isomorphic to each other and has degree $p$.

**Lifting characters from $Z_p \times Z_p$**

To find the rest of the characters we use the method of lifting characters from an abelian subgroup $G$ with a homomorphism which also is a class function.

Let $\eta : (Z_p \times Z_p) \rtimes Z_p \to Z_p \times Z_p$ by $((x, y), z) \mapsto (x, z)$, observe that this is a homomorphism. Then $\varphi_{\alpha\beta} = \tau_{\alpha\beta} \circ \eta$ is a class function, and I intend to show that these are irreducible characters. To do this we look at the inner product

$$\begin{aligned}(\varphi_{\alpha\beta}, \varphi_{\alpha'\beta'}) &= \frac{1}{|G|}\sum_{g\in G}\tau_{\alpha\beta}(\eta(g))\overline{\tau_{\alpha'\beta'}(\eta(g))} \\ &= \frac{1}{p^3}\sum_{x,y,z}\lambda^{(\alpha x+\beta z)}\lambda^{-(\alpha' x+\beta' z)} \\ &= \frac{p}{p^3}\sum_x \lambda^{(\alpha-\alpha')x}\sum_z \lambda^{(\beta-\beta')z},\end{aligned}$$

and since each of these sums are zero if (for the first sum) $\alpha \neq \alpha'$ and $p$ if $\alpha = \alpha'$ (and likewise for the second) we see that

$$(\varphi_{\alpha\beta}, \varphi_{\alpha'\beta'}) = \delta_{\alpha\alpha'}\delta_{\beta\beta'},$$

which implies that $\varphi_{\alpha\beta}$ are irreducible characters (again by Theorem 3.1.7).

Since $\varphi_{\alpha\beta}((0,0),0) = \tau_{\alpha\beta}(\eta((0,0),0)) = \lambda^{(\alpha\cdot 0+\beta\cdot 0)} = 1$ we see that all of these characters has degree 1 and that $\varphi_{00}$ is the principal character.

**Character table**

We have found two orthogonal sets of irreducible characters but we still need to verify that they are non-isomorphic to each other.

$$\begin{aligned}(\chi_\zeta, \varphi_{\alpha\beta}) &= \frac{1}{|G|}\sum_{g\in G}\chi_\zeta(g)\overline{\varphi_{\alpha\beta}(g)} \\ &= \frac{1}{p^3}\sum_{((x,y),z)\in Z(G)} p\lambda^{\zeta y}\lambda^{-\alpha x}\lambda^{-\beta z} \\ &= \frac{p}{p^3}\sum_{y}\lambda^{\zeta y}\end{aligned}$$

We see that if $\zeta \neq 0$ then we get $(\chi_\zeta, \varphi_{\alpha\beta}) = 0$ which is what we needed to prove that the characters are orthogonal. Thus we have found $p^2$ characters of degree 1 and $p-1$ characters of degree $p$, thus by Theorem 3.1.13 we have found all irreducible characters.

Let $((0,y),0)$ be the elements in $Z(G)$ and let $((x,0),z)$ be the representatives of the non-trivial conjugacy classes. Assume further that $\alpha, \beta, \zeta \in Z_p$ and also that $\zeta \neq 0$, then we get the character table as

| | $((0,y),0)$ | $((x,0),y)$ |
|---|---|---|
| $\varphi_{\alpha\beta}$ | $1$ | $\lambda^{\alpha x+\beta z}$ |
| $\chi_\zeta$ | $p\lambda^{\zeta y}$ | $0$ |

Observe that we can identify the principal character as $\varphi_{00}$.

### 3.3.2 Characters of $Z_{p^2} \rtimes Z_p$

Let $G = Z_{p^2} \rtimes Z_p$ with the group action as

$$(x,y) * (x',y') = (x + x' + px'y, y + y').$$

From Example 1.4.8 it is clear that any element $g = (x,y)$ can be written as

$$\begin{pmatrix} 1+py & x \\ 0 & 1 \end{pmatrix}.$$

Using this we find the formula for $g^{-1} = (x,y)^{-1}$ as

$$(x,y)^{-1} = (-x(1-py), -y),$$

from which we can determine the conjugacy classes of $G$. Let $g = (x,y)$, then its conjugates are of the form

$$(u,v)^{-1} * (x,y) * (u,v) = (x + p(yu - xv), y).$$

To find the center of $G$ we look for elements such that

$$(u,v)^{-1} * (x,y) * (u,v) = (x,y),$$

and is satisfied by, for example, the elements of the type $(pr, 0)$ for $r \in Z_p$. There are $p$ such elements and they form a subgroup of $G$ isomorphic to $Z_p$ and thus $Z(G) = \{(pr,0) \mid r \in Z_p\}$.

The representatives of the non-trivial conjugacy classes are $(x,y)$ where we count both coordinates modulo $p$. So there are $p^2 - 1$ non-trivial classes because the choice $(0,0)$ will lie in $Z(G)$, and thus we have a total of $p^2 + p - 1$ classes.

