Aspects of automorphism towers


Supervisor: prof.dr. H.W. Lenstra

Mathematical Institute, University of Leiden
## Contents

1 Introduction .............................................. 3
2 Definitions, conventions and an essential lemma .......... 4
3 Automorphism group and normalizer ...................... 5
4 Specific height ........................................... 7
5 Automorphism tower of \( p \)-adic integers .............. 10
6 Automorphism groups of finite products of abelian groups 14
7 Abelian automorphism towers for finitely generated abelian groups 16
8 Basic subgroups ......................................... 18
9 Abelian automorphism groups ............................ 22
10 References .............................................. 24
1 Introduction

For a group $G$ denote $\theta_G : G \to \text{Aut } G, g \mapsto (x \mapsto gxg^{-1})$. Whenever the group $G$ is clear from the context, it will be omitted from the notation. Define $G_0 = G$ and for $i \in \mathbb{Z}_{\geq 1}$ define $G_i = \text{Aut } G_{i-1}$. I use the notation $\text{Aut}^i G$ for $G_i$. This sequence of groups combined with the maps $\theta_{G_i}$ is called the automorphism tower of $G$.

When introducing a new definition, new questions arise. I cannot answer all questions in this thesis, hence I focused on three aspects of the automorphism towers: the height, stable categories and the abelian automorphism towers.

Wielandt ([1], 1939) showed that for a finite group with a trivial center there exists $m \in \mathbb{Z}_{\geq 0}$ such that $\theta_{G_m}$ is an isomorphism. It would be logical to give such smallest $m$ a name. We say that a group $G$ has height $m$ if $m$ is the smallest non-negative integer such that $G_m \cong G_{m+1}$. Note that in my definition of height I do not specify what the isomorphism between the groups is, because later on I will use the definition for abelian groups as well. The height of a finite group with a trivial center is finite, but can we reach all possible heights? The answer is yes and is shown by the following theorem.

**Theorem 1.1.** For all $m \in \mathbb{Z}_{\geq 0}$ there exists a finite group $G$ with trivial center such that $G$ has height $m$ and the map $\theta_{G_m}$ is an isomorphism.

This will be proven in chapter 4. One could also ask the question if we can find an infinite group with a trivial center such that its automorphism tower has infinite height. The construction used for theorem 1.1 can be extended to get such a group. Since it takes little effort, I will show this in chapter 4 as well.

Calculating automorphism towers can become quite difficult. For example the automorphism tower of the group of 2-adic integers $\mathbb{Z}_2$ is already quite difficult after 6 steps (calculating the tower for $\mathbb{Z}_3$ is a fun exercise). This is the reason that I don’t work out specific examples. It would be nice if we could formulate some kind of theorem that shows that if $G$ has some property then $\text{Aut } G$ has that as well. These kinds of theorems show that every group in the automorphism tower of $G$ has a certain property. This inspired the following definition. For a category $\mathcal{C}$ denote $\mathcal{C}_0$ the collection of objects and $\mathcal{C}_1$ the collection of morphisms. Let $\mathcal{C}$ be a full subcategory of the category of groups. We call $\mathcal{C}$ stable if for all $C \in \mathcal{C}_0$ there exists a $D \in \mathcal{C}_0$ such that $\text{Aut } C \cong D$. The following stable category is actually used in the proof of theorem 1.1.

A group $G$ is called semi-simple if $G$ is isomorphic to a direct sum of simple groups and is called perfect if $G = [G, G]$.

**Theorem 1.2.** Let $S$ be a perfect semi-simple group. Then the category $\mathcal{C}_S$ with $(\mathcal{C}_S)_0 = \{ G \subset \text{Aut } S | \theta_S(S) \subset G \}$ is a stable category.

I will prove this theorem in chapter 3. As said before, I calculated the automorphism tower of $\mathbb{Z}_2$ for a few steps. I could not find out whether this tower has finite height or not, but I could deduce a pattern which led to the following result.

**Theorem 1.3.** Let $p$ be a prime. Then the category $(\mathcal{C}_p)_0 = \{ G | \exists f : G \to \mathbb{Z}_p : \# \ker(f) < \infty \}$ is a stable category.

I will prove this in chapter 5. I will also show that the existence of a surjective group homomorphism $G \to \mathbb{Z}_p$ with a finite kernel is equivalent to two other statements.

Let $A$ be an abelian group. If all groups in the automorphism tower of $A$ are abelian,
then $A$ has an abelian automorphism tower. I have tried to classify all abelian groups that have an abelian automorphism tower. For finitely generated abelian groups I have found a classification. For infinitely generated abelian groups I do not have a classification, but I do have a result that eliminates a lot of groups.

**Theorem 1.4.** Let $A$ be a finitely generated abelian group. Then $A$ has an abelian automorphism tower iff $A$ is cyclic and $|A|$ is contained in one of the following sets:

- $\{3^m, 2 \cdot 3^m | m \in \mathbb{Z}_{\geq 1}\}$
- $\{2 \cdot 3^m + 1, 2(2 \cdot 3^m + 1) | m \in \mathbb{Z}_{\geq 1}, 2 \cdot 3^m + 1 \text{ is prime}\}$
- $\{1, 2, 4, 5, 10, 11, 22, 23, 46, 47, 94\}$
- $\{\infty\}$

This theorem will be proven in chapter 7. Note that $\mathbb{Z}/3^m\mathbb{Z}$ has height $m + 1$ for $m \geq 1$. This shows that for each $m \in \mathbb{Z}_{\geq 0}$ we can find a group that has an abelian automorphism tower of height $m$. From theorem 1.4 we can deduce that if we want to find a group with an abelian automorphism tower of infinite height, we need to look at infinitely generated abelian groups.

**Theorem 1.5.** Let $A$ be an abelian group such that $Aut_i^i A$ is abelian for $i = 0, ..., 4$ and $Aut A$ is infinite. Then $Aut A \cong \mathbb{Z}/2\mathbb{Z} \oplus C$ where $C$ is a $\mathbb{Z}[2^{-1}]$-module.

I will prove this in chapter 9, which uses $p$-basic subgroups. I do not assume that the reader knows this, hence chapter 8 covers this topic. I have not been able to show that for each $m \in \mathbb{Z}_{\geq 0}$ there exists an infinitely generated abelian group such that its abelian automorphism tower has height $m$ (finding a non-trivial group for $m = 0$ is a fun exercise), which is considerably harder than in the finitely generated case. I did not show either there exists a group with an abelian automorphism tower of infinite height.

### 2 Definitions, conventions and an essential lemma

For a set $X$ denote $\text{Sym} X$ as the symmetric group acting on $X$. For $n \in \mathbb{Z}_{\geq 0}$ denote $\underline{n}$ as the set $\{0, 1, ..., n - 1\}$.

For a group $G$ and a set $X$ I will denote $G^X := \prod_{x \in X} G$ and $G^{(X)} := \bigoplus_{x \in X} G$. I will denote $G_x$ as the $x$-th coordinate axis.

For a non-trivial ring $R$ with a multiplicative unit, denote $R^*$ as the group of invertible elements of $R$.

**Definition 2.1.** Let $G$ be a group. The exponent of $G$ is the least common multiple of the orders of all elements in $G$. If there is no least common multiple, the exponent is infinite.

**Definition 2.2.** Let $G$ and $H$ be groups and $\Omega$ an $H$-set. Define $\psi : H \to Aut(G^{\Omega}), h \mapsto ((g_w)_{w \in \Omega} \mapsto (g_{h^{-1}w})_{w \in \Omega})$. Define the wreath product $G \wr_\psi H := G^{H} \times_\psi H$.

I will often leave out $\Omega$, since it should be obvious from the context which set is used in the definition.

An abelian group will be written additively and $0$ is the identity element. The only exceptions to this rule are automorphism groups. I will not denote automorphism groups additively even if they are abelian, since this would be more confusing. I will also denote $id_G$ as the identity element of $\text{Aut} G$ and $\circ$ as the symbol for composition. Groups which
are not specified to be abelian will be written multiplicatively and 1 is the identity element. Whenever I write 1 or 0 as a group, I mean the trivial group.

**Lemma 2.3.** Let $1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1$ be a short exact sequence of groups and $s : C \to B$ a homomorphism such that $g \circ s = \text{id}_C$. Then $B$ is isomorphic to $A \times_{\psi} C$ where $\psi : C \to \text{Aut} A, c \mapsto (x \mapsto g(c)xg(c)^{-1})$.

*Proof.* See lemma 2.1 of [2], which is a more general version. \hfill \Box

### 3 Automorphism group and normalizer

In this chapter I will prove two theorems that show a connection between taking automorphism groups and taking normalizers. Note that theorem 3.2 directly implies theorem 1.2. Theorem 3.1 will be needed for the next chapter.

**Theorem 3.1.** Let $T$ be a non-abelian simple group, $X$ a set and $H \subset \text{Sym} X$ a subgroup. Then $\text{Aut}((\text{Aut} T) \wr H) \cong (\text{Aut} T) \wr N_{\text{Sym} X}(H)$.

**Theorem 3.2.** Let $S$ be a perfect semi-simple group. Let $G \subset \text{Aut} S$ be a subgroup with $\theta_S(S) \subset G$. Then $\psi : N_{\text{Aut} S}(G) \to \text{Aut} G, x \mapsto (g \mapsto xgx^{-1})$ is an isomorphism.

Before proving these theorems, I will show some easy results and recall some definitions.

**Lemma 3.3.** Let $I$ be a set, $S_i$ simple groups for $i \in I$ and define $S = \bigoplus_{i \in I} S_i$. Then $S$ is perfect iff for all $i \in I$ holds that $S_i$ is non-abelian.

*Proof.* Follows from $[S, S] = \bigoplus_{i \in I} [S_i, S_i]$. \hfill \Box

Whenever I denote $S$ a perfect semi-simple group, I will always use the letters $I$ for the set and $S_i$ for the simple non-abelian groups. Since these letters will stay fixed throughout this chapter, I will not define them any more.

**Theorem 3.4.** Let $\sigma \in \text{Aut} G$ and $g \in G$. Then holds: $\theta_G(\sigma(g)) = \sigma \circ \theta_G(g) \circ \sigma^{-1}$.

This theorem is trivial, writing out the definitions will just give the equality. However I state it as a theorem since I will be using it a lot.

**Lemma 3.5.** Let $G$ be a group with a trivial center. Then $C_{\text{Aut} G}(\theta_G(G))$ is trivial and $\text{Aut} G$ has a trivial center.

*Proof.* We know $\ker(\theta_G) = Z(G) = 1$, so $\theta_G$ is injective. Let $\sigma \in \text{Aut} G$ such that $\sigma$ commutes with $\theta_G(g)$ for all $g \in G$. By theorem 3.4 and the commuting property, we get $\theta_G(g) = \theta_G(\sigma(g))$. This implies $\sigma = \text{id}_G$, hence $C_{\text{Aut} G}(\theta_G(G)) = 1$. Note that the inclusion $Z(\text{Aut} G) \subset C_{\text{Aut} G}(\theta_G(G))$ always holds, hence $\text{Aut} G$ has a trivial center. \hfill \Box

**Lemma 3.6.** Let $S$ be a perfect semi-simple group. Then any non-trivial normal subgroup $N \triangleleft S$ contains $S_i$ for some $i \in I$. Also, the set of minimal normal subgroups of $S$ equals $\{S_i | i \in I \}$.

*Proof.* Let $N$ be a non-trivial normal subgroup of $S$. Suppose that for all $i \in I$ we have $N \cap S_i = 1$. Now for all $i \in I$ we have $[N, S_i] \subset N \cap S_i$, so $N$ and $S_i$ centralize each other. Since $S$ is the direct sum of these $S_i$, we see that $N \subset Z(S)$. Since all $S_i$ are non-abelian and simple, we must have $Z(S) = 1$. Since $N$ is non-trivial, we get a contradiction. So there exists $i \in I$ such that $[N, S_i] = S_i \subset N$. 

5
Let $i \in I$ and $N < S$ be non-trivial with $N \subset S_i$. By the above, $N$ contains some $S_j$ for $j \in J$. Clearly if $i \neq j$ we have $S_i \cap S_j = 1$, hence we must have $i = j$. This shows $N = S_i$, hence $S_i$ is a minimal normal subgroup.

Let $N$ be a minimal normal subgroup of $S$. Let $i \in I$ such that $S_i \subset N$. Now $S_i$ is normal in $S$ and $N$ was minimal, hence $S_i = N$. So the set of minimal normal subgroups is $\{S_i | i \in I\}$. □

**Definition 3.7.** Let $G$ be a group. The socle of $G$ is the subgroup generated by all minimal normal subgroups of $G$. It is denoted by $\text{Soc}(G)$.

**Definition 3.8.** Let $H \subset G$ be groups. Then $H$ is called a characteristic subgroup if for all $\sigma \in \text{Aut} G$ we have $\sigma(H) = H$.

**Lemma 3.9.** Let $G$ be a group. Then $\text{Soc}(G)$ is a characteristic subgroup of $G$.

*Proof.* This is left as an exercise for the reader. □

The proof of theorem 3.1 uses theorem 3.2, so I will prove 3.2 first.

*Proof of 3.2.* In the rest of the proof I will only use the group $S$ for $\theta_S$, therefore I will shorten notation to $\theta$. I will first show that $\theta(S)$ is a characteristic subgroup of $G$, which I will do by showing that $\theta(S)$ is actually the socle of $G$.