**Lifting characters from $Z_p \times Z_p$**

Define $\eta : G \to Z_p \times Z_p$ as $(x,y) \mapsto (x \mod p, y)$, this defines a homomorphism which is also constant on the conjugacy classes of $G$. So let $\varphi_{\alpha\beta} = \tau_{\alpha\beta} \circ \eta$, and verify that they form an orthonormal set of irreducible characters

$$(\varphi_{\alpha\beta}, \varphi_{\alpha'\beta'}) = \frac{1}{p^3} \sum_{x,y} \tau_{\alpha\beta}(\eta(z,y)) \overline{\tau_{\alpha'\beta'}(\eta(z,y))}.$$

Now since $\eta$ counts modulo $p$ in the first coordinate we get, with $x' = x \mod p$

$$\begin{aligned}
(\varphi_{\alpha\beta}, \varphi_{\alpha'\beta'}) &= \frac{p}{p^3} \sum_{x',y} \tau_{\alpha\beta}(x'y) \overline{\tau_{\alpha'\beta'}(x',y)} \\
&= \frac{1}{p^3} \sum_{x'y} \lambda^{(\alpha x' + \beta y)} \lambda^{-(\alpha' x' + \beta' y)} \\
&= \frac{1}{p^2} \sum_{x'} \lambda^{(\alpha - \alpha')x'} \sum_{y} \lambda^{(\beta - \beta')y} \\
&= \delta_{\alpha\alpha'} \delta_{\beta\beta'}.
\end{aligned}$$

This is again by the fact that a sum over all roots of unity is zero.

**Orthogonality relations**

Instead of using induction to obtain the rest of the irreducible characters one can make a guess and then use the orthogonality relations to show that they are irreducible. And if we look at the previous group and make a bold guess, we assume that the irreducible characters of $Z_{p^2} \rtimes Z_p$ are the of same type as those of $(Z_p \times Z_p) \rtimes Z_p$. So we let $\chi_\zeta$ be zero outside $Z(G)$ and defined therein by

$$\chi_\zeta(pr, 0) = p\lambda^{\zeta r}.$$

Verification of the irreducibility is easy

$$\begin{aligned}(\chi_\zeta, \chi_{\zeta'}) &= \frac{1}{p^3}\sum_g \chi_\zeta(g)\overline{\chi_{\zeta'}(g)} \\ &= \frac{1}{p^3}\sum_r p\lambda^{\zeta r} p\lambda^{-\zeta' r} \\ &= \frac{1}{p}\sum_r \lambda^{(\zeta-\zeta')r} \\ &= \delta_{\zeta\zeta'}.\end{aligned}$$

We also want to show that they are orthogonal to the $\varphi_{\alpha\beta}$ by calculating

$$\begin{aligned}(\chi_\zeta, \varphi_{\alpha\beta}) &= \frac{1}{|G|}\sum_{g\in G} \chi_\zeta(g)\overline{\varphi_{\alpha\beta}(g)} \\ &= \frac{1}{p^3}\sum_{(pr,0)\in Z(G)} p\lambda^{\zeta r}\lambda^{-\alpha p r}\lambda^{-\beta 0} \\ &= \frac{p}{p^3}\sum_r \lambda^{\zeta r}\end{aligned}$$

thus if $\zeta \neq 0$ we have $(\chi_\zeta, \varphi_{\alpha\beta}) = 0$ are done by Theorem 3.1.7 and have found $p-1$ irreducible characters.

**Character table**

This group has a very similar character table to the other non-abelian $p$-group of order $p^3$. So the table is, with $x' = x \mod p$ and $\zeta \neq 0$

| | $(pr,0)$ | $(x',y)$ |
|---|---|---|
| $\varphi_{\alpha\beta}$ | 1 | $\lambda^{\alpha x'+\beta y}$ |
| $\chi_\zeta$ | $p\lambda^{\gamma r}$ | 0 |

## 3.4 Characters of $p$-groups of order $p^4$

We proceed through the list of the non-abelian $p$-groups presented in Section 1.6.3. Again we will throughout this section use $\lambda$ as an arbitrary non-trivial $p$-th root of unity and $\mu$ as any $p^2$-th root.

### 3.4.1 Method

Two of the groups are direct products of the groups of order $p^3$ and $Z_p$ so the characters are obtained as in Section 3.2.2.

The other groups are divided into two cases characterized by $|Z(G)| = p^2$ and $|Z(G)| = p$. The first case is treated as described below but the case where $|Z(G)| = p$ is trickier and I have yet to find a method for this case.

(i) Find the group operation and the formula for the inverse.

(ii) Find the conjugacy classes of the group using the inverse.

(iii) Lift characters with a homomorphism $\eta$ from $G$ to an abelian subgroup of $G$. We will let $\eta$ be defined by collapsing the conjugacy classes, that is, it maps the classes onto their representatives. As it turns out $\eta$ will define a map from $G$ to $G/Z_p$ and for each case we need to verify that it is a well-defined homomorphism to an abelian group. One also need to check that the composition of $\eta$ and the characters of $G/Z_p$ is a class function and that it is an irreducible character. But since a homomorphism to an abelian group always be a class function it is enough to check the irreducibility.