I will first show $\text{Soc}(G) \subset \theta(S)$. Let $N$ be a minimal normal subgroup of $G$. Note that $\theta(S)$ is the inner automorphism group, hence it is normal in $\text{Aut} S$. Therefore it is also normal in $G$. Now consider $\theta(S) \cap N$. It is normal in $G$, but also contained in $N$. Since $N$ is a minimal normal subgroup, the intersection is trivial or equal to $N$. Suppose it is trivial. We have $[N, \theta(S)] \subset \theta(S) \cap N$, so $N$ and $\theta(S)$ centralize each other. But $C_{\text{Aut} S}(\theta(S))$ is trivial by lemma 3.5. Any minimal normal subgroup must be non-trivial by definition, so we have a contradiction. Hence $\theta(S) \cap N = N$, or equivalently $N \subset \theta(S)$.

To make the proof of $\theta(S) \subset \text{Soc}(G)$ easier, I will introduce a new definition.

**Definition 3.10.** Let $H \subset G$ be groups. Now define the normal closure (or also called conjugate closure) of $H$ in $G$, denoted $H^G$, as the smallest normal subgroup in $G$ that contains $H$. In symbols we have $H^G = \bigcap_{H \subset N \subset G} N$.

To show $\theta(S) \subset \text{Soc} G$, it is enough to prove that for all $i \in I$ we have $\theta(S_i) \subset \text{Soc} G$. I will do this by constructing a minimal normal subgroup of $G$, that contains $\theta(S_i)$. In fact, this minimal normal subgroup is exactly $\theta(S_i)^G$. To show this, it is useful to know $H^G = \langle gHg^{-1} | g \in G \rangle$. This is left as an exercise for the reader.

Let $i \in I$ and consider $\theta(S_i)^G$. Note that any automorphism of $S$ must send minimal normal subgroups of $S$ to minimal normal subgroups of $S$. Using theorem 3.4 and lemma 3.6 we get that for all $\sigma \in \text{Aut} S$ we have $\sigma \theta(S_i) \sigma^{-1} = \theta(\sigma(S_i)) = \theta(S_j)$ for some $j \in I$. Hence $\theta(S_i)^G = \langle \theta(S_j) | j \in J \rangle$ for some $J \subset I$. Take such a $J$.

Now all I need to show is that $\theta(S_i)^G$ is actually a minimal normal subgroup of $G$. Suppose $M$ is a non-trivial normal subgroup of $G$ with $M \subset \theta(S_i)^G$. Note that $\theta^{-1}(M)$ is also normal in $S$, hence by lemma 3.6 it must contain some $S_k$ for $k \in I$. In particular $\theta(S_k) \subset \theta(S_i)^G$. Note that holds:

$$\theta(\langle S_j | j \in J \rangle) = \langle \theta(S_j) | j \in J \rangle.$$  

Since $\theta$ is injective, we must have $k \in J$. Hence there exists $g \in G$ such that $\theta(S_k) = g\theta(S_i)g^{-1}$. Now also $\theta(S_i) \subset \theta(S_k)^G$, hence $\theta(S_k)^G = \theta(S_i)^G$. From $\theta(S_k)^G \subset M \subset \theta(S_i)^G$ follows $M = \theta(S_i)^G$.  


So now I have proven \( \theta(S) = \operatorname{Soc} G \), which is a characteristic subgroup of \( G \) by lemma 3.9. Now I will prove that \( \psi \) is an isomorphism. Clearly the kernel of \( \psi \) is exactly the centralizer of \( G \) in \( N_{\Aut S}(G) \). But every element that centralizes \( G \), also centralizes \( \theta(S) \). However, from lemma 3.5, we know \( C_{\Aut S}(\theta(S)) = 1 \), hence the kernel must be trivial. This proves injectivity.

Let \( \sigma \in \Aut G \). I will show \( \sigma \in \operatorname{Im}(\psi) \). Since \( \theta(S) \) is a characteristic subgroup, we have that \( \sigma \big|_{\theta(S)} \) is an automorphism. Take \( \tau \in \Aut S \) such that for all \( s \in S \) we have \( \sigma(\theta(s)) = \theta(\tau(s)) \). Define \( \gamma : G \to \Aut S, \alpha \mapsto \tau \circ \alpha \circ \tau^{-1} \). By theorem 3.4, we see that \( \sigma \) and \( \gamma \) are the same map on \( \theta(S) \). Let \( h \in \theta(S) \) and \( g \in G \). Since \( \theta(S) \) is normal in \( G \) we have:

\[
g h g^{-1} = \gamma \sigma^{-1} (g h g^{-1}) = \gamma \sigma^{-1} (g) \gamma \sigma^{-1} (g^{-1})
\]

\[
\Rightarrow \gamma \sigma^{-1} (g^{-1}) h = h \gamma \sigma^{-1} (g^{-1}) g
\]

\[
\Rightarrow \gamma \sigma^{-1} (g^{-1}) g \in C_G(\theta(S)).
\]

From lemma 3.5 we know \( C_G(\theta(S)) = 1 \), hence \( \sigma(g) = \gamma(g) \). This shows that the image of \( \gamma \) is \( G \) and therefore we have \( \tau \in N_{\Aut S}(G) \) and \( \psi(\tau) = \sigma \). Since \( \psi \) is surjective and injective, it is an isomorphism. \( \square \)

**Proof of 3.1.** Define \( S = T^{|X|} \) and denote \( T_x \) as the \( x \)-th coordinate axis. Note that \( T \) is non-abelian and simple, hence \( S \) is a perfect semi-simple group. I will first show that \( \Aut T \wr \Sym X \) is isomorphic to \( \Aut S \). We have a homomorphism \( f : (\Aut T)^{|X|} \to \Aut S \), which is applying an automorphism of \( T \) on each coordinate of \( X \). From lemma 3.6 follows:

\[
\forall \alpha \in \Aut S, x \in X : \exists y \in X : \alpha(T_x) = T_y.
\]

From this we see that \( \alpha \) induces a bijection on \( X \). This way we get a homomorphism \( g : \Aut S \to \Sym X \). We have the following short exact sequence:

\[
0 \longrightarrow (\Aut T)^{|X|} \overset{f}{\longrightarrow} \Aut S \overset{g}{\longrightarrow} \Sym X \longrightarrow 0.
\]

We can create a map \( s : \Sym X \to \Aut S \), which sends \( \sigma \in \Sym X \) to the automorphism that permutes the coordinates of \( S \) using \( \sigma \). Clearly \( gs = \text{id}_{\Sym X} \). Now using lemma 2.3, we have \( \Aut S \cong (\Aut T) \wr \Sym X \). Note that \( \psi \) from lemma 2.3 is the same \( \psi \) as in the definition of the wreath product, hence we have \( \Aut S \cong (\Aut T) \wr \Sym X \). Denote the isomorphism \( \Phi : (\Aut T) \wr \Sym X \to \Aut S \).

Let \( H \subset \Sym X \) and consider \( G = \Phi((\Aut T) \wr H) \). Note that we have \( \theta(S) \subset \Phi((\Aut T) \wr 1) \), hence \( \theta(S) \subset G \). Now \( G \) satisfies the requirements for theorem 3.2, so \( N_{\Aut S}(G) \cong \Aut G \). Since \( \Phi \) is an isomorphism, we have \( N_{\Aut S}(G) \cong N_{(\Aut T) \wr \Sym X}((\Aut T) \wr H) \). Now \( \Phi(H) \subset H \subset \Sym X \). From the third isomorphism theorem we see that any subgroup of \( (\Aut T) \wr \Sym X \) that also contains \( (\Aut T) \wr 1 \) must be of the form \( (\Aut T) \wr K \) for some subgroup \( K \subset \Sym X \). Also, the bijection from the third isomorphism theorem preserves conjugation. Thus \( N_{(\Aut T) \wr \Sym X}((\Aut T) \wr H) \) is exactly \( (\Aut T) \wr N_{\Sym X}(H) \). \( \square \)

4 Specific height

In this chapter I will shorten my notation of taking normalizers. I will not denote the group in which I take the normalizer, since this group is always \( \Sym 2^m \) for some \( m \in \mathbb{Z}_{\geq 0} \). Note that \( A_5 \) is a finite simple non-abelian group, hence theorem 4.1 implies 1.1.
Theorem 4.1. Let \( m \in \mathbb{Z}_{\geq 0} \). Then there exists a subgroup \( H \subset \text{Sym} \frac{2^m}{m} \) such that for each simple non-abelian group \( T \) the height of \((\text{Aut} T) \upharpoonright H\) is \( m \), \( \text{Z}(\text{Aut} T) \upharpoonright H) = 1 \) and \( \theta_{\text{Aut}^m(\text{Aut} T) \upharpoonright H} \) is an isomorphism.

Theorem 4.2. There exists a subgroup \( H \subset \text{Sym} \mathbb{Z}_{\geq 0} \) such that for each simple non-abelian group \( T \) the height of \((\text{Aut} T) \upharpoonright H\) is infinite and \( \text{Z}(\text{Aut} T) \upharpoonright H) = 1 \).

Theorem 4.3. For all \( m \in \mathbb{Z}_{\geq 0} \) there exists a chain of subgroups \( H_0 \subset \ldots \subset H_m \subset \text{Sym} \frac{2^m}{m} \) which satisfy the following statements:

1. \( N(H_i) = H_{i+1} \) for \( 0 \leq i < m \),
2. \( N(H_m) = H_m \),
3. \( H_i \) acts transitively on \( \frac{2^m}{m} \) iff \( i = m \),
4. \( |H_{i+1}:H_i| = 2 \) for \( 0 \leq i < m \),
5. \( H_0 \) stabilizes \( 0 \),
6. \( H_m \) is a 2-Sylow subgroup of \( \text{Sym} \frac{2^m}{m} \),
7. \( H_0 \) is a 2-Sylow subgroup of \( \text{Sym} (\frac{2^m}{m}\setminus\{0\}) \).

To use theorem 4.3 and 3.1 for proving 4.1 conditions 3-7 are not needed. However, proving conditions 1 and 2 is easier if I show 3-5 first. Conditions 6 and 7 give a good idea of what the groups in the chains are.

Before going into the proofs, I want to state a very important convention. I will be taking products of subgroups of symmetric groups, so I will define how to interpret this product. Let \( m \in \mathbb{Z}_{\geq 0} \). Define \( X_1 = \{0,1,\ldots,2^m-1\} \) and \( X_2 = \{2^m,\ldots,2^m+1-1\} \). Note: \( X_1 \cup X_2 = \frac{2^m+1}{m} \). Since \( |X_1| = |X_2| = 2^m \), we have \( \text{Sym} X_1 \cong \text{Sym} X_2 \). So if we have subgroups \( G,H \subset \text{Sym} \frac{2^m}{m} \), we can see \( G \times H \) as a subgroup of \( \text{Sym} \frac{2^m+1}{m+1} \) where for \( (g,h) \in G \times H \), \( x \in X_1 \) and \( y \in X_2 \) we have: \( (g,h)x = gx \) and \( (g,h)y = hy \). The notation \( X_1 \) and \( X_2 \) will be used throughout this chapter.

Proof of 4.3. For \( m = 0 \), we can take \( H_0 = \text{Sym} 1 \). This chain satisfies the needed conditions trivially. Now suppose \( m \geq 1 \) and we have a chain \( H_0 \subset \ldots \subset H_m \subset \text{Sym} \frac{2^m}{m} \) with all the above properties. I want to create a chain which has \( m+1 \) inclusions. Define \( G_0 = H_0 \times H_m \) and define \( G_{i+1} = N(G_i) \). I claim that the chain \( G_0 \subset \ldots \subset G_{m+1} \subset \text{Sym} \frac{2^m}{m+1} \) satisfies the needed conditions. Conditions 1 and 5 trivially hold.

First I will show \( N(H_i \times H_m) = H_{i+1} \times H_m \) for \( 0 \leq i < m \). The following fact about orbits is very useful: if \( Y \subset X \) is an orbit of \( H \subset \text{Sym} X \), then for each \( \alpha \in \text{Sym} X \) the set \( \alpha(Y) \) is an orbit of \( \alpha H \alpha^{-1} \). In particular, \( N(H) \) permutes the orbits of \( H \). Let \( \alpha \in N(H_i \times H_m) \). Since \( H_m \) is transitive, we see that \( X_2 \) is an orbit of \( H_i \times H_m \). Using the fact above, we see that \( \alpha(X_2) \) is an orbit of \( H_i \times H_m \). However, \( H_i \) does not act transitively on \( \frac{2^m}{m} \) so \( H_i \times H_m \) has exactly one orbit of size \( \frac{2^m}{m} \), which is \( X_2 \). Therefore \( \alpha(X_2) = X_2 \). Since \( X_1 \) is the complement of \( X_2 \) in \( \frac{2^m+1}{m+1} \), we also have \( \alpha(X_1) = X_1 \). We see that \( \alpha \) must be contained in \( \text{Sym} X_1 \times \text{Sym} X_2 \). If we write \( \alpha = (g,h) \), we have \( H_i \times H_m = \alpha^{-1}(H_i \times H_m) \alpha = g^{-1}H_i g \times h^{-1}H_m h \). So \( \alpha \in N(H_i) \times N(H_m) \). But by induction we know that this equals \( H_{i+1} \times H_m \). So we know \( G_i = H_i \times H_m \) for \( i \leq m \).

To show that the other conditions hold it is useful to give an explicit form of \( G_{m+1} \). Denote \( \gamma = \prod_{i=0}^{2^m-1}(i + 2^m) \in \text{Sym} \frac{2^m+1}{m+1} \), which is an element that switches \( X_1 \) and \( X_2 \). Note that \( \gamma \) normalizes \( G_m \), hence \( \gamma \in G_{m+1} \). I will show \( G_{m+1} = G_m \cup \gamma G_m \). This proves that \( G_{m+1} \) is isomorphic to \( H_m \wr \text{Sym} 2 \).

Let \( \alpha \in G_{m+1} \). Again, \( \alpha(X_2) \) is an orbit of \( G_m \), but now we have two possibilities: \( \alpha(X_2) \) can be either \( X_1 \) or \( X_2 \). Suppose \( \alpha(X_2) = X_2 \). Then \( \alpha \in \text{Sym} X_1 \times \text{Sym} X_2 \), and using the same argument as before we have \( \alpha \in G_m \). Suppose \( \alpha(X_2) = X_1 \). Define \( \beta = \gamma \alpha \). So
now $\beta$ satisfies $\beta(X_1) = X_1$ and $\beta(X_2) = X_2$. Again using the same argument as before, we see that $\beta \in G_m$. Since $\gamma^2 = 1$, we have $\alpha = \gamma \beta$.

From the induction hypothesis it is clear that $|G_{i+1} : G_i| = 2$ for $i < m$. From the above, it is clear that this also holds for $i = m$. Therefore condition 4 is proven. Also $G_{m+1}$ acts transitively on $\mathbb{Z}^{m+1}$ and $G_i$ for $i < m$ does not, which proves condition 3. I will now show condition 2. Let $\alpha \in N(G_{m+1})$. Since $G_{m+1}$ is transitive, we can take $\delta \in G_{m+1}$ such that $\alpha(0) = \delta(0)$. Define $\beta = \delta^{-1} \alpha$, which stabilizes $0$.

For any set $X$ and subgroup $K \subset \text{Sym } X$ denote $(K)_x$ as the subgroup of all elements which stabilize $x \in X$. The following holds:

$$\beta \in (\text{Sym } \mathbb{Z}^{m+1})_0 \cap N(G_{m+1})$$
$$\subset N((\text{Sym } \mathbb{Z}^{m+1})_0) \cap N(G_{m+1})$$
$$\subset N((\text{Sym } \mathbb{Z}^{m+1})_0 \cap G_{m+1})$$
$$= N((G_{m+1})_0).$$

All elements of $G_0$ stabilize 0, therefore $G_0 \subset (G_{m+1})_0$. From condition 4 follows $|G_{m+1} : G_0| = 2^{m+1}$. Since $G_{m+1}$ is transitive, we see that $G_{m+1}/(G_{m+1})_0$ is in bijective correspondence to $\mathbb{Z}^{m+1}$. Hence the index of $(G_{m+1})_0$ is $2^{m+1}$. Therefore $G_0 = (G_{m+1})_0$. This shows that $\beta$ is contained in $G_1$. Hence $\beta \in G_{m+1}$ and also $\alpha \in G_{m+1}$. This shows $N(G_{m+1}) = G_{m+1}$.

Conditions 6 and 7 are left as an exercise for the reader.

Proof of 4.1. Let $m \in \mathbb{Z}_{\geq 0}$ and $T$ a simple non-abelian group. Take a chain of subgroups $H_0 \subset \ldots \subset H_m \subset \text{Sym } \mathbb{Z}^{m}$ as in theorem 4.3. I will show that $(\text{Aut } T) \wr H_0$ satisfies the theorem.

From 3.1, 4.3.1 and 4.3.2, it follows that for $i \leq m$ holds $\text{Aut}^i((\text{Aut } T) \wr H_0) = (\text{Aut } T) \wr H_i$ and for $i \geq m$ holds $\text{Aut}^i((\text{Aut } T) \wr H_0) = (\text{Aut } T) \wr H_m$. Hence $(\text{Aut } T) \wr H_0$ has height at most $m$. Suppose $(\text{Aut } T) \wr H_i \cong (\text{Aut } T) \wr H_j$ for some $i$ and $j$. One can extend theorem 3.2, with an almost identical proof, to get the following theorem: let $S$ be a perfect semi-simple group. Let $G_1, G_2 \subset \text{Aut } S$ be subgroups with $\theta_S(S) \subset G_1, G_2$. Then the following map is a bijection:

$$\psi : \{\sigma \in \text{Aut } S | \sigma G_1 \sigma^{-1} = G_2\} \rightarrow \{f \in \text{Hom}(G_1, G_2) | f \text{ is an isomorphism}\},$$
$$\sigma \mapsto (x \mapsto \sigma x \sigma^{-1}).$$

Denote $S = T(\mathbb{Z}^{m})$. For all $k$ we have $\theta(S) \subset (\text{Aut } T) \wr H_k \subset \text{Aut } S$, hence we can use the extended version. Since $(\text{Aut } T) \wr H_i$ and $(\text{Aut } T) \wr H_j$ are isomorphic, we see that they are conjugate subgroups of $\text{Aut } S$. Therefore $H_i$ and $H_j$ are also conjugate. From cardinality follows $i = j$. From theorem 3.2 follows $Z((\text{Aut } T) \wr H_0) \subset \ker \psi = 1$. Hence $(\text{Aut } T) \wr H_0$ has a trivial center. Note that $\theta_{(\text{Aut } T)\wr H_m}$ is an isomorphism, since this is exactly $\psi$ from theorem 3.2.

Proof of 4.2. For $m \geq 0$ and $0 \leq i \leq m$ denote $G_{i,m}$ as the $i$-th subgroup in the normalizer chain of length $m$ as in 4.3. For $k \in \mathbb{Z}_{\geq 0}$ define $\Gamma_k = \prod_{m \geq k} G_{m,m}$. For $k \in \mathbb{Z}_{\geq 0}$ denote $H_k = G_{k,k} \times \Gamma_k$ as a subgroup of $\text{Sym } \mathbb{Z}^{\geq 0}$.

Claim 4.4. Let $i \in \mathbb{Z}_{\geq 0}$. Then $N(H_i) = H_{i+1}$.

Claim 4.5. The center of $(\text{Aut } T) \wr H_0$ is trivial.
5 Automorphism tower of p-adic integers

Theorem 1.3 is a direct consequence of theorem 5.2.

Theorem 5.1. Let \( p \) be a prime and \( G \) a group. Then the following are equivalent:

1. \( G \cong B \times \psi \mathbb{Z}_p \) for some finite group \( B \) and some homomorphism \( \psi : \mathbb{Z}_p \to \text{Aut} \, B \).
2. there exists a surjective homomorphism \( \varphi : \mathbb{Z}_p \to \mathbb{Z}/n \mathbb{Z} \), with a finite kernel, \( n \)
3. \( G \) is isomorphic to a subgroup of finite index of \( C \times \mathbb{Z}_p \) for some finite group \( C \).

Theorem 5.2. If \( G \) satisfies (1)-(3) from theorem 5.2, then so does \( \text{Aut} \, G \).

Lemma 5.3. Let \( G \) be a group with \( |[G,G]| < \infty \). Then there exists \( m \in \mathbb{Z}_{>0} \) such that for all \( g \in G \) holds \( g^m \in Z(G) \).

Proof. I use the notation \( [a,b] = aba^{-1}b^{-1} \). Note \( \#\{[a,b] | a,b \in G\} < \infty \). Denote \( G^g = \{hgh^{-1} | h \in G\} \). Let \( g \in G \), then we have:

\[
\#G^g = \#G \cdot g^{-1} = \#\{[x,g] : x \in G\} \leq \#G, G.
\]

For convenience, denote \( n = \#G, G \). Consider the following exact sequence:

\[
1 \longrightarrow Z(G) \longrightarrow G \longrightarrow \prod_{x \in G} \text{Sym}^{G,G}x.
\]

Note that, for all \( x \), \( G \) acts on \( ^Gx \) by conjugation, which gives us a map \( G \to \text{Sym}^{G,G}x \). This way we get the map in the exact sequence. Now we know \( \#G \leq n \), therefore we see that the exponent of \( \prod_{x \in G} \text{Sym}^{G,G}x \) divides \( n! \). Now it is clear that \( G/Z(G) \) has finite exponent since \( \prod_{x \in G} \text{Sym}^{G,G}x \) has finite exponent.

In the proofs of the theorems 5.1 and 5.2, I need quite a lot of properties of \( \mathbb{Z}_p \). The focus in this thesis lies on understanding automorphism towers, not on working out details of properties of \( \mathbb{Z}_p \). I will state the needed properties of \( \mathbb{Z}_p \) as lemmas. Readers familiar with \( \mathbb{Z}_p \) will most likely know them, other readers can use them as an exercise.

Lemma 5.4. Let \( p \) be prime. We have \( \text{Aut} \, \mathbb{Z}_p \cong \mathbb{Z}_p^* \).

Lemma 5.5. Let \( p \) be a prime and \( H \subseteq \mathbb{Z}_p \) be a subgroup of finite index. Then \( H \) is of the form \( p^m \mathbb{Z}_p \) with \( m \in \mathbb{Z}_{\geq 0} \), which is isomorphic to \( \mathbb{Z}_p \).

Lemma 5.6. Let \( p \) be a prime and \( n \in \mathbb{Z}_{\geq 0} \). Then \( \mathbb{Z}_p / p^n \mathbb{Z}_p \cong \mathbb{Z}/p^n \mathbb{Z} \).

Lemma 5.7. Let \( p \) be a prime. Then \( \mathbb{Z}_p \) consists of exactly all elements of \( \mathbb{Z}_p \) that are not divisible by \( p \). Also \( \mathbb{Z}_2^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z} \) and for \( p > 2 \) we have \( \mathbb{Z}_p^* \cong \mathbb{Z}_p \oplus \mathbb{Z}/(p-1)\mathbb{Z} \).

Lemma 5.8. Let \( p \) be a prime and \( m \in \mathbb{Z}_{\geq 0} \). Then \( p^m \mathbb{Z}_p \) is a characteristic subgroup of \( \mathbb{Z}_p \).

The following lemma is somewhat trivial, but will be used throughout the proofs.

Lemma 5.9. Let \( A \subseteq B \) and \( C \) be groups with \( |B:A| < \infty \) and \( f : B \to C \) a surjective group homomorphism. Then \( |C : f(A)| < \infty \).
Proof. Left as an exercise for the reader. □

Proof of theorem 5.1. (1) ⇒ (3). Define $C = B \rtimes \psi$. Let $B$ where $\psi' = \text{id}_{\text{Aut}B}$. Clearly the map $f : G \to C \times \mathbb{Z}_p, (b, x) \mapsto (b, \varphi(x), x)$ is an injective homomorphism. Note that since $B$ is finite, $\text{Aut}B$ is finite. Therefore $C$ is finite. Note that $C \times 0$ is a complete set of representatives of all cosets of $f(G)$ in $C \times \mathbb{Z}_p$. So $f(G)$ has finite index in $C \times \mathbb{Z}_p$.

(3) ⇒ (2). Let $\pi : C \times \mathbb{Z}_p \to \mathbb{Z}_p$ be the projection map. Since $G$ is a subgroup of $C \times \mathbb{Z}_p$ of finite index, it follows from lemma 5.9 that $\pi(G)$ is also of finite index in $\mathbb{Z}_p$. But by lemma 5.5 we see that $\pi(G)$ is isomorphic to $\mathbb{Z}_p$. So there exists a surjective map from $G$ to $\mathbb{Z}_p$. Note that $\ker \pi \cong C$, which is finite.

(2) ⇒ (1). Let $\varphi : G \to \mathbb{Z}_p$ be a surjective map. I will be taking restrictions of the domain and codomain of $\varphi$ very often. To avoid impractical notation, I will only use the restriction of the domain in the notation. It should be clear from the context what the codomain should be. We have the following short exact sequence:

$$1 \longrightarrow \ker(\varphi) \longrightarrow G \xrightarrow{\varphi} \mathbb{Z}_p \longrightarrow 0.$$ 

I want to find a subgroup of $G$ that is isomorphic to $\mathbb{Z}_p$, where a restriction of $\varphi$ is this isomorphism. If we can do this, we can use lemma 2.3 to get the needed result. Note that $G/\ker(\varphi)$ is abelian, hence $[G, G] \subseteq \ker(\varphi)$. The kernel of $\varphi$ is finite, hence $|[G, G]| < \infty$. From lemma 5.3, we can pick $m \in \mathbb{Z}_{>0}$ such that for all $g \in G$ holds $g^m \in Z(G)$. Now define $H = \langle \{g^m | g \in G \} \rangle$, which is a subgroup of $Z(G)$. We get the following short exact sequence:

$$1 \longrightarrow \ker(\varphi) \cap H \longrightarrow H \xrightarrow{\varphi|_H} m\mathbb{Z}_p \longrightarrow 0.$$ 

Denote by $k$ the exponent of $\ker(\varphi) \cap H$ and $H^k = \{h^k | h \in H \}$. Note that $H^k$ is a group since $H$ is abelian. We see that $\varphi|_{H^k} : H^k \to mk\mathbb{Z}_p$ is surjective and I will show that $\varphi|_{H^k}$ is also injective. Let $h^k \in H^k$ and suppose $\varphi|_{H^k}(h^k) = 0$. Note that $\mathbb{Z}_p$ is torsion-free, therefore $\varphi|_{H^k}(h) = 0$. We can conclude $h \in \ker(\varphi) \cap H$. Since $k$ was exactly the exponent of this group, we have $h^k = 0$. Thus $\varphi|_{H^k}$ is injective. This shows $H^k \cong mk\mathbb{Z}_p$, where a restriction of $\varphi$ is this isomorphism.