(iv) Make a guess and find the characters of degree $p$. A good starting point is to guess that characters are zero outside the center and has a similar appearance as the $\chi_\zeta$ of the groups of order $p^3$.

(v) When we have found all characters (we know that the number of characters are exactly the same as the number of conjugacy classes, see Theorem 3.1.13) we verify that our characters are irreducible and are non-isomorphic using Theorem 3.1.7.

### 3.4.2 (vi) $Z_{p^3} \rtimes Z_p$

Let $G = Z_{p^3} \rtimes Z_p$. The operation is

$$(x, y) * (x', y') = (x + x' + p^2yx', y + y')$$

and using this we can find the conjugacy classes by first finding the inverse of an arbitrary element.

$$\begin{aligned}(x, y)^{-1} &= ((x, 0) * (0, y))^{-1} \\ &= (0, y)^{-1} * (x, 0)^{-1} \\ &= (0, -y) * (-x, 0) \\ &= (-x + p^2xy, -y).\end{aligned}$$

Then the conjugates of $(x, y)$ by $(u, v)$ are

$$\begin{aligned}
&(u,v)^{-1} * (x,y) * (u,v) = \\
&= (-u + p^2uv, -v) * (x + u + p^2yu, y + v) \\
&= (-u + p^2uv + x + u + p^2yu + p^2(-v)(x + u + p^2yu), -v + y + v) \\
&= (x + p^2(yu - vx), y).
\end{aligned}$$

Thus we see that $Z(G) = \{(pr, 0) \mid r \in Z_{p^2}\}$ since the center of a $p$-group of order $p^4$ has order $p$ or $p^2$ and we have found $p^2$ elements which have trivial conjugacy classes. The non-trivial classes are of size $p$ and have the representatives $(x, y)$ where $x \in Z_{p^2}, y \in Z_p$ and $p \nmid x$, thus we have $p(p^2 - 1)$ such classes ($p^2$ choices for $x$ and $p$ for $y$ and $p$ of those are in $Z(G)$). The total number of classes is $p^3 + p^2 - p$.

**Lifting characters from $Z_{p^2} \times Z_p$**

We want to find a homomorphism which maps the conjugacy classes to their representatives, so let $\eta : (x, y) \mapsto (x \mod p^2, y)$ and $\eta : G \to Z_{p^2} \times Z_p$. This is a homomorphism because

$$\eta((x, y) * (x', y')) = \eta((x + x' + p^2yx', y + y')) = (x + x', y + y')$$

and

$$\eta((x, y)) * \eta((x', y')) = (x, y) * (x', y') = (x + x', y + y').$$

Let $\tau_{\alpha\beta}(x, y) = \mu^{\alpha x}\lambda^{\beta y}$, then we get $p^3$ irreducible characters by taking $\varphi_{\alpha\beta} = \tau_{\alpha\beta} \circ \eta$, which are irreducible because

$$\begin{aligned}
(\varphi_{\alpha\beta}, \varphi_{\alpha'\beta'}) &= \frac{1}{p^4} \sum_{x \in Z_{p^3}, y \in Z_p} \tau_{\alpha\beta} \circ \eta(x, y)\overline{\tau_{\alpha\beta} \circ \eta(x, y)} \\
&= \frac{p}{p^4} \sum_{x' \in Z_{p^2}, y \in Z_p} \tau_{\alpha\beta}(x', y)\overline{\tau(x', y)} \\
&= \frac{1}{p^3} \sum_{x' \in Z_{p^2}, y \in Z_p} \mu^{(\alpha-\alpha')x'}\lambda^{(\beta-\beta')y} \\
&= \frac{1}{p^2} \sum_{x' \in Z_{p^2}} \mu^{(\alpha-\alpha')x'} \frac{1}{p} \sum_{y \in Z_p} \lambda^{(\beta-\beta')y} \\
&= \delta_{\alpha\alpha'}\delta_{\beta\beta'}.
\end{aligned}$$

**Orthogonality relations**

For $(pr,0) \in Z(G)$ let $\theta_\gamma(pr,0) = p\mu^{\gamma r}$, where $\mu$ is a $p^2$-th root of unity, and $\theta_\gamma = 0$ for values outsize $Z(G)$. We verify irreducibility as

$$\begin{aligned}(\theta_\gamma, \theta_{\gamma'}) &= \frac{1}{p^4} \sum_{x \in Z_{p^3}, y \in Z_p} \theta_\gamma(x,y)\overline{\theta_\gamma(x,y)} \\ &= \frac{1}{p^4} \sum_{r \in Z_{p^2}} p\mu^{\gamma r} p\mu^{-\gamma' r} \\ &= \frac{p^2}{p^4} \sum_{r \in Z_{p^2}} \mu^{(\gamma-\gamma')r} \\ &= \delta_{\gamma\gamma'}.\end{aligned}$$

We check that the $\theta_\gamma$ are non-isomorphic to $\varphi_{\alpha\beta}$ by

$$\begin{aligned}(\theta_\gamma, \varphi_{\alpha\beta}) &= \frac{1}{p^4} \sum_{x \in Z_{p^3}, y \in Z_p} \theta_\gamma(x,y)\overline{\varphi_{\alpha\beta}(x,y)} \\ &= \frac{1}{p^4} \sum_{r \in Z_{p^2}} p\mu^{\gamma r} \mu^{\alpha p r} \lambda^{\beta 0} \\ &= \frac{p}{p^4} \sum_{r \in Z_{p^2}} \mu^{(\gamma-\alpha p)r}\end{aligned}$$

and we see that so long as $\gamma \not\equiv \alpha p$ for all $\alpha$ then $(\theta_\gamma, \varphi_{\alpha\beta}) = 0$. So we get $p^2 - p$ choices for $\gamma$ and thus we have found the rest of the irreducible representations.