Let $\gamma \in G$ such that $\varphi(\gamma) = 1$. Write $mk = p^n \cdot l$ with $p \nmid l$ and $n \in \mathbb{Z}_{>0}$. For convenience, denote $\varphi|_{\langle \gamma^l \rangle \cdot H^k}$ instead of $\varphi|_{\langle \gamma \rangle \cdot H^k}$. From lemma 5.7 follows that $\mathbb{Z}_p$ is equal to $\mathbb{Z}_p$ and from lemma 5.6 we can conclude $\mathbb{Z}_p/mk\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$. We have the following diagram:

$$\begin{array}{cccccc}
0 & \longrightarrow & H^k & \longrightarrow & \langle \gamma^l \rangle \cdot H^k & \longrightarrow & \langle \gamma^l H^k \rangle \\
& \downarrow{\varphi|_{H^k}} & \downarrow{\varphi} & & \downarrow{f} & & 0 \\
0 & \longrightarrow & mk\mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p & \xrightarrow{\pi} & \mathbb{Z}/p^n\mathbb{Z} \\
\end{array}$$ 

Note $\langle \gamma^l H^k \rangle \subset G/H^k$. Define $f$ by lifting an element to $\langle \gamma^l \rangle \cdot H^k$ and then applying $\pi \circ \varphi|$. If $a, b \in \langle \gamma^l \rangle \cdot H^k$ are two different lifts, then $a - b \in H^k$. Using exactness and that the left square commutes we have $\pi(\varphi(a) - \varphi(b)) = 0$. This shows that $f$ is well-defined. Note that $\gamma^l$ is a lift of the coset $\gamma^l H^k$. Also $\varphi|_{\langle \gamma^l \rangle}$ is a generator of $\mathbb{Z}/p^n\mathbb{Z}$ because $p \nmid l$, hence $f$ is surjective. Also note that $\langle \gamma^l H^k \rangle$ has at most $p^n$ elements since $\gamma^p \cdot l = \gamma^{mk} \in H^k$. Since $f$ is surjective and $\mathbb{Z}/p^n\mathbb{Z}$ has $p^n$ elements, it must be an isomorphism.

The short five lemma states that if the diagram commutes, the two rows are short exact sequences and the maps $\varphi|_{H^k}$ and $f$ are isomorphisms, then so is $\varphi|$. All these conditions are true, hence $\varphi|_{H^k}$ is also an isomorphism. Define $g : \mathbb{Z}_p \to G$ as the map $\varphi^{-1}$ with a
bigger codomain. We have \( g \varphi = \text{id}_{Z_p} \), thus from lemma 2.3 follows that \( G \) is isomorphic to \( \ker(\varphi) \rtimes Z_p \). \[ \square \]

In the next proof I use a little bit of group cohomology. The following two definitions will cover everything I need.

**Definition 5.10.** Let \( G \) be a group, \( M \) an abelian group and \( \psi : G \times M \to M \) a map. We say that \( M \) is a left \( G \)-module if \( \psi \) is a left group action from \( G \) on \( M \) such that for all \( g \in G, a, b \in M \) we have \( g(a + b) = ga + gb \), where \( ga \) denotes \( \psi(g, a) \).

**Definition 5.11.** Let \( G \) be a group and \( M \) a left \( G \)-module. A crossed homomorphism or 1-cocycle is a map \( f : G \to M \) such that for all \( g, h \in G \) holds \( f(gh) = f(g) + gf(h) \). The abelian group of crossed homomorphisms is denoted \( Z^1(G, M) \).

**Proof of 5.2.** Since \( G \) satisfies (1), we can take \( B \) such that \( G \cong B \rtimes \mathbb{Z}_p \). It is enough to show that there exists a surjective homomorphism \( \text{Aut}(B \rtimes \mathbb{Z}_p) \to \mathbb{Z}_p \) with finite kernel.

Note that \( B \) is a characteristic subgroup of \( G \), since \( B \) is the set of torsion elements of \( G \), and \( G/B \cong \mathbb{Z}_p \). Let \( \sigma \in \text{Aut} G \). Note that \( \sigma G / B \to G / B, g \mapsto \sigma(g) \) is a well-defined automorphism. This shows that we have a map \( f_1 : A \to \text{Aut} \mathbb{Z}_p \). I will now show that the image of \( f_1 \) has finite index in \( \text{Aut} \mathbb{Z}_p \). I will do this by showing that the subgroup \( H := \{ \alpha \in \text{Aut} \mathbb{Z}_p : \psi \alpha = \psi \} \) has finite index in \( \text{Aut} \mathbb{Z}_p \) and is contained in \( \text{Im}(f_1) \).

From lemma 5.8 we have the canonical map \( \gamma_n : \text{Aut} \mathbb{Z}_p \to \text{Aut} (\mathbb{Z}_p / p^n \mathbb{Z}_p) \). Write \( |\text{Aut} B| = p^m \cdot l \) with \( p \nmid l \) for some \( m \in \mathbb{Z}_{\geq 0} \). Let \( \alpha \in \ker(\gamma_m) \). We have that the following diagram commutes, where \( \overline{\psi} \) is defined such that the right triangle commutes:

\[
\begin{array}{ccc}
\mathbb{Z}_p & \xrightarrow{\alpha} & \mathbb{Z}_p \\
\downarrow{\pi} & & \downarrow{\pi} \\
\mathbb{Z}_p / p^n \mathbb{Z}_p & \xrightarrow{\text{id}} & \mathbb{Z}_p / p^n \mathbb{Z}_p \\
\end{array}
\]

From this follows \( \ker(\gamma_m) \subset H \). Clearly \( \ker(\gamma_m) \) has finite index in \( \text{Aut} \mathbb{Z}_p \), hence \( H \) has finite index in \( \text{Aut} \mathbb{Z}_p \) as well. For \( \alpha \in H \) we can define \( g_\alpha : G \to G, (b, x) \mapsto (b, \alpha(x)) \). From \( \psi \alpha = \psi \) follows that \( g_\alpha \) is an automorphism. Since \( \alpha \) is an automorphism, \( g_\alpha \) is as well. We can now conclude \( H \subset \text{Im}(f_1) \), which shows that \( \text{Im}(f_1) \) has finite index in \( \text{Aut} \mathbb{Z}_p \).

I will now show that the kernel of \( f_1 \) is finite. Define \( \gamma : \ker(f_1) \to \text{Aut} B, \sigma \mapsto \sigma|_B \). We have the following exact sequence:

\[
0 \longrightarrow \ker(\gamma) \overset{}{\longrightarrow} \ker(f_1) \overset{\gamma}{\longrightarrow} \text{Aut} B.
\]

Note that for any exact sequence of groups \( G_1 \to G_2 \to G_3 \) holds that if both \( G_1 \) and \( G_3 \) are finite, then so is \( G_2 \). Hence it is enough to show that \( \ker(\gamma) \) is finite. Let \( \sigma \in \ker(\gamma) \), so we have \( \sigma|_B = \text{id}_B \). Since \( \ker(\gamma) \subset \ker(f_1) \), we have that by definition of \( f_1 \) the following diagram commutes:

\[
\begin{array}{ccc}
0 & \to & B \\
\downarrow{\text{id}} & & \downarrow{\sigma} \\
G & \xrightarrow{\pi} & \mathbb{Z}_p \\
\downarrow{\text{id}} & & \downarrow{\text{id}} \\
0 & \to & B \\
\end{array}
\]

Note that the rows are exact since \( G / B \cong \mathbb{Z}_p \). Define \( \alpha : G \to B, x \mapsto \sigma(x)x^{-1} \). The map
α is not necessarily a group homomorphism. It is well-defined, since we have:

\[ \sigma(x)x^{-1} \in B \Leftrightarrow \pi(\sigma(x)x^{-1}) = 0 \]
\[ \Leftrightarrow \pi(\sigma(x)) = \pi(x). \]

The last statement is true since the diagram above commutes. Clearly \( \sigma(x) = \alpha(x)x \), so if I can show that there are at most finitely many \( \alpha \) we are done. Let \( x \in G \) and \( y \in B \). Since \( \sigma \) is the identity on \( B \), we have:

\[ \alpha(xy) = \sigma(x)\sigma(y)y^{-1}x^{-1} = \sigma(x)x^{-1} = \alpha(x). \]

Note \( xy \in Bx = xB \) since \( B \) is normal in \( G \). Therefore \( \alpha(xy) = \alpha(x) \). From this follows:

\[ \alpha(x) = \alpha(yx) = \sigma(y)\alpha(x)y^{-1} = y\alpha(x)y^{-1}. \]

This proves \( \alpha(x) \in Z(B) \). Combining the above, we have a map \( \overline{\alpha} : \mathbb{Z}_p \rightarrow Z(B) \). Since \( \overline{\alpha} \) and \( \alpha \) correspond bijectively (follows from universal property), I only need to show there are only finitely many maps like \( \overline{\alpha} \). Define the following action of \( \mathbb{Z}_p \) on \( Z(B) \): for \( a \in \mathbb{Z}_p \) and \( b \in Z(B) \) pick the lift \( (1, a) \in G \). Define \( a \cdot b = (1, a)(b, 0)(1, -a) \) and \( \varphi : \mathbb{Z}_p \rightarrow Aut \mathbb{Z}(B) \) as the map corresponding to this action. I will denote \( a^b = a \cdot b \) to be consistent with previous notation. Note that \( a^b \) is contained in \( Z(B) \) because \( \varphi \) is the composition of \( \psi \) and the restriction map \( Aut B \rightarrow Aut Z(B) \), which exists because \( Z(B) \) is characteristic in \( B \). To avoid confusion, I will denote \( Z(B) \) multiplicatively. Let \( (1, a), (1, b) \in G \). Note \( \overline{\alpha}(a) = \alpha(1, a) \). Then we have:

\[ \overline{\alpha}(a + b) = \alpha(1, a + b) \]
\[ = \sigma(1, a)\sigma(1, b)(1, -a - b) \]
\[ = \sigma(1, a)(1, -a)(1, a)\sigma(1, b)(1, -b)(1, -a) \]
\[ = \alpha(1, a). (1,a) \alpha(1, b) \]
\[ = \overline{\alpha}(a)^a \overline{\alpha}(b). \]

So we see \( \overline{\alpha} \in Z^1(\mathbb{Z}_p, Z(B)) \). I need to prove that \( Z^1(\mathbb{Z}_p, Z(B)) \) is finite. Since \( Aut Z(B) \) is finite, we see that the kernel of \( \varphi \) must be a subgroup of finite index in \( \mathbb{Z}_p \). Thus by lemma 5.5 we can take \( m \in \mathbb{Z}_{\geq 0} \) such that \( \ker(\varphi) = p^m \mathbb{Z}_p \). We have the following exact sequence:

\[ 0 \longrightarrow p^m \mathbb{Z}_p \overset{\varphi}{\longrightarrow} \mathbb{Z}_p \overset{\varphi}{\longrightarrow} Aut Z(B). \]

We see that the action of \( p^m \mathbb{Z}_p \) on \( Z(B) \) is trivial, hence \( \overline{\alpha}(a + b) = \overline{\alpha}(a)\overline{\alpha}(b) \) for \( a, b \in p^m \mathbb{Z}_p \). This proves \( Z^1(p^m \mathbb{Z}_p, Z(B)) = \text{Hom}(p^m \mathbb{Z}_p, Z(B)) \), which is finite. Define \( r : Z^1(\mathbb{Z}_p, Z(B)) \rightarrow \text{Hom}(p^m \mathbb{Z}_p, Z(B)) \), \( f \mapsto f|_{p^m \mathbb{Z}_p} \). We have the following exact sequence:

\[ 0 \longrightarrow \ker(r) \overset{\varphi}{\longrightarrow} Z^1(\mathbb{Z}_p, Z(B)) \overset{r}{\longrightarrow} \text{Hom}(p^m \mathbb{Z}_p, Z(B)). \]

Let \( f \in \ker(r) \). Let \( a \in \mathbb{Z}_p \) and \( x \in p^m \mathbb{Z}_p \). We have:

\[ f(a + x) = f(a) \cdot a f(x) \]
\[ = f(a) \cdot a 1 \]
\[ = f(a). \]

The second equality holds because \( f \) was trivial on \( p^m \mathbb{Z}_p \). Thus we can define the map \( \overline{r} : \mathbb{Z}_p/p^m \mathbb{Z}_p \rightarrow Z(B) \) which is contained in \( Z^1(\mathbb{Z}_p/p^m \mathbb{Z}_p, Z(B)) \). This proves \( |\ker(r)| \leq \)
$|Z^1(\mathbb{Z}/p^n\mathbb{Z}, Z(B))|$. From lemma 5.6 we know that $\mathbb{Z}/p^n\mathbb{Z}$ is finite. Since $Z(B)$ is as well, we see that $Z^1(\mathbb{Z}/p^n\mathbb{Z}, Z(B))$ must be finite and $\ker(r)$ is finite as well.