**Character table**

We have found $p^3$ characters of degree 1 and $p^2 - p$ characters of degree $p$, we know that there are no more since there are $p^3 + p^2 - p$ conjugacy classes of $G$. Thus the character table of $G$ is, where $p \nmid \gamma$

| | $(pr,0)$ | $(x \mod p^2, y)$ |
|---|---|---|
| $\varphi_{\alpha\beta}$ | $\mu^{\beta pr}$ | $\lambda^{\alpha x}\mu^{\beta y}$ |
| $\theta_\gamma$ | $p\mu^{\gamma r}$ | $0$ |

### 3.4.3 (vii) $(Z_{p^2} \times Z_p) \rtimes Z_p$

Let $G$ be $(Z_{p^2} \times Z_p) \rtimes Z_p$ and we know the operation of this group as

$$((x,y),z) * ((x',y'),z') = ((x + x' + pzy', y + y'), z + z').$$

The inverse of an arbitrary element is

$$\begin{aligned}((x,y),z)^{-1} &= (((x,0),0)*((0,y),0)*((0,0),z))^{-1}\\ &= ((0,0),z)^{-1}*((0,y),0)^{-1}*((x,0),0))^{-1}\\ &= ((0,0),-z)*((0,-y),0)*((-x,0),0))\\ &= ((pyz,-y),-z)*((-x,0),0)\\ &= ((-x+pyz,-y),-z)\end{aligned}$$

thus the conjugates of $((x,y),z)$ by $((u,v),w)$ are

$$\begin{aligned}&((u,v),w)^{-1}*((x,y),z)*((u,v),w) =\\ &= ((-u+pvw,-v),-w)*((x+u+pzv,y+v),z+w)\\ &= ((x+p(zv-yw),y,z).\end{aligned}$$

We see that $Z(G)=\{((x,0),0)\}$ and that the representatives of the non-trivial classes are $((x \mod p,y),z)$ where $y$ and $z$ not both zero. Thus we have $p^3-p$ classes of size $p$ and the total number of classes is $p^3+p^2-p$.

**Lifting characters from $Z_p \times Z_p \times Z_p$**

Let $\eta : ((x,y),z) \mapsto (x \mod p,y,z)$ which takes $G$ to $Z_p \times Z_p \times Z_p$. This will define our homomorphism since it collapses the conjugacy classes and it truly is a homomorphism since

$$\eta(((x,y),z)*((x',y'),z')) = \eta(((x+x'+pzy',y+y'),z+z') = (x+x',y+y',z+z')$$

and

$$\eta(((x,y),z))*\eta(((x',y'),z')) = (x,y,z)*(x',y',z') = (x+x',y+y',z+z').$$

We use $\eta$ to lift the character $\tau_{\alpha\beta\gamma}(x,y,z) = \lambda^{\alpha x}\lambda^{\beta y}\lambda^{\gamma z}$ to a character on $G$ as $\varphi_{\alpha\beta\gamma} = \tau_{\alpha\beta\gamma}\circ\eta$. These characters are irreducible since

$$\begin{aligned}(\varphi_{\alpha\beta\gamma},\varphi_{\alpha'\beta'\gamma'}) &= \frac{1}{p^4}\sum_{x\in Z_{p^2},y,z\in Z_p}\varphi_{\alpha\beta\gamma}((x,y),z)\overline{\varphi_{\alpha'\beta'\gamma'}((x,y),z)}\\ &= \frac{p}{p^4}\sum_{x',y,z\in Z_p}\lambda^{(\alpha-\alpha')x'}\lambda^{(\beta-\beta')y}\lambda^{(\gamma-\gamma')z}\\ &= \delta_{\alpha\alpha'}\delta_{\beta\beta'}\delta_{\gamma\gamma'}.\end{aligned}$$

**Orthogonality relations**

Let $\theta_\zeta((x,0),0) = p\mu^{\zeta x}$ and $\theta_\zeta = 0$ outside $Z(G)$. Check that $\theta_\zeta$ is irreducible

$$\begin{aligned}(\theta_\zeta, \theta_{\zeta'}) &= \frac{1}{p^4} \sum_{x\in Z_{p^2}, y,z\in Z_p} \theta_\zeta((x,y),z)\overline{\theta_{\zeta'}((x,y),z)} \\ &= \frac{p^2}{p^4} \sum_{xZ_{p^2}} \mu^{(\zeta-\zeta')x'} \\ &= \delta_{\zeta\zeta'}.\end{aligned}$$

Check that the $\theta_\zeta$ are non-isomorphic to $\varphi_{\alpha\beta\gamma}$

$$\begin{aligned}(\theta_\zeta, \varphi_{\alpha\beta\gamma}) &= \frac{1}{p^4} \sum_{x\in Z_{p^2}, y,z\in Z_p} \theta_\zeta((x,y),z)\overline{\varphi_{\alpha\beta\gamma}((x,y),z)} \\ &= \frac{1}{p^4} \sum_{x\in Z_{p^2}} p\mu^{\zeta x}\lambda^{-\alpha x}\lambda^{-\beta 0}\lambda^{-\gamma 0} \\ &= \frac{p}{p^4} \sum_{x\in Z_{p^2}} \mu^{\zeta x}\lambda^{\alpha x}\end{aligned}$$

Observe now that for some suitable non-zero $a$ we have $\lambda = \mu^{pa}$ since $\lambda$ is a $p$-root and $\mu$ is a $p^2$-th root, then we get that

$$(\theta_\zeta, \varphi_{\alpha\beta\gamma}) = \frac{p}{p^4} \sum_{x\in Z_{p^2}} \mu^{(\zeta - pa\alpha)x}.$$

For this to be zero for all $\alpha$ we need that $\zeta \not\equiv pa\alpha \mod p$, but this is saying that $p \nmid \zeta$. So we get $p^2 - p$ choices for $\zeta$ thus we have found our irreducible representations of degree $p$.

**Character table**

We have found $p^3$ characters of degree 1 and $p^2 - p$ characters of degree $p$, we know that there are no more since there are $p^3 + p^2 - p$ conjugacy classes of $G$. Thus the character table of $G$ is, where $p \nmid \zeta$

| | $((x,0),0)$ | $((x \mod p, y), z)$ |
|---|---|---|
| $\varphi_{\alpha\beta\gamma}$ | $\lambda^{\alpha x}$ | $\lambda^{\alpha x}\lambda^{\beta y}\lambda^{\gamma z}$ |
| $\theta_\zeta$ | $p\mu^{\zeta x}$ | $0$ |

### 3.4.4 (viii) $Z_{p^2} \rtimes Z_{p^2}$

Let $G$ be $Z_{p^2} \rtimes Z_{p^2}$ with the operation

$$(x, y) * (x', y') = (x + x' + pyx', y + y').$$

The inverse of an arbitrary element is

$$\begin{aligned}(x, y)^{-1} &= ((x, 0) * (0, y))^{-1} \\ &= (0, y)^{-1} * (x, 0)^{-1} \\ &= (0, -y) * (-x, 0) \\ &= (-x + pxy, -y)\end{aligned}$$

and thus we get the conjugates of $(x, y)$ by $(u, v)$ as

$$\begin{aligned}(u, v)^{-1} * (x, y) * (u, v) &= (-u + puv, -v) * (x + u + pyu, y + v) \\ &= (x + p(yu - vx), y)\end{aligned}$$

Thus the center of $G$ is $\{(pr, ps) \mid r, s \in Z_p\}$ and the non-trivial classes are represented by $(x \mod p, y)$ where if $x = 0$ then $y \not\equiv 0 \mod p$ since otherwise $(x, y) \in Z(G)$. There are $p^3 - p$ such classes and they are of size $p$, so we have a total of $p^3 + p^2 - p$ conjugacy classes of $G$.

#### Lifting characters from $Z_p \times Z_{p^2}$

Let $\eta : (x, y) \mapsto (x \mod p, y)$ which is a homomorphism from $G$ to $Z_p \times Z_{p^2}$, since

$$\eta((x, y) * (x', y')) = \eta((x + x' + pyx', y + y')) = (x + x', y + y')$$

and

$$\eta((x, y)) * \eta((x', y')) = (x, y) * (x', y') = (x + x', y + y').$$

So we use $\eta$ to lift the characters $\tau_{\alpha\beta}(x, y) = \lambda^{\alpha x}\mu^{\beta y}$ of $Z_p \times Z_{p^2}$ to $G$. Let $\varphi_{\alpha\beta} = \tau_{\alpha\beta} \circ \eta$ and verify irreducibility

$$\begin{aligned}(\varphi_{\alpha\beta}, \varphi_{\alpha'\beta'}) &= \frac{1}{p^4} \sum_{x,y \in Z_{p^2}} \varphi_{\alpha\beta}(x, y)\overline{\varphi_{\alpha'\beta'}(x, y)} \\ &= \frac{p}{p^4} \sum_{x' \in Z_p, y \in Z_{p^2}} \lambda^{(\alpha-\alpha')x'}\mu^{(\beta-\beta')y} \\ &= \delta_{\alpha\alpha'}\delta_{\beta\beta'}.\end{aligned}$$