Since we have an exact sequence where both $\ker(r)$ and $\text{Hom}(p^n\mathbb{Z}, Z(B))$ are finite, we see that $Z^1(\mathbb{Z}, Z(B))$ is finite. This proves that there are only finitely many $\alpha$, thus only finitely many $\alpha$ and thus $\ker(f_1)$ is finite.

By lemma 5.4 and 5.7, we have a surjective map with finite kernel $f_2 : \text{Aut} \mathbb{Z}/p \to \mathbb{Z}/p$. Using lemma 5.9, we see that the image of $f_2 \circ f_1$ has finite index in $\mathbb{Z}/p$. Now using lemma 5.5, this is isomorphic to $\mathbb{Z}/p$. Call the isomorphism $f_3$. Now $f_3 \circ f_2 \circ f_1$ is a surjective map. Each $f_i$ has a finite kernel, hence the composition has finite kernel as well. 

\[ \square \]

### 6 Automorphism groups of finite products of abelian groups

Let $\mathcal{C}$ be a category. Denote $\mathcal{C}_0$ as the collection of objects and $\mathcal{C}_1$ as the collection of morphisms. Let $X, Y \in \mathcal{C}_0$, I denote $\mathcal{C}(X, Y)$ as the set of morphisms from $X$ to $Y$ and $\text{Aut} X$ as the set of invertible morphisms from $X$ to $X$.

**Definition 6.1.** Let $\mathcal{C}$ be a category. Then $\mathcal{C}$ is an additive category if for each $X, Y \in \mathcal{C}_0$ we have that $\mathcal{C}(X, Y)$ is an abelian group, composition is bilinear and $\mathcal{C}$ has all finite products.

**Theorem 6.2.** Let $\mathcal{C}$ be an additive category, $I$ a finite set and let $X_i \in \mathcal{C}_0$ for each $i \in I$. Denote $Z = \prod_{i \in I} X_i$. Then $B = \prod_{i,j \in I} \mathcal{C}(X_j, X_i)$ is a ring where addition is coordinate wise and multiplication is defined as

\[
(f_{ij})_{i,j \in I} \cdot (g_{ij})_{i,j \in I} := \left( \sum_{k \in I} f_{ik} \circ g_{kj} \right)_{i,j \in I},
\]

where we have $(f_{ij})_{i,j \in I}, (g_{ij})_{i,j \in I} \in B$ with $f_{ij}, g_{ij} \in \mathcal{C}(X_j, X_i)$. Also, $\mathcal{C}(Z, Z)$ is a ring, with composition as multiplication, which is isomorphic as a ring to $B$. And $\text{Aut} Z$ and $B^*$ are isomorphic as groups.

The operations of $B$ are similar to the matrix operations. I will call $B$ the matrix ring over $(X_i)_{i \in I}$, and its elements are called matrices.

**Theorem 6.3.** Let $\mathcal{C}$ be an additive category, $I$ a finite set and let $X_i \in \mathcal{C}_0$ for each $i \in I$. Then $\text{Aut}(\prod_{i \in I} X_i)$ is abelian iff the following statements hold:

1. $\forall i \in I : \text{Aut} X_i$ is abelian,
2. $\forall i,j \in I, i \neq j, f \in \text{Aut} X_i : (\forall g \in \mathcal{C}(X_j, X_i) : fg = g) \land (\forall g \in \mathcal{C}(X_i, X_j) : gf = g)$,
3. $\forall i,j,k \in I, i \neq k \neq j : \mathcal{C}(X_k, X_j)\mathcal{C}(X_i, X_k) = 0$.

Also if $\text{Aut}(\prod_{i \in I} X_i)$ is abelian, then holds:

\[
\text{Aut} \left( \prod_{i \in I} X_i \right) \cong \left( \prod_{i \in I} \text{Aut} X_i \right) \Pi \left( \prod_{i \neq j \in I} \text{Hom}(X_i, X_j) \right).
\]

I want to emphasize that I did not make a mistake in 6.3.3, I do allow $i = j$.

Products and coproducts are equal in additive categories, see [3] page 196. This is needed in the following lemma.
Lemma 6.4. Let \( \mathcal{C} \) be an additive category, \( I \) a finite set and let \( X_i \in \mathcal{C}_0 \) for each \( i \in I \). Denote \( Z = \prod_{i \in I} X_i \), \( \pi_i : Z \to X \) the projections and \( p_i : Z \to X \) the coprojections. Let \( Y \in \mathcal{C}_0 \). Then \( \varphi : \mathcal{C}(Y,Z) \to \prod_{i \in I} \mathcal{C}(Y,X_i) \), \( f \mapsto (\pi_i \circ f)_{i \in I} \) and \( \varphi' : \mathcal{C}(Z,Y) \to \prod_{i \in I} \mathcal{C}(X_i,Y) \), \( f \mapsto (f \circ p_i)_{i \in I} \) are isomorphisms.

**Proof.** Note that since composition is bilinear, we see that \( \varphi \) is actually a group homomorphism. If we are given \( (f_i)_{i \in I} \in \prod_{i \in I} \mathcal{C}(Y,X_i) \), then by the categorical definition of the product we get a unique map \( f : Y \to Z \) such that for each \( i \in I \) we have \( f_i = \pi_i \circ f \). It is clear by this condition that mapping such a collection to the unique map is the inverse of \( \varphi \). The proof that \( \varphi' \) is an isomorphism is very similar. \( \Box \)

**Proof of theorem 6.2.** Let \( f \in \mathcal{C}(Z,Z) \). By applying lemma 6.4, we see that \( f \) corresponds bijectively to the family \( (f_{ij} : X_j \to X_i)_{i,j \in I} \). Define \( \Phi : \mathcal{C}(Z,Z) \to B, f \mapsto (f_{ij})_{i,j \in I} \). It is clear that \( \Phi \) is a group isomorphism. Also \( \Phi \) respects composition, which can be verified by working out the definition. Thus \( \Phi \) is a ring isomorphism, from which it also follows that \( B \) is a ring. In particular, invertible elements are mapped to invertible elements. This means \( \mathcal{C}(Z,Z)^* \) and \( B^* \) are isomorphic, where the isomorphism is \( \Phi \) with restricted domain and codomain. Note that \( \mathcal{C}(Z,Z) \) is actually \( \mathcal{C}(Z,Z)^* \). \( \Box \)

**Proof of theorem 6.3.** Let \( B \) be the matrix ring over \( (X_i)_{i \in I} \). We know from theorem 6.2 that \( B^* \) is isomorphic to \( \text{Aut}(\prod_{i \in I} X_i) \). In the proof I will only use \( B^* \) instead of \( \text{Aut}(\prod_{i \in I} X_i) \). Note that if \( I \) is empty or contains exactly one element, the theorem is trivial. Assume \( |I| \geq 2 \) for the rest of the proof.

\( \Rightarrow \). I will prove the statements in order. I will constantly be defining elements of \( B \), which I do by defining what they are on each “coordinate” \((i,j)\). Whenever I do so, I will only specify what is different from the identity element (identity morphisms on the diagonal and zero elsewhere). This saves a lot of words. I will also be redefining \( a \) and \( b \) in every part, so they “reset” after a statement is done proving.

1. Let \( i \in I \) and \( f,g \in \text{Aut} X_i \). Define \( a,b \in B^* \) as the elements with \( a_{ii} = f \) and \( b_{ii} = g \). Now \( B^* \) is assumed to be abelian, so we have \( fg = (ab)_{ii} = (ba)_{ii} = gf \). This shows that \( \mathcal{C}(X_i,X_i)^* \) is abelian.

2. Let \( i,j \in I \) with \( i \neq j \), \( f \in \text{Aut} X_i \) and \( g \in \mathcal{C}(X_i,X_j) \). Redefine \( a,b \in B^* \) as elements with \( a_{ii} = f \) and \( b_{jj} = g \). Now \( gf = (ba)_{ji} = (ab)_{ji} = g \). The other statement has an analogous proof.

3. Let \( i,j,k \in I \) with \( i \neq k \neq j \). Let \( f \in \mathcal{C}(X_k,X_j) \) and \( g \in \mathcal{C}(X_i,X_k) \). Redefine \( a,b \in B^* \) as elements with \( a_{jk} = f \) and \( b_{ki} = g \). Now if \( i \neq j \) we have \( fg = (ab)_{ji} = (ba)_{ji} = 0 \). If \( i = j \) we have \( id + fg = (ab)_{ii} = (ba)_{ii} = id \), which also implies \( fg = 0 \).

\( \Leftarrow \). Let \( a,b \in B^* \). Write \( a = (a_{ij})_{i,j \in I} \) and \( b = (b_{ij})_{i,j \in I} \) with \( a_{ij},b_{ij} \in \mathcal{C}(X_j,X_i) \). Then we have:

\[
(\begin{align*}
(ab)_{ij} &= \sum_{k \in I} a_{ik} \circ b_{kj}, \\
(ba)_{ij} &= \sum_{k \in I} b_{ik} \circ a_{kj}.
\end{align*})
\]

I will need to show that \( ab \) and \( ba \) are equal on each coordinate. From 6.3.3 follows the equality \( (ab)_{ii} = a_{ii}b_{ii} \). From 6.3.1 we get \( (ab)_{ii} = (ba)_{ii} \) for each \( i \in I \). Now take \( i,j \in I \) with \( i \neq j \). We have:

\[
(\begin{align*}
(\begin{align*}
(ab)_{ij} &= \sum_{k \in I} a_{ik}b_{kj} = b_{ij} + a_{ij} + \sum_{k \neq i,j} a_{ik}b_{kj} = b_{ij} + a_{ij}.
\end{align*})
\end{align*})
\]
Note that the second equality holds because of 6.3.2 and the third equality holds because of 6.3.3. Clearly this now must be equal to \((ba)_{ij}\), so \(a\) and \(b\) commute.

The last statement about the isomorphism is obvious when one works out matrix multiplication and uses conditions 1-3 to simplify the result. \(\square\)

7 Abelian automorphism towers for finitely generated abelian groups

Theorem 7.1. Let \(A\) be a finitely generated abelian group. Then \(A\) has an abelian automorphism tower iff \(A\) is cyclic and \(|A|\) is contained in one of the following sets:

a) \(\{3^m, 2 \cdot 3^m | m \in \mathbb{Z}_{\geq 1}\}\)

b) \(\{2 \cdot 3^m + 1, 2(2 \cdot 3^m + 1) | m \in \mathbb{Z}_{\geq 1}, 2 \cdot 3^m + 1 \text{ is prime}\}\)

c) \(\{1, 2, 4, 5, 10, 11, 22, 23, 46, 47, 94\}\)

d) \(\{\infty\}\)

In this chapter I will refer to these four sets as \(X_a, X_b, X_c\) and \(X_d\).

Theorem 7.2. Let \(A\) be a finitely generated abelian group. Then \(\text{Aut} A\) is abelian iff \(A\) is cyclic or \(A \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\).

Proof. \(\Leftarrow\). We have \(\text{Aut}(\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong V_4\) and \(\text{Aut} \mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}\). Let \(n \in \mathbb{Z}_{\geq 1}\) such that \(A \cong \mathbb{Z}/n\mathbb{Z}\). We have \(\text{End} A \cong \mathbb{Z}/n\mathbb{Z}\) (as rings), so clearly \(\text{Aut} A = (\text{End} A)^*\) is abelian.

\(\Rightarrow\). Since \(A\) is finitely generated, we have \(A \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^n \mathbb{Z}/k_i\mathbb{Z}\) with \(k_i | k_{i+1}\), \(r, n \in \mathbb{Z}_{\geq 0}\) and if \(n > 0\) then \(k_1 > 1\).

Suppose \(r > 1\). Then there is an injective map from \(\text{Aut}(\mathbb{Z} \oplus \mathbb{Z})\) into \(\text{Aut} A\). We can now apply theorem 6.3 with \(I = 2\) and \(X_0 = X_1 = \mathbb{Z}\). By statement 6.3.3 must hold \(\text{Hom}(\mathbb{Z}, \mathbb{Z}) \circ \text{Hom}(\mathbb{Z}, \mathbb{Z}) = 0\). Clearly this is not the case, hence \(\text{Aut}(\mathbb{Z} \oplus \mathbb{Z})\) is not abelian. This means \(\text{Aut} A\) cannot be abelian, which is a contradiction. So \(r \leq 1\).

Suppose \(n > 1\). There is an injective map from \(\text{Aut}(\mathbb{Z}/k_1\mathbb{Z} \oplus \mathbb{Z}/ak_1\mathbb{Z})\) to \(\text{Aut} A\), with \(a \in \mathbb{Z}\) such that \(ak_1 = k_2\). Define \(f : \mathbb{Z}/ak_1\mathbb{Z} \to \mathbb{Z}/k_1\mathbb{Z}\) the projection map and define \(g : \mathbb{Z}/k_1\mathbb{Z} \to \mathbb{Z}/ak_1\mathbb{Z}\) as multiplying by \(a\). Now holds: \(gf(1+ak_1\mathbb{Z}) = g(1+k_1\mathbb{Z}) = a+ak_1\mathbb{Z}\). Since \(k_1 > 1\) and \(a > 0\) we have \(gf \neq 0\). By 6.3.3, we see that \(\text{Aut}(\mathbb{Z}/k_1\mathbb{Z} \oplus \mathbb{Z}/ak_1\mathbb{Z})\) is not abelian, and neither is \(\text{Aut} A\). This is a contradiction, so \(n \leq 1\).