**Orthogonality relations**

Let $\theta_{\varepsilon\zeta}(pr,ps) = p\lambda^{\varepsilon r}\lambda^{\zeta s}$ for $(pr,ps) \in Z(G)$ and let $\theta_{\varepsilon\zeta} = 0$ otherwise. These characters are irreducible since

$$\begin{aligned}(\theta_{\varepsilon\zeta},\theta_{\varepsilon'\zeta'}) &= \frac{1}{p^4}\sum_{x,y\in Z_{p^2}} \theta_{\varepsilon\zeta}(x,y)\overline{\theta_{\varepsilon'\zeta'}(x,y)} \\ &= \frac{p^2}{p^4}\sum_{r,s\in Z_p} \lambda^{(\varepsilon-\varepsilon')r}\lambda^{(\zeta-\zeta')s} \\ &= \delta_{\varepsilon\varepsilon'}\delta_{\zeta\zeta'}.\end{aligned}$$

They are non-isomorphic to the $\varphi_{\alpha\beta}$ since

$$\begin{aligned}(\theta_{\varepsilon\zeta},\varphi_{\alpha,\beta}) &= \frac{1}{p^4}\sum_{x,y\in Z_{p^2}} \theta_{\varepsilon\zeta}(x,y)\overline{\varphi_{\alpha\beta}(x,y)} \\ &= \frac{1}{p^4}\sum_{(pr,ps)\in Z(G)} p\lambda^{\varepsilon r}\lambda^{\zeta s}\lambda^{-\alpha pr}\mu^{-\beta ps} \\ &= \frac{p}{p^4}\sum_{r\in Z_p}\lambda^{(\varepsilon-p\alpha)r}\sum_{s\in Z_p}\lambda^{\zeta s}\mu^{-\beta ps}\end{aligned}$$

because if $\varepsilon \neq 0$ then $\sum_{r\in Z_p}\lambda^{(\varepsilon-p\alpha)r} = 0$ and thus $(\theta_{\varepsilon\zeta},\varphi_{\alpha,\beta}) = 0$, so the $\theta_{\varepsilon\zeta}$ are $p(p-1)$ irreducible characters.

**Character table**

We have found $p^3$ characters of degree 1 and $p^2-p$ characters of degree $p$, we know that there are no more since there are $p^3+p^2-p$ conjugacy classes of $G$. Thus the character table of $G$ is, where $\varepsilon \neq 0$

| | $(pr,ps)$ | $(x \mod p, y)$ |
|---|---|---|
| $\varphi_{\alpha\beta}$ | $\mu^{\beta ps}$ | $\lambda^{\alpha x}\mu^{\beta y}$ |
| $\theta_{\varepsilon\zeta}$ | $p\lambda^{\varepsilon r}\lambda^{\zeta s}$ | $0$ |

### 3.4.5 (ix) $(Z_{p^2} \rtimes Z_p) \times Z_p$

Let $G$ be $(Z_{p^2} \rtimes Z_p) \times Z_p$ and observe that $G$ is a direct product of two groups of which we know the irreducible characters, see Section 3.3.2. We also observe that the conjugacy classes of $G$ are represented by the products of the representatives of the classes in $Z_{p^2} \rtimes Z_p$ and $Z_p$. Thus we have $p(p^2+p-1)$ classes in $G$ represented by

$((x \mod p, y), z)$ and the center is $\{((pr, 0), z) \mid r, z \in Z_p\}$. We then proceed as we did in Section 3.2.2 and the characters as are

| | $((pr,0),z)$ | $((x \mod p, y), z)$ |
|---|---|---|
| $\varphi_{\alpha\beta\gamma}$ | $\lambda^{\gamma z}$ | $\lambda^{\alpha x}\lambda^{\beta y}\lambda^{\gamma z}$ |
| $\theta_{\varepsilon\zeta}$ | $p\lambda^{\varepsilon r}\lambda^{\zeta z}$ | $0$ |

### 3.4.6 (x) $(Z_p \times Z_p) \rtimes Z_{p^2}$

Let $G$ be $(Z_p \times Z_p) \rtimes Z_{p^2}$ with the group operation as

$$((x, y), z) * ((x', y'), z') * ((x + x', y + y' + zx'), z + z').$$

The inverse of an element in $G$ is

$$\begin{aligned}((x,y),z)^{-1} &= (((x,0),0) * ((0,y),0) * ((0,0),z))^{-1} \\ &= ((0,0),-z)^{-1} * ((0,-y),0)^{-1} * ((-x,0),0)^{-1} \\ &= ((0,-y),-z) * ((-x,0),0) \\ &= ((-x,-y+xz),-z).\end{aligned}$$

Then the conjugates of an element $((x, y), z)$ by $((u, v), w)$ is

$$\begin{aligned}&((u,v),w)^{-1} * ((x,y),z) * ((u.v),w) = \\ &= ((-u,-v+uw),-w) * ((x+u,y+v+zu),z+w) \\ &= ((x,y+zu-xw),z).\end{aligned}$$

So we see that $Z(G) = \{((0, y), pr) \mid y, r \in Z_p\}$ and the representatives of the non-trivial classes are $((x, 0), z)$ where $p \nmid z$ if $x = 0$. Thus we get $p(p^2 - 1)$ such classes of size $p$, and a total of $p^3 + p^2 - p$ conjugacy classes of $G$.

#### Lifting characters from $Z_p \times Z_{p^2}$

Let $\eta : ((x, y), z) \mapsto (x, z)$ which is both a homomorphism from $G$ to $Z_p \times Z_{p^2}$.

$$\eta((x,y),z) * ((x',y'),z')) = \eta(((x+x',y+y'+zx'),z+z') = (x+x',z+z')$$

and

$$\eta(((x,y),z)) * \eta(((x',y'),z')) = (x,z) * (x',z') = (x+x',z+z').$$

Let $\varphi_{\alpha\beta} = \tau_{\alpha\beta} \circ \eta$ where $\tau_{\alpha\beta}(x, y) = \lambda^{\alpha x}\mu^{\beta y}$. Then $\varphi_{\alpha\beta}$ are irreducible

$$\begin{aligned}(\varphi_{\alpha\beta}, \varphi_{\alpha'\beta'}) &= \frac{1}{p^4} \sum_{x,y \in Z_p, z \in Z_{p^2}} \varphi_{\alpha\beta}((x,y),z)\overline{\varphi_{\alpha'\beta'}((x,y),z)} \\ &= \frac{p}{p^4} \sum_{x \in Z_p, z \in Z_{p^2}} \lambda^{(\alpha-\alpha')x'}\mu^{(\beta-\beta')z} \\ &= \delta_{\alpha\alpha'}\delta_{\beta\beta'}.\end{aligned}$$

**Orthogonality relations**

Let $\theta_{\varepsilon\zeta}((0,y),pr) = p\lambda^{\varepsilon y}\lambda^{\zeta r}$ for $((0,y),pr) \in Z(G)$ and let $\theta_{\varepsilon\zeta} = 0$ otherwise. These characters are irreducible since

$$\begin{aligned}(\theta_{\varepsilon\zeta},\theta_{\varepsilon'\zeta'}) &= \frac{1}{p^4}\sum_{x,y\in Z_p,z\in Z_{p^2}} \theta_{\varepsilon\zeta}((x,y),z)\overline{\theta_{\varepsilon'\zeta'}((x,y),z)}\\ &= \frac{p^2}{p^4}\sum_{y,r\in Z_p}\lambda^{(\varepsilon-\varepsilon')y}\lambda^{(\zeta-\zeta')r}\\ &= \delta_{\varepsilon\varepsilon'}\delta_{\zeta\zeta'}\end{aligned}$$

and they are non-isomorphic to the $\varphi_{\alpha\beta}$

$$\begin{aligned}(\theta_{\varepsilon\zeta},\varphi_{\alpha,\beta}) &= \frac{1}{p^4}\sum_{x,y\in Z_p,z\in Z_{p^2}} \theta_{\varepsilon\zeta}((x,y),z)\overline{\varphi_{\alpha\beta}((x,y),z)}\\ &= \frac{1}{p^4}\sum_{((0,y),pr)\in Z(G)} p\lambda^{\varepsilon y}\lambda^{\zeta r}\lambda^{-\alpha 0}\mu^{-\beta pr}\\ &= \frac{p}{p^4}\sum_{y\in Z_p}\lambda^{\varepsilon r}\sum_{s\in Z_p}\lambda^{\zeta r}\mu^{-\beta pr}\end{aligned}$$

which is zero whenever $\varepsilon \neq 0$ thus we get $p(p-1)$ irreducible characters.

**Character table**

We have found $p^3$ characters of degree 1 and $p^2-p$ characters of degree $p$, we know that there are no more since there are $p^3+p^2-p$ conjugacy classes of $G$. Thus the character table of $G$ is, where $\varepsilon \neq 0$

| | $((0,y),pr)$ | $((x,0),z)$ |
|---|---|---|
| $\varphi_{\alpha\beta}$ | $\mu^{\beta pr}$ | $\lambda^{\alpha x}\mu^{\beta z}$ |
| $\theta_{\varepsilon\zeta}$ | $p\lambda^{\varepsilon y}\lambda^{\zeta r}$ | $0$ |

## 3.4.7 (xi) $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_1} Z_p$

Let $G$ be $(Z_{p^2} \rtimes Z_p) \rtimes_{\varphi_1} Z_p$ with the operation

$$((x,y),z) * ((x',y'),z') = ((x+x'+pzx'\frac{x'-1}{2}+pyx', y+y'+x'z), z+z').$$

The inverse of $((x,y),z)$ is

$$\begin{aligned}((x,y,z),w)^{-1} &= ((0,0),-z) * ((0,-y),0) * ((-x,0),0)\\ &= ((0,-y),-z) * ((-x,0),0)\\ &= ((-x-pzx\frac{x+1}{2}+pxy, -y+xz), -z).\end{aligned}$$

Then the conjugates of $((x,y),z)$ by $((u,v),w)$ are

$$\begin{aligned}
&((u,v),w)^{-1} * ((x,y),z) * ((u,v),w) = \\
&= ((-u - pwu\frac{u+1}{2} + puv, -v + uw), -w) \\
&\quad *((x + u + pzu\frac{u-1}{2} + pyu, y + v + uz), z + w) \\
&= ((x + p(yu - vx + zu\frac{u-1}{2} - wx\frac{x-1}{2}), y + uz - xw), z).
\end{aligned}$$

Thus we see that $Z(G) = \{((pr,0),0) \mid r \in Z_p\}$. The observe also that the conjugacy classes of order $p$ are represented by $((0,y),z)$ and there are thus $p^2-1$ of them. Further we get $p(p-1)$ classes of order $p^2$ with $((x \mod p, 0), z)$ as representatives, and so we have $2p^2-1$ conjugacy classes in $G$.