If \((r, n)\) is \((0, 0), (1, 0)\) or \((0, 1)\) we see that \(A\) satisfies the theorem. Suppose \((r, n) = (1, 1)\). This means \(A \cong \mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}\) for some \(m \in \mathbb{Z}_{\geq 2}\). Define \(\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}\) the canonical quotient map and \(f \in \text{Aut}(\mathbb{Z}/m\mathbb{Z})\). Now from 6.3.2 follows \(f\pi = \pi\). Since \(\pi\) is surjective, we have that \(f\) is the identity. Thus \(\text{Aut}(\mathbb{Z}/m\mathbb{Z}) = 1\), which implies \(m = 2\). \(\square\)

Definition 7.3. Define \(\lambda : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}\) as a map of sets where \(\lambda(n)\) is the exponent of \((\mathbb{Z}/n\mathbb{Z})^*\). This \(\lambda\) is called the Carmichael function.

Proposition 7.4. Let \(n \in \mathbb{Z}_{\geq 1}\). Then \(\varphi(n) = \lambda(n)\) iff \(n\) equals \(1, 2, 4, p^k\) or \(2p^k\) for an odd prime \(p\) and an integer \(k \in \mathbb{Z}_{\geq 1}\).

Proof. See theorem 7.3 of [4]. \(\square\)

Lemma 7.5. Let \(A\) be a finitely generated abelian group. Then \(\text{Aut} A\) is cyclic iff \(A \cong \mathbb{Z}\) or \(A \cong \mathbb{Z}/n\mathbb{Z}\) with \(\varphi(n) = \lambda(n)\).
Proof. \(\leftarrow\). We have \(\text{Aut} \mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}\). Let \(n \in \mathbb{Z}_{\geq 1}\). Note that \((\mathbb{Z}/n\mathbb{Z})^*\) is isomorphic to \(\text{Aut} \mathbb{Z}/n\mathbb{Z}\). Also \(\varphi(n) = |\text{Aut} \mathbb{Z}/n\mathbb{Z}|\). So we can conclude \(\text{Aut} \mathbb{Z}/n\mathbb{Z}\) is cyclic iff \(\varphi(n) = \lambda(n)\).

\(\Rightarrow\). Since \(\text{Aut} A\) is cyclic, it is certainly abelian. So from theorem 7.2 follows that \(A \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\) or \(A\) is cyclic. We have \(\text{Aut} (\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong V_4\), which is not cyclic. Hence \(A\) must be cyclic. Suppose \(A \not\cong \mathbb{Z}\). Take \(n \in \mathbb{Z}_{\geq 1}\) such that \(A \cong \mathbb{Z}/n\mathbb{Z}\). It is clear from the above that \(\varphi(n) = \lambda(n)\).

\textbf{Lemma 7.6.} Let \(n \in \mathbb{Z}_{\geq 1}\) such that \(\varphi(n) = \lambda(n)\) and \(\varphi(n) \in X_a \cup X_b\). Then \(n \in X_a \cup X_b\).

\textbf{Proof.} From lemma 7.4 follows that \(n\) equals 1, 2, 4, \(p^k\) or \(2p^k\) for an odd prime \(p\) and integer \(k \in \mathbb{Z}_{\geq 1}\). The smallest integer in \(X_a \cup X_b\) is 3 so \(n\) cannot be 1, 2 or 4. Let \(p\) be an odd prime and \(k \in \mathbb{Z}_{\geq 1}\) such that \(n = p^k\) or \(n = 2p^k\). In either case we have \(\varphi(n) = (p-1)p^{k-1}\).

Assume \(\varphi(n) = 2 \cdot 3^m\) with \(m \geq 1\). If \(k > 1\), we see that \(p\) must equal 3 so \(n \in X_a\). Suppose \(k = 1\). There can only be one possible prime such that \(\varphi\) sends it to \(2 \cdot 3^m\) and that is \(2 \cdot 3^m + 1\). So \(n \in X_b\).

Assume \(\varphi(n) = 2q\), where \(q = 2 \cdot 3^m + 1\) is prime and \(m \geq 1\). Suppose \(k > 1\). Then we have \((p-1)p^{k-1} = 2q\). Since there is at least one factor \(p\), we must have \(p = q\). However, also \(p - 1 = 2\) must hold. This is a contradiction. For \(k = 1\) we have \(p - 1 = 2q\). We have: \(2q + 1 = 4 \cdot 3^m + 3\), which is divisible by 3. So \(p\) is not prime, which is a contradiction.

Other cases do not exist, since either \(\varphi(n) = 1\) or \(2 | \varphi(n)\).

\textbf{Proof of theorem 7.1.} \(\leftarrow\). We have \(\text{Aut} \mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}\) and \(\text{Aut}^2 \mathbb{Z} \cong 0\), so \(\mathbb{Z}\) does indeed have an abelian automorphism tower.

Suppose \(A \cong \mathbb{Z}/n\mathbb{Z}\) for \(n = 2 \cdot 3^m\). We have \(\varphi(n) = \lambda(n)\) by proposition 7.4, hence by lemma 7.5 we see that \(\text{Aut} A\) is cyclic. Now \(\varphi(2 \cdot 3^m) = 2 \cdot 3^{m-1}\). We now see that \(\text{Aut}^2 A\) is also cyclic. Since we keep getting powers of 3 multiplied by 2, we keep getting cyclic groups. After \(m+1\) steps, we get the trivial group. Hence \(A\) has an abelian automorphism tower. Note that for any odd integer \(n \in \mathbb{Z}_{\geq 1}\) holds \(\varphi(2n) = \varphi(n)\). Therefore \(\mathbb{Z}/3^m\mathbb{Z}\) also has an abelian automorphism tower.

Suppose \(A \cong \mathbb{Z}/n\mathbb{Z}\) for \(n = 2 \cdot 3^m + 1\) prime. This prime is odd, so it satisfies proposition 7.4. Now \(\varphi(n) = n - 1 = 2 \cdot 3^m\). We have already checked above that a cyclic group of this order has an abelian automorphism tower, hence \(A\) does as well. Since \(n\) is odd, we see that \(\varphi(2n) = \varphi(n)\). So \(\mathbb{Z}/2n\mathbb{Z}\) also has an abelian automorphism tower.

From proposition 7.4 and lemma 7.5 follows that for all \(n \in X_c\) we have \(\text{Aut} \mathbb{Z}/n\mathbb{Z}\) is cyclic. One can also calculate that for all \(n \in X_c\) we have \(|\text{Aut} \mathbb{Z}/n\mathbb{Z}| \in X_c\). Thus \(\mathbb{Z}/n\mathbb{Z}\) has an abelian automorphism tower for \(n \in X_c\).

\(\Rightarrow\). Note \(\text{Aut}^2 (\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \text{Sym} 3\). From theorem 7.2, we can conclude that every group in the automorphism tower of \(A\) is cyclic. Assume \(A \not\cong \mathbb{Z}\). So \(A\) is a finite group and all groups in the automorphism tower of \(A\) must be finite as well. Take \(n \in \mathbb{Z}_{\geq 1}\) such that \(A \cong \mathbb{Z}/n\mathbb{Z}\). We can repeatedly use lemma 7.5 and we get the following statement: for all \(i \geq 0\) holds \(\text{Aut}^i A \cong \mathbb{Z}/\varphi^i(n)\mathbb{Z}\), where \(\varphi^i(n)\) is the \(i\)-th iteration of \(\varphi\). Note \(\varphi^0(n) = n\). We also have that \(\varphi^i(n) = \lambda^i(n)\) for all \(i \geq 0\), again from lemma 7.5.

Let \(n \in \mathbb{Z}_{\geq 1}\) such that for all \(i \geq 0\) holds \(\varphi^i(n) \notin X_a \cup X_b\). To prove this theorem, it is enough to show that \(n\) must be contained in either \(X_a\), \(X_b\) or \(X_c\). Assume \(n \notin X_a \cup X_b\). The cases \(n = 1\) and \(n = 2\) are trivial, so also assume \(n \geq 4\). By repeated use of lemma 7.6, we see that for all \(i \geq 0\) holds \(\varphi^i(n) \notin X_a \cup X_b\). I claim that there exists an \(i \geq 0\)
such that \( \varphi'(n) = 4 \). We know by proposition 7.4, that \( \varphi'(n) \) must be 4, \( p^k \) or \( 2p^k \) for an odd prime \( p \) and \( k \geq 1 \). The automorphism tower must eventually reach the trivial group, hence there is some \( i \geq 0 \) such that \( \varphi^i(n) = 1 \). This implies, if we take \( i \) minimal, \( \varphi^{i-1}(n) = 2 \). The only way to get 2 is through 3, 6 or 4. Since 3, 6 \( \in X_a \cup X_b \), we must reach it through 4. The only thing we want to do is calculate the following set:

\[
\{ n \in \mathbb{Z}_{\geq 4} | n \in \{ 4, p^k, 2p^k | p \text{ odd prime}, k \in \mathbb{Z}_{\geq 1} \}, \exists i \in \mathbb{Z}_{\geq 0} : \varphi^i(n) = 4 \}.
\]

There is no \( \varphi^{-1} \), but we can calculate what integers map to \( n \) under \( \varphi \) by hand for small numbers. If we work our way backwards from 4, one would not expect that we get a finite set. However, since every element must be (2 times) a prime power, we do get a finite set. The set is \{5, 10, 11, 22, 23, 47, 94\}. So \( n \in X_c \), which completes the proof.

\[\square\]

8 Basic subgroups

In this chapter I will develop the theory of \( p \)-basic subgroups, which some readers may already know. I approach the theory with a definition that is less common in the literature. I will also show useful properties about \( p \)-basic subgroups that are needed for the proofs in the next chapter. First I will introduce a useful convention when talking about vector spaces, after which I will need a long introduction for the definition of a \( p \)-basic subgroup.

Let \( K \) be a field, \( V \) be a \( K \)-vector space, \( I \) a set and let \( a : I \to V, i \mapsto a_i \) be a function. Now \( a \) induces a map \( f_a : K(I) \to V, (\lambda_i)_{i \in I} \mapsto \sum_{i \in I} \lambda_i a_i \). We say \( a \) generates \( V \) when \( f_a \) is surjective. We say \( a \) is linearly independent over \( K \) when \( f_a \) is injective. We say that \( a \) is a basis for \( V \) if \( f_a \) is an isomorphism.

Let \( A \) be an abelian group and \( p \) a prime. For \( n \in \mathbb{Z}_{\geq 1} \) define \( A[n] := \{ a \in A : na = 0 \} \). Denote \( V = A/pA \) as an \( \mathbb{F}_p \)-vector space. For \( i \in \mathbb{Z}_{\geq 0} \) define \( V_i := \text{im}(A[p^i] \to A/pA, x \mapsto x + pA) \) and \( V_{\infty} := \bigcup_{i \in \mathbb{Z}_{\geq 0}} V_i \) as subspaces of \( V \). So we get the following sequence:

\[
0 = V_0 \subset V_1 \subset \ldots \subset V_\infty \subset V = A/pA.
\]

Choose \( S_\infty \subset A \) such that \( S_\infty \to V/V_\infty, s \mapsto (s + pA) + V_\infty \) is a basis for \( V/V_\infty \). For each \( i \in \mathbb{Z}_{\geq 1} \) choose \( S_i \subset A[p^i] \) such that \( S_i \to V_i/V_{i-1}, s \mapsto (s + pA) + V_{i-1} \) is a basis for \( V_i/V_{i-1} \). Define the following group:

\[
B := \left( \bigoplus_{i \in \mathbb{Z}_{\geq 1}} \left( \mathbb{Z}/p^i\mathbb{Z} \right)^{\left( S_i \right)} \right) \oplus \mathbb{Z}^{\left( S_\infty \right)}.
\]

Note that we have \( |S_\infty| = \dim_{\mathbb{F}_p}(V/V_\infty) \) and \( |S_i| = \dim_{\mathbb{F}_p}(V_i/V_{i-1}) \). Note that \( B \) only depends on the size of \( S_i \), so \( B \) does not depend on the choice of \( S_i \) (up to isomorphism). Now define \( \varphi : B \to A \) in the same manner we induced \( f_a \) from \( a \), which does depend on the choice of \( S_i \).

**Definition 8.1.** Let \( A \) be an abelian group and \( p \) a prime. Then \( (B, (S_i)_{i \in \{ \infty \} \cup \mathbb{Z}_{\geq 1}}, \varphi) \) is called a \( p \)-basic subgroup of \( A \).

As done more often with definitions, I will just say that \( B \) is a \( p \)-basic subgroup of \( A \) and not state \( S_i \) and \( \varphi \) explicitly. Throughout this and the next chapter I will always denote the sets \( S_i \) and the map \( \varphi \) whenever I talk about a \( p \)-basic subgroup. The definition becomes
more useful when \( \varphi \) is actually injective, so we can see \( B \) as a subgroup of \( A \). This is actually the case. The following two theorems show some important properties of a \( p \)-basic subgroup.

**Theorem 8.2.** Let \( A \) be an abelian group, \( p \) a prime and \( B \) a \( p \)-basic subgroup. Then \( \varphi \) is injective.

**Theorem 8.3.** Let \( A \) be an abelian group, \( p \) a prime, \( B \) a \( p \)-basic subgroup and \( n \in \mathbb{Z}_{\geq 1} \). Denote the following subgroup of \( B \):

\[
B_n := \bigoplus_{i \in \{1, \ldots, n\}} (\mathbb{Z}/p^i\mathbb{Z})^{(S_i)}.
\]

Then the following short exact sequence is split:

\[
0 \to B_n \xrightarrow{\varphi|_{B_n}} A \to A/\varphi(B_n) \to 0.
\]

The following theorem is a useful result and is crucial in my proofs of the two theorems above.

**Theorem 8.4.** Let \( A \) be an abelian group, \( p \) a prime, \( B \) a \( p \)-basic subgroup and \( n \in \mathbb{Z}_{\geq 1} \). Then \( \varphi \) induces a map \( \psi_n : B/p^nB \to A/p^nA \), which is an isomorphism.

Before proving these three theorems, I will prove two lemmas. These lemmas are helpful in general, since they give an idea of what the \( V_i \) look like.

**Lemma 8.5.** We have \( V/V_\infty \cong A/(pA + A_{\text{tors}}) \) and for \( i \in \mathbb{Z}_{>0} \) we have \( V_i/V_{i-1} \cong A[p^i]/(pA[p^{i+1}] + A[p^{i-1}]) \), where the isomorphisms are \( \mathbb{F}_p \)-vector space isomorphisms.

**Proof.** First note that any isomorphism between abelian groups is also a \( \mathbb{Z} \)-module isomorphism. In all stated quotients we see that multiplying any element by \( p \) is always the zero element, so any group isomorphism will be an \( \mathbb{F}_p \)-vector space isomorphism.

Define \( \varphi : A \to V/V_\infty, a \mapsto (a + pA) + V_\infty \). This \( \varphi \) is a surjective map. So if I can show that the kernel is exactly \( pA + A_{\text{tors}} \), the first isomorphism theorem proves the first part. Let \( a \in A \), then we have:

\[
\varphi(a) = 0 \iff a + pA \in V_\infty
\]
\[
\iff \exists i \in \mathbb{Z}_{\geq 0} : a + pA \in V_i
\]
\[
\iff \exists i \in \mathbb{Z}_{\geq 0} : \exists b \in A[p^i] : a + pA = b + pA
\]
\[
\iff \exists i \in \mathbb{Z}_{\geq 0} : \exists b \in A[p^i], c \in A : a = b + pc
\]
\[
\iff \exists b \in A_{\text{tors}}, c \in A : a = b + pc.
\]

It is enough to show that the converse of the last implication holds. Let \( a \in pA + A_{\text{tors}} \) and write \( a = pc + b \). Let \( n \) be the order of \( b \). I need to find an \( i \in \mathbb{Z}_{\geq 1} \), \( y \in A[p^i] \) and \( c' \in A \) such that \( pc + b = pc' + y \). It is enough to find a \( c' \in A \) such that \( p(c - c') + b \) has order dividing \( p^i \). To have fewer letters: it is enough to find \( i \in \mathbb{Z}_{\geq 1} \) and \( d \in A \) such that \( p^i(b + pd) = 0 \).

Write \( n = p^t \cdot n' \) with \( p \nmid n' \). Sinds \( \mathbb{Z}/p\mathbb{Z} \) is a field, we can take \( k \in \mathbb{Z}_{\geq 1} \) such that \( kn' \equiv 1 \mod p \). Take \( i = t \) and \( d = \frac{kn'-1}{p}b \) and it works.

I will now prove the other isomorphism. Define \( \psi : A[p^i] \to V_i/V_{i-1}, a \mapsto a + pA + V_{i-1} \). Again \( \psi \) is surjective, so by the first isomorphism theorem it is enough to show \( \psi \) has
Let $a \in A[p^i]$, then:

\[
\psi(a) = 0 \iff a + pA \in V_{i-1} \\
\implies \exists b \in A[p^{i-1}] : a + pA = b + pA \\
\implies \exists b \in A[p^{i-1}], c \in A : a = b + pc \\
\implies \exists b \in A[p^{i-1}], c \in A[p^{i+1}] : a = b + pc.
\]

I will show that the other implication holds as well. Let $a \in A[p^i]$ such that $\psi(a) = 0$ and write $a = b + pc$ with $b \in A[p^{i-1}]$ and $c \in A$. Now we have:

\[
0 = p^i a = p^i(b + pc) = p^i b + p^{i+1} c = p^{i+1} c.
\]

Hence we have $c \in A[p^{i+1}]$ and we are done.

**Lemma 8.6.** For $n \in \mathbb{Z}_{\geq 1}$ we have that $\bigoplus_{i=1}^{n} S_i$ is a basis for $V_n$ as $\mathbb{F}_p$-vector space. Also $\bigoplus_{i \in \mathbb{Z}_{\geq 1}} S_i$ is a basis for $V_\infty$ and $S_{\infty} \bigoplus_{i \in \mathbb{Z}_{\geq 1}} S_i$ is a basis for $V$.\[\square\]

**Proof.** I will show the first part using induction on $n$. Since $V_0 = 0$, the case $n = 1$ is clear. Let $n > 1$. Now we have the following short exact sequence:

\[
0 \to V_n \to V_{n+1} \to V_{n+1}/V_n \to 0.
\]

Every short exact sequence of vector spaces splits, which tells us we have the following isomorphism: $V_{n+1} \cong V_n \oplus V_{n+1}/V_n$. From this isomorphism and induction it is evident that $S_{n+1} \bigoplus \prod_{i=1}^{n} S_i$ is a basis for $V_{n+1}$.

Since $V_\infty$ is the union of all $V_i$, the disjoint union of the bases of $V_i$ will give a basis for $V_\infty$. The last part follows with an analogous proof from a short exact sequence.\[\square\]

**Proof of theorem 8.4.** Consider the following diagram:

\[
\begin{array}{ccc}
B & \xrightarrow{\psi} & A \\
\downarrow & & \downarrow \pi_n \\
B/p^n B & \xrightarrow{\psi_n} & A/p^n A
\end{array}
\]

The map $\psi_n$ comes from the universal property of the quotient group. So $\psi_n$ is unique and exists if $p^n B$ is contained in the kernel of $\pi_n \circ \phi$. Note that we have $\varphi(p^n B) = p^n \varphi(B) \subset p^n A$, hence $\psi_n$ exists.

I will prove this theorem by induction on $n$. For any $n \in \mathbb{Z}_{\geq 1}$, we have the following isomorphism:

\[
B/p^n B \cong \left( \bigoplus_{i \in \{1,...,n-1\}} (\mathbb{Z}/p^i \mathbb{Z})^{(S_i)} \right) \oplus \left( \bigoplus_{i \in \mathbb{Z}_{\geq n}} (\mathbb{Z}/p^n \mathbb{Z})^{(S_i)} \right) \oplus (\mathbb{Z}/p^n \mathbb{Z})^{(S_{\infty})}.
\]

For the base case, $n = 1$, we see that $B/pB$ is a large direct sum consisting of only $\mathbb{F}_p$.

Define $a : S_\infty \bigoplus \prod_{i \in \mathbb{Z}_{\geq 1}} S_i \to V$ as in lemma 8.6 such that $a$ is a basis for $V$ as $\mathbb{F}_p$-vector space. Now $\psi_1$ is exactly $f_a$, so $\psi_1$ is an isomorphism.

Suppose $n > 1$. We have the following diagram:

\[
\begin{array}{cccccc}
0 & \to & pB/p^n B & \xrightarrow{\iota_1} & B/p^n B & \xrightarrow{\pi_1} & B/pB & \to & 0 \\
& & \downarrow \psi_n pB & & \downarrow \psi_n & & \downarrow \psi_1 \\
0 & \to & pA/p^n A & \xrightarrow{\iota_2} & A/p^n A & \xrightarrow{\pi_2} & A/pA & \to & 0
\end{array}
\]

\[20\]
The short five lemma states that if the diagram commutes, the two rows are short exact
sequences and the maps \( \psi_n|_{pB} \) and \( \psi_1 \) are isomorphisms, then so is \( \psi_n \). By the induction
hypothesis we know that \( \psi_1 \) is an isomorphism. It is fairly straightforward to show that
both squares commute, hence I will leave this to the reader.

To show that \( \psi_n|_{pB} \) is an isomorphism, we need to do some work. First, define \( A' = A/A[p] \).
Define \( V = A'/pA' \) and \( V'_1 \) and \( V'_\infty \) in the same manner as before with \( A \) replaced by \( A' \).
I claim we can choose \( S'_i = S_{i+1} \) and \( S'_\infty = S_\infty \) to define \( B' \) as a \( p \)-basic subgroup. The
following proves this, using lemma 8.5:

\[
V'_i/V'_{i-1} \cong A'[p]/(pA'[p^{i+1}] + A'[p^{i-1}]) \\
\cong A[p^{i+1}]/(pA[p^{i+2}] + A[p]) \\
\cong V'_{i+1}/V_i.
\]

Now if we express \( B' \) in terms of \( S_i \), we have the following:

\[
B' = \left( \bigoplus_{i \in \mathbb{Z}_2} (\mathbb{Z}/p^i\mathbb{Z})^{(S_{i+1})} \right) \oplus \mathbb{Z}^{(S_\infty)}.
\]

Consider the map \( f : A \to pA, a \mapsto pa \). Clearly the kernel is \( A[p] \), so \( f \) induces an
isomorphism between \( A' \) and \( pA \). Now we have:

\[
pA/p^n A = pA/p^{n-1}(pA) \cong A'/p^{n-1}A'.
\]

This isomorphism is induced by \( f \), so again it is multiplication by \( p \). Denote this isomor-
phism by \( \tilde{f} : A'/p^{n-1}A' \to pA/p^n A \). In exactly the same manner, we get the isomorphism
\( \tilde{g} : B'/p^{n-1}B' \to pB/p^n B \). Since \( A' \) satisfies the induction hypothesis, we have \( \psi_{n-1} \) is an
isomorphism. We have the following diagram:

\[
\begin{array}{ccc}
B'/p^{n-1}B' & \xrightarrow{\tilde{f}} & pB/p^n B \\
\downarrow{\psi_{n-1}} & & \downarrow{\psi_n|_{pB}} \\
A'/p^{n-1}A' & \xrightarrow{\tilde{g}} & pA/p^n A
\end{array}
\]

Showing that the square commutes is showing that multiplying with \( p \) before \( \psi \) is the same
as multiplying after \( \psi \). However, \( \psi \) is \( \mathbb{Z} \)-linear so this is trivial. This shows that \( \psi_n|_{pB} \)
is an isomorphism since the three other maps are isomorphisms. \( \square \)

**Proof of theorem 8.2.** Let \( n \in \mathbb{Z}_{\geq 1} \), denote \( \psi_n \) the isomorphism as in theorem 8.4 and
\( \pi_n : B \to B/p^n B \) the quotient map of \( B \). The following diagram commutes:

\[
\begin{array}{ccc}
B & \xrightarrow{\varphi} & A \\
\downarrow{\pi_n} & & \downarrow{} \\
B/p^n B & \xrightarrow{\psi_n} & A/p^n A
\end{array}
\]

From the commuting property and that \( \psi_n \) is an isomorphism follows ker(\( \varphi \)) \subseteq ker(\( \pi_n \)) =
\( p^n B \). We even get: ker(\( \varphi \)) \subseteq \bigcap_{n \in \mathbb{Z}_{\geq 1}} p^n B. We know \( B \) explicitly and it is clear that
\( \bigcap_{n \in \mathbb{Z}_{\geq 1}} p^n B = 0 \). Hence ker(\( \varphi \)) = 0. \( \square \)
Proof of theorem 8.3. First note that by theorem 8.2, the map \( \varphi \) is injective and we do have an exact sequence. By the splitting lemma it is enough to show there is a homomorphism \( r : A \to B_n \) such that \( r \varphi|_{B_n} = \text{id}_{B_n} \). As stated in the proof of theorem 8.4, we know that \( B/p^nB \) is isomorphic to a large direct sum. Now \( B_n \) is part of this direct sum, so define \( B' \) as the rest of the direct sum such that \( f_n : B_n \oplus B' \to B/p^nB \) is an isomorphism. Consider the following diagram:

\[
\begin{array}{ccc}
B_n & \xrightarrow{e_1} & B & \xrightarrow{\varphi} & A \\
\downarrow{s} & & \downarrow{\pi_B} & & \downarrow{\pi_A} \\
B_n \oplus B' & \xrightarrow{f_n} & B/p^nB & \xrightarrow{\psi_n} & A/p^nA
\end{array}
\]

Take \( e_1 \) and \( e_2 \) the canonical embeddings and \( s \) the projection map. By definition of \( f_n \) we have \( f_n \circ e_2 = \pi_B \circ e_1 \) and by definition of \( \psi_n \) follows that the right square commutes. Note that we have \( s \circ e_2 = \text{id}_{B_n} \). Taking \( r = s \circ f_n^{-1} \circ \psi_n^{-1} \circ \pi_A \) satisfies \( r \varphi|_{B_n} = \text{id}_{B_n} \). \( \square \)

9 Abelian automorphism groups

Let \( A \) be an abelian group. Then \(-1_A : A \to A, a \mapsto -a\).

**Theorem 9.1.** Let \( A \) be an abelian group such that \( \text{Aut}^i A \) is abelian for \( i = 0, ..., 4 \) and \( \text{Aut} A \) is infinite. Then \( \text{Aut} A \cong \mathbb{Z}/2\mathbb{Z} \oplus C \) where \( C \) is a \( \mathbb{Z}[2^{-1}] \)-module.

The following theorem is trivial, but is crucial in this chapter.

**Definition 9.2.** Let \( A \) and \( B \) be abelian groups. We say \( B \) is a direct summand of \( A \) if there exists an abelian group \( C \) such that \( A \cong B \oplus C \). I use the notation \( B \mid A \).

**Theorem 9.3.** Let \( A \) and \( B \) be abelian groups with \( B \mid A \) and \( \text{Aut} A \) abelian. Then \( \text{Aut} B \) is abelian and \( \text{Aut} B \mid \text{Aut} A \). Moreover if \( A \) has an abelian automorphism tower, then \( B \) has an abelian automorphism tower as well.

**Proof.** The proof is obvious from theorem 6.3, which shows that we have \( \text{Aut}(B \oplus C) \cong \text{Aut}(B) \oplus \text{Aut}(C) \oplus \text{Hom}(B,C) \oplus \text{Hom}(C,B) \). \( \square \)

**Lemma 9.4.** Let \( G \) be a group with exponent 2. Then there exists a set \( X \) such that \( G \cong (\mathbb{Z}/2\mathbb{Z})^{(X)}\).

**Proof.** Note \( aba^{-1}b^{-1} = abab = 1 \), therefore \( G \) is abelian. It is enough to show that \( G \) is a vector space over the field \( \mathbb{F}_2 \), from which follows that \( G \) has a basis and we can choose \( X \) as the set consisting of all the basis elements. Choose the addition of \( G \) as a vector space the same as the operation from \( G \). For \( g \in G \) define \( 0 \cdot g = 0 \) and \( 1 \cdot g = g \). I leave it to the reader to verify that with these operations \( G \) is indeed a vector space over \( \mathbb{F}_2 \). \( \square \)

**Lemma 9.5.** Let \( A \) be an abelian group such that \( \text{Aut} A \) is abelian and \(-1_A = \text{id}_A\). Then \( A \) is either trivial or \( \mathbb{Z}/2\mathbb{Z} \).

**Proof.** From \(-1_A = \text{id}_A\) follows that every element in \( A \) has order at most 2. From lemma 9.4 we can take \( X \) a set such that \( A \cong (\mathbb{Z}/2\mathbb{Z})^{(X)} \). Suppose \( |X| \geq 2 \). Now \( \text{Aut}(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) \cong \text{Sym} 3 \) must be abelian by theorem 9.3, which is a contradiction. Thus \( X \) cannot have more than one element. \( \square \)

For a prime \( p \) denote \( \Gamma_p = \mathbb{Z}[p^{-1}]/\mathbb{Z} \). For an abelian group \( A \) and \( n \in \mathbb{Z}_{\geq 1} \) denote \( A[n] = \{ a \in A | na = 0 \} \). For a prime \( p \) denote \( A[p^\infty] = \{ a \in A | \exists n \in \mathbb{Z}_{\geq 0} : p^n a = 0 \} \).
In the following lemma and the previous notation some arbitrary prime $p$ is used. In this chapter I will always use $p = 2$.

**Lemma 9.6.** Let $A$ be an abelian group and $p$ a prime such that there exists $a \in A \setminus \{0\}$ with $pa = 0$. Then $\Gamma_p \mid A$ or there exists an $n \in \mathbb{Z}_{\geq 1}$ such that $\mathbb{Z}/p^n\mathbb{Z} \mid A$.

**Proof.** We have either $A[p^\infty] \subset pA$ or $A[p^\infty] \not\subset pA$. I will consider both cases.

Suppose $A[p^\infty] \subset pA$. Let $a_1 \in A[p]\setminus \{0\}$. Now $a_1 \in pA$, so there exists $a_2 \in A[p^2]$ such that $pa_2 = a_1$. We can iterate this to find $a_i$ for each $i \geq 1$ such that $pa_i = a_{i-1}$. Define $f : \Gamma_p \to A$ where $f(p^{-i}) = a_i$. This map is well-defined and also injective. Consider the exact sequence, where $C$ is the quotient:

$$0 \to \Gamma_p \to A \to C \to 0.$$ 

Note that $\Gamma_p$ is a divisible group. Divisible abelian groups are injective $\mathbb{Z}$-modules (see chapter 10 of [5]), meaning that they split each short exact sequence of abelian groups. Thus $\Gamma_p$ is a direct summand of $A$.

Suppose $A[p^\infty] \not\subset pA$. Suppose for all $n \in \mathbb{Z}_{\geq 1}$ we have $\mathbb{Z}/p^n\mathbb{Z} \nmid A$. Let $B$ be a $p$-basic subgroup of $A$. From theorem 8.3 follows $V = V_\infty$. This can only happen if each element with order $p^n$ for some $n \geq 1$ is divisible by $p$, or equivalently $A[p^\infty] \subset pA$. This is a contradiction. Hence there exists $n \in \mathbb{Z}_{\geq 1}$ such that $\mathbb{Z}/p^n\mathbb{Z} \mid A$. □

**Lemma 9.7.** Let $A$ and $B$ be non-trivial abelian groups such that $\text{Aut}(A \oplus B)$ is abelian. Then there exists a set $X$ such that $\text{Aut}(A \oplus B) \cong \text{Aut}(A) \oplus \text{Aut}(B) \oplus (\mathbb{Z}/2\mathbb{Z})^{|X|}$. Moreover, if $\text{Aut}^2(A \oplus B)$ is abelian, then $|X| \leq 1$. If also $\text{Aut}^3(A \oplus B)$ is abelian, then $|X| = 0$.

**Proof.** From theorem 6.3 we have $\text{Aut}(A \oplus B) \cong \text{Aut}(A) \oplus \text{Aut}(B) \oplus \text{Hom}(A,B) \oplus \text{Hom}(B,A)$. Note $-1_A \in \text{Aut} A$. So for any $f \in \text{Hom}(A,B)$, we have that from 6.3.2 follows $-f = f$. This shows $2f = 0$, so the exponent of $\text{Hom}(A,B)$ and $\text{Hom}(B,A)$ divides 2. From lemma 9.4 we can take a set $X$ such that $\text{Hom}(A,B) \oplus \text{Hom}(B,A) \cong (\mathbb{Z}/2\mathbb{Z})^{|X|}$.

Suppose also $\text{Aut}^2(A \oplus B)$ is abelian. If $|X| \geq 2$ then theorem 9.3 implies that $\text{Sym} \mathbb{Z} \cong \text{Aut}(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})$ is abelian, which is a contradiction. Therefore $|X| \leq 1$.

Suppose also $\text{Aut}^3(A \oplus B)$ is abelian. Let $X$ be a set such that $\text{Aut}(A \oplus B) \cong \text{Aut}(A) \oplus \text{Aut}(B) \oplus (\mathbb{Z}/2\mathbb{Z})^{|X|}$. By the previous statement we know $|X| \leq 1$. Assume $|X| = 1$.

Assume that both $A$ and $B$ contain at least 3 elements. We see by lemma 9.5 that $-1 \neq \text{id}$ in both $\text{Aut} A$ and $\text{Aut} B$. Therefore $\text{Hom}(\mathbb{Z}/2\mathbb{Z}, \text{Aut} A)$ and $\text{Hom}(\mathbb{Z}/2\mathbb{Z}, \text{Aut} B)$ are both non-zero. Also these groups have exponent 2, so we have $(\mathbb{Z}/2\mathbb{Z})^2 \mid \text{Aut}^2(A \oplus B)$. Now theorem 9.3 implies that $\text{Sym} \mathbb{Z}$ is abelian, which is a contradiction.

Suppose without loss of generality $|A| = 2$. If $-1_B = \text{id}_B$, then $B \cong \mathbb{Z}/2\mathbb{Z}$ by lemma 9.5. This would mean that $\text{Aut}(A \oplus B) \cong \text{Sym} \mathbb{Z}$, which is a contradiction. Therefore $-1_B \neq \text{id}_B$ and we can use lemma 9.6 for $\text{Aut} B$. Assume $\mathbb{Z}/2^n\mathbb{Z} \mid \text{Aut} B$ for some $n \in \mathbb{Z}_{>1}$. We can take a group $C$ such that we have:

$$\text{Aut}(A \oplus B) \cong \text{Aut}(\mathbb{Z}/2\mathbb{Z} \oplus B) \cong C \oplus \mathbb{Z}/2^n\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$ 

Now $\text{Aut}(\mathbb{Z}/2^n\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})$ is non-abelian by theorem 7.2. This is a contradiction, so $\Gamma_2 \mid \text{Aut} B$. Thus we can take a group $C'$ such that we have:

$$\text{Aut}(A \oplus B) \cong \text{Aut}(\mathbb{Z}/2\mathbb{Z} \oplus B) \cong C' \oplus \Gamma_2 \oplus \mathbb{Z}/2\mathbb{Z}.$$
I leave it to the reader to verify that the automorphism group of $\Gamma_2$ is $\mathbb{Z}_2^*$, which is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$ by lemma 5.7. Note that $\text{Hom}(\mathbb{Z}/2\mathbb{Z}, \Gamma_2)$ is non-trivial and has exponent 2. Now $(\mathbb{Z}/2\mathbb{Z})^{(2)} \mid \text{Aut}^2(A \oplus B)$ and from theorem 9.3 follows a contradiction.

All cases lead to a contradiction, hence the assumption $|X| = 1$ is false. Thus $|X| = 0$. □

Proof of theorem 9.1. From lemma 9.5 we see $-1_A \neq \text{id}_A$, therefore $\text{Aut} A$ has an element of order 2. This means we can use lemma 9.6 for $\text{Aut} A$. Suppose $\Gamma_2 \mid \text{Aut} A$. We have $(\mathbb{Z}/2\mathbb{Z})^{(2)} \mid \text{Aut}^2 \Gamma_2$ which is a contradiction by theorem 9.3. Let $n \in \mathbb{Z}_{\geq 1}$ such that $\mathbb{Z}/2^n\mathbb{Z} \mid \text{Aut} A$. Note $\text{Aut} \mathbb{Z}/2^n\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{n-1}\mathbb{Z}$ for $n \geq 3$. Since this is not a cyclic group, we see by theorem 7.2 that its automorphism group is not abelian. Theorem 9.3 implies a contradiction. Hence $n \leq 2$. If $n = 1$ we have $\mathbb{Z}/2\mathbb{Z} \mid \text{Aut} A$, so assume $n = 2$.

Write $\text{Aut} A \cong \mathbb{Z}/4\mathbb{Z} \oplus C$. Note $\mathbb{Z}/2\mathbb{Z} \mid \text{Aut}^2 A$. Since $\text{Aut} A$ is infinite, we see that $C$ must be infinite. From lemma 9.5 follows $-1_C \neq \text{id}_C$. If there is some $m \in \mathbb{Z}_{\geq 1}$ such that $\mathbb{Z}/2^m\mathbb{Z} \mid \text{Aut} C$, then $\text{Aut}(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^m\mathbb{Z}) \mid \text{Aut}^2 A$ which is a contradiction by theorem 7.2 and 9.3. From lemma 9.6 follows $\Gamma_2 \mid \text{Aut} C$. We have $\Gamma_2 \oplus \mathbb{Z}/2\mathbb{Z} \mid \text{Aut}^2 A$. Note $\mathbb{Z}/2\mathbb{Z} \mid \text{Aut} \Gamma_2$ and $\mathbb{Z}/2\mathbb{Z} \mid \text{Hom}(\mathbb{Z}/2\mathbb{Z}, \Gamma_2)$, thus $(\mathbb{Z}/2\mathbb{Z})^{(2)} \mid \text{Aut}(\Gamma_2 \oplus \mathbb{Z}/2\mathbb{Z})$. This is a contradiction by theorem 9.3. So $\mathbb{Z}/2\mathbb{Z} \mid \text{Aut} A$.

Write $\text{Aut} A \cong \mathbb{Z}/2\mathbb{Z} \oplus C$. Note that any abelian group is also a $\mathbb{Z}$-module. We have that $C$ is a $\mathbb{Z}[2^{-1}]$-module iff the map $f : C \to C, x \mapsto 2x$ is an isomorphism. Now $f$ is exactly an isomorphism iff $C = 2C$ and $C[2] = 0$. From theorem 6.3 we get:

$$\text{Aut}^2 A \cong \text{Aut}(\mathbb{Z}/2\mathbb{Z} \oplus C) \cong \text{Aut}(C) \oplus \text{Hom}(C, \mathbb{Z}/2\mathbb{Z}) \oplus \text{Hom}(\mathbb{Z}/2\mathbb{Z}, C).$$

However we can apply theorem 9.7 to $\mathbb{Z}/2\mathbb{Z} \oplus C$ and we see that both Hom-groups must be zero. We have $\text{Hom}(C, \mathbb{Z}/2\mathbb{Z}) = \text{Hom}(C/2C, \mathbb{Z}/2\mathbb{Z}) = 0$, so $C = 2C$. We also have $\text{Hom}(\mathbb{Z}/2\mathbb{Z}, C) = 0$, therefore $C[2] = 0$. □

10 References