In this group $|Z(G)| = p$ and thus our method fails and I have not found another way of obtaining the characters yet.

### 3.4.8 (xiv) $((Z_p \times Z_p) \rtimes Z_p) \times Z_p$

Observe that this group is a direct product and proceed as in Section 3.4.5. We know the characters of $(Z_p \times Z_p) \rtimes Z_p$ from Section 3.3.1 and the conjugacy classes, so we conclude that we have $p(p^2+p-1)$ classes represented by $(((x,0),z),w)$ and the center is $(((0,y),0),w)$. Thus the character table looks like, where $\varepsilon \neq 0$

| | $(((0,y),0),w)$ | $(((x,0),z),w)$ |
|---|---|---|
| $\varphi_{\alpha\beta\gamma}$ | $\lambda^{\gamma w}$ | $\lambda^{\alpha x}\lambda^{\beta z}\lambda^{\gamma w}$ |
| $\theta_{\varepsilon\zeta}$ | $p\lambda^{\varepsilon y}\lambda^{\zeta z}$ | $0$ |

### 3.4.9 (xv) $(Z_p \times Z_p \times Z_p) \rtimes Z_p$, $p > 3$

Let $G$ be $(Z_p \times Z_p \times Z_p) \rtimes Z_p$ with the operation

$$((x,y,z),w)*((x',y',z'),w') = ((x+x'+y'w+z'\frac{w(w-1)}{2}, y+y'+wz', z+z'), w+w').$$

The inverse of an element is then

$$\begin{aligned}
((x,y,z),w)^{-1} &= ((0,0,0),-w) * ((0,0,-z),0) \\
&\quad *((0,-y,0),0) * ((-x,0,0),0) \\
&= ((-zw\frac{w+1}{2}, zw, -z), -w) * ((-x,-y,0),0) \\
&= ((-x - zw\frac{w+1}{2} + yw, -y + zw, -z), -w).
\end{aligned}$$

So the conjugates of $((x,y,z),w)$ by $((x',y',z'),w')$ are

$$\begin{aligned}
&((x',y',z'),w')^{-1} * ((x,y,z),w) * ((x',y',z'),w') = \\
&= ((-x'-z'w'\frac{w'+1}{2}+y'w', -y'+z'w', -z'), -w') \\
&\quad *((x+x'+y'w+z'w\frac{(w-1)}{2}, y+y'+wz', z+z'), w+w') \\
&= ((x+y'w-yw'-z'ww'+z'w\frac{w-1}{2}+zw'\frac{w'+1}{2}, y+wz'-w'z, z), w).
\end{aligned}$$

We observe that $Z(G)$ is the elements of the type $((x,0,0),0)$. In this group we have $p(p-1)$ classes of order $p^2$ with representatives $((0,0,z),w)$ where $w \neq 0$ and $p^2-1$ classes of order $p$ represented by $((0,y,z),0)$. So in total we have $2p^2-1$ conjugacy classes in $G$.

Since $|Z(G)| = p$ our method does not work for this group and I haven't found the characters of this group yet.

## 3.5 Observations and conjectures

When we calculated the conjugacy classes of these $p$-groups we noted that they all seemed to behave similarly. If we would calculate the conjugacy classes of the remaining two groups of the type $(Z_{p^2} \rtimes Z_p) \rtimes_\varphi Z_p$ I believe we would get that

**Conjecture 3.5.1.** *In the case of $|G| = p^3$ with $p > 2$ or $|G| = p^4$ with $p > 3$ the number of conjugacy classes are determined by the size of the center.*

It would be interesting to investigate whether this is true for all $p$-groups or is this perhaps just a low-order accident?

Another thing that might be worth looking into is if the method of obtaining the characters will work for larger $p$-groups.

**Conjecture 3.5.2.** *Let $|G| = p^\alpha$, then if $Z(G)$ has maximal size our method presented in Section 3.4.1 will work and we will get a character table which looks like the ones we have seen.*

# Bibliography


[1] Maple 12.0. Copyright (c) Maplesoft, a division of Waterloo Maple inc. 1981-2008.

[2] J. L. Alperin and Rowen B. Bell. *Groups and representations*, volume 162 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[3] William Burnside. *Theory of groups of finite order*. Cambridge University Press, first edition, 1897. Reprinted 2010 through Nabu Press.

[4] Keith Conrad. Groups of order $p^3$. Downloaded 2010-03-02 http://www.math.uconn.edu/∼conrad/blurbs/grouptheory/groupsp3.pdf.

[5] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004. 0-471-43334-9.

[6] John B. Fraleigh. *A First Course on Abstract Algebra*. 7th edition edition.

[7] D.L. Johnson. *Presentations of Groups*. Cambridge University Press, second edition, 1997.

[8] Jean-Pierre Serre. *Linear representations of finite groups*, volume 42 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott.