Groups that split short exact sequences

Apon, R.J.

R.J. Apon

Groups that split short exact sequences

Thesis, June 2, 2014

Supervisor: prof.dr. H.W. Lenstra

Mathematical Institute, University of Leiden

Contents

1 Introduction

For this thesis I studied groups that, in one of several senses yet to be defined, split all short exact sequences. However, I will not do this for abelian groups, but for arbitrary groups. Abelian groups that, in the same sense, split short exact sequences of abelian groups are already classified [1]. In this thesis I will prove which groups split all short exact sequences for the arbitrary case. If I define a short exact sequence, I will always mean a short exact sequence of groups.

Because I don't restrict the groups to be abelian, a short exact sequence can be split in two ways. The following definition shows this.

Definition 1.1. *Let* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *be a short exact sequence. The sequence is called split iff there exists an isomorphism* $\phi : B \to A \times C$ *such that the following diagram, with* $\varepsilon_A : A \to A \times C, x \mapsto (x, e)$ *and* $\pi_C : A \times C \to C, (x, y) \mapsto y$*, commutes:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \| & & \phi\downarrow & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{\varepsilon_A} & A \times C & \xrightarrow{\pi_C} & C & \longrightarrow & 0. \end{array}$$

The short exact sequence is called half-split iff there exists an isomorphism $\phi : B \to A \rtimes_\psi C$ *with a homomorphism* $\psi : C \to \mathrm{Aut}\,(A)$ *such that the following diagram, with* $\varepsilon'_A : A \to A \rtimes_\psi C, x \mapsto (x, e)$ *and* $\pi'_C : A \rtimes_\psi C \to C, (x, y) \mapsto y$*, commutes:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \| & & \phi\downarrow & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{\varepsilon'_A} & A \rtimes_\psi C & \xrightarrow{\pi'_C} & C & \longrightarrow & 0. \end{array}$$

My definition of half-split is known as split for other mathematicians. My definition for a sequence to be split did not have a name yet. I changed the names so that it is more logical, as split is a stronger requirement than half-split. The extra definition for a sequence to be split will also introduce some extra definitions for groups.

Definition 1.2. *A group* G *is called (half-)projective iff every short exact sequence* $0 \to A \to B \to G \to 0$ *is (half-)split.*

The definition of projective is very similar to the abelian case. Half-projective is also a name invented for this thesis. In the following theorem the definition of a free group is needed. The definition can be found at the start of section 3.

Theorem 1.3. *Let G be a group. Then is G half-projective iff G is free.*

This theorem is a similar result as for the abelian case, for which projective groups are free abelian groups. However, the definition of projective for arbitrary groups is useless.

Theorem 1.4. *Let G be a group. Then is G projective iff G is the trivial group.*

Those are all the results for groups that are the last in the short exact sequence. Now the results for the groups that are in the middle of the sequence.

Definition 1.5. *A group G is called (half-)semisimple iff every short exact sequence $0 \to A \to G \to C \to 0$ is (half-)split.*

I am not sure how many readers will know the definition of a complement. Therefore I will give this definition, which is needed in the theorem that follows.

Definition 1.6. *Let G be a group and $H \subset G$ a subgroup. Then a complement of H in G is a subgroup $K \subset G$ such that holds $G = HK$ and $H \cap K = \{e\}$.*

Theorem 1.7. *Let G be a group. Then holds: G is half-semisimple iff every normal subgroup of G has a complement.*

This theorem is merely a restatement of the definition, because $G = A \rtimes_\psi C$ is equivalent to $G = AC$, $A \cap C = \{e\}$ and $A \lhd G$. I have not been able to prove anything that gives more information than this theorem. To make it up for the readers, I will give an example of a half-semisimple group.

Theorem 1.8. *Let $n \in \mathbb{Z}_{\geq 1}$. Then S_n is half-semisimple.*

For injective groups, I can say far more. But I will need some extra definitions.

Definition 1.9. *Let G be a group and $H, H' \subset G$ two subgroups. Then H and H' centralize each other iff $\forall a \in H, b \in H' : ab = ba$.*

Note that if two subgroups centralize each other, it does not mean that the subgroups H or H' themselves are abelian. However, a subgroup is abelian if and only if it centralizes itself.

Definition 1.10. *Let G be a group. Then G is called simple if $\#\{N \subset G : N \lhd G\} = 2$.*

Note that the group $\{e\}$ is not simple, because it has only one normal subgroup.

Theorem 1.11. *Let G be a group. The following statements are equivalent:*

(i) *G is generated by a collection of simple subgroups that centralize each other.*
(ii) *G is generated by a collection of simple normal subgroups that centralize each other.*
(iii) *$G \cong \bigoplus_{i \in I} S_i$ with every S_i simple and I some set.*
(iv) *G is semisimple.*

The previous result is very similair to the result for abelian groups. If you restrict the groups and subgroups to be abelian, you get the theorem for abelian groups. This has a simple reason: if the middle group (mostly named B) in a short exact sequence is abelian, both groups on the side have to be as well.

Definition 1.12. *A group G is called (half-)injective iff every short exact sequence $0 \to G \to B \to C \to 0$ is (half-)split.*

The group $\mathrm{Out}(G)$ is not well-known, so I will give this definition. Then I can give a theorem.

Definition 1.13. *The quotient group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is denoted by $\mathrm{Out}(G)$.*

Theorem 1.14. *Let G be a group. Then holds: G is half-injective iff $0 \to G \xrightarrow{i} \mathrm{Aut}(G) \xrightarrow{j} \mathrm{Out}(G) \to 0$ with $i : G \to \mathrm{Aut}(G), \alpha \mapsto (x \mapsto \alpha x \alpha^{-1})$ and j the canonical homomorphism is a half-split short exact sequence.*

Projective and semisimple groups had similar results for arbitrary groups as for abelian groups, but injective groups are completely different. We can see that $i : G \to \mathrm{Aut}(G)$ must be injective. But $\ker(i) = \mathrm{Z}(G)$, so a half-injective group has a trivial center. Also if a group G is half-injective, this gives us information about $\mathrm{Aut}(G)$. For an injective group, it gives us even more information.

Definition 1.15. *Let G be a group. Then G is complete iff every automorphism of G is an inner automorphism and $\mathrm{Z}(G) = \{e\}$.*

Note that this definition is equivalent to saying: $i : G \to \mathrm{Aut}(G), g \mapsto (x \mapsto gxg^{-1})$ is an isomorphism.

Theorem 1.16. *Let G be a group. Then holds: G is injective iff G is complete.*

Knowledge of group theory is indispensable for reading this thesis. Knowledge about short exact sequences is pleasant, but the important lemmas will be provided in chapter 2. These lemmas will be familiar to mathematicians that worked with short exact sequences, but they are different because the groups are not restricted to be abelian.

I will start in chapter 2 with essential lemmas that I will use several times. In chapter 3 I will prove the theorem that classifies half-projective groups.

I will do the same for projective groups in chapter 4. The same structure repeats for (half-)semisimple and (half-)injective groups in that order.

2 Conventions, definitions and essential lemmas

Before I start with some lemmas, I will note a convention. Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence. We see that $f(A)$ is a subgroup of B. But f is injective, thus $f(A) \cong A$. Therefore I will speak of A as if it is contained in B with f the inclusion.

It is very useful to know some statements that are equivalent to saying that a short exact sequence is split or half-split. In the abelian case there are such statements. For the arbitrary case the statements are fairly similar. The following two lemmas are very useful and will be used multiple times in this thesis.

Lemma 2.1. *Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence. It half-splits iff there exists a homomorphism $s : C \to B$ such that holds: $g \circ s = \mathrm{id}_C$.*

The homomorphism s is called a section of g.

Proof. ($\Rightarrow$). Let $\phi : B \to A \rtimes_\psi C$ be an isomorphism with a homomorphism $\psi : C \to \mathrm{Aut}(A)$ such that the diagram, as in the definition of half-split, commutes.

Let $h : C \to A \rtimes_\psi C, x \mapsto (e, x)$. Denote $s = \phi^{-1} \circ h$. The function s is a homomorphism because it is a composition of homomorphisms. The diagram commutes, therefore $g = \pi_C \circ \phi$. Then holds: $g \circ s = \pi_C \circ \phi \circ \phi^{-1} \circ h = \pi_C \circ h$. By definition of h and π_C it is clear that holds $\pi_C \circ h = \mathrm{id}_C$. Thus $g \circ s = \mathrm{id}_C$, so there exists a section.

($\Leftarrow$). Let s be a section of g. Note that s is injective because $g \circ s$ is. Thus we can see C as a subgroup of B. I will treat C as such.

To prove that B is a semidirect product of A and C it is enough to prove the following: $A \lhd B$, $B = AC$ and $A \cap C = \{e\}$.

We know $A \lhd B$ because $\ker(f) = A$. The inclusion $AC \subset B$ is clear. I will prove the other inclusion. Let $b \in B$. Take $c \in C$ such that $f(b) = c$. But we also know $g(b) = g(s(c))$. Thus $bs(c)^{-1} \in \ker(g) = \mathrm{im}(f)$. Let $a \in A$ such that $bs(c)^{-1} = f(a)$. This gives $b = f(a)s(c) \in f(A)s(C)$. I consider A and C subgroups of B with f and s the inclusions, thus $b \in AC$.

Let $x \in A \cap C$. We know $g(x) = \{e\}$ because $x \in \ker(g) = A$. Also $x \in \mathrm{im}(s)$ thus $g(x) = x$. So $x = e$. Thus $A \cap C = \{e\}$.

Note: I've also proven that A is a complement of C. Thus every element $b \in B$ can be uniquely expressed as a product $b = ac$ with $a \in A$ and $c \in C$. Now I can make the following homomorphism. Let $\phi : B \to A \rtimes_\psi C, ac \mapsto (a, g(c))$ with a homomorphism $\psi : C \to \mathrm{Aut}\,(A), c \mapsto (x \mapsto cxc^{-1})$. So the short exact sequence is half-split. $\square$

Lemma 2.2. *Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence. It splits iff there exists a homomorphism $r : B \to A$ such that holds: $r \circ f = \mathrm{id}_A$.*

The homomorphism r is called a retract of f.

Proof. ($\Rightarrow$). Let $\phi : B \to A \times C$ be an isomorphism as in definition 1.1. Let $h : A \times C \to A$ be the homomorphism that forgets the second coordinate. Denote $r = h \circ \phi$. The function r is a homomorphism because it is a composition of homomorphisms.

The following holds: $r \circ f = h \circ \phi \circ f = h \circ \varepsilon_A = \mathrm{id}_A$. Thus there exists a retract.

($\Leftarrow$). Let r be a retract of f. Let $\phi : B \to A \times C, b \mapsto (r(b), g(b))$. I will prove that ϕ is an isomorphism.

First note that ϕ is a homomorphism because r and g are. Let $x \in \ker(\phi)$. Then holds $r(x) = e$ and $g(x) = e$. From this follows $x \in \ker(r) \cap \ker(g)$. Let $a \in A$ such that $f(a) = x$. This a exists because $x \in \ker(g) = \mathrm{im}\,(f)$. We also know $a = r(f(a)) = r(x) = e$. Thus we get $x = f(e) = e$. So $\ker(\phi) = \{e\}$. Therefore ϕ is injective.

Let $(a, c) \in A \times C$. Let $b_2 \in g^{-1}(c)$. This b_2 exists because g is surjective. We have: $\phi(b_2) = (r(b_2), c) \in \mathrm{im}\,(\phi)$. We also have:

$$\begin{aligned}\phi(f(a \cdot r(b_2)^{-1})) &= ((r \circ f)(a \cdot r(b_2)^{-1}), (g \circ f)(a \cdot r(b_2)^{-1})) \\ &= (a \cdot r(b_2)^{-1}, e) \in \mathrm{im}\,(\phi)\end{aligned}$$

The product of $\phi(f(a \cdot r(b_2)^{-1}))$ and $\phi(b_2)$ is exactly (a, c). Thus $(a, c) \in \mathrm{im}\,(\phi)$ and ϕ is surjective.

It is easy to verify that the first diagram in definition 1.1 commutes. I will leave this to the reader. $\square$

The following lemma is about normal subgroups, which I will use often.

Lemma 2.3. *Let G be a group and $N, N' \lhd G$. If $N \cap N' = \{e\}$ then holds $[N, N'] = \{e\}$.*

Proof. Note: $[N, N'] \subset N$ and $[N, N'] \subset N'$ because both subgroups are normal. Thus $[N, N'] \subset N \cap N'$. We already know $N \cap N' = \{e\}$ so $[N, N'] = \{e\}$. $\square$

I will use sections more often than retracts in the proofs. Therefore I would also like to know when a sequence is split in terms of a section. The following lemma gives me this information.

Lemma 2.4. *Let $0 \to A \to B \to C \to 0$ be a short exact sequence. Then holds: the sequence is split iff there exists a section $s : C \to B$ with $s(C) \lhd B$.*

Proof. ($\Rightarrow$). The sequence is split so let $\psi : B \to A \times C$ be an isomorphism such that the diagram in 1.1 commutes. Let $s : C \to B, x \mapsto \phi^{-1}(e, x)$. Then holds: $\phi(s(C)) = \{e\} \times C \lhd A \times C$. Thus $s(C) \lhd B$.

($\Leftarrow$). Let $s : C \to B$ be a section with $s(C) \lhd B$. Note that holds: $B \cong A \rtimes_\psi s(C)$ with a homomorphism $\psi : s(C) \to \mathrm{Aut}\,(A)$. Because $s(C) \lhd B$ follows $s(C) \lhd A \rtimes_\psi s(C)$.

We already know $A \lhd A \rtimes_\psi s(C)$. Also $A \cap s(C) = \{(e, e)\}$ (see proof 2.1), so from lemma 2.3 we get that A and $s(C)$ centralize each other. If we consider A and C subgroups of B, which we can because f and s are injective, we get $B = AC \cong A \times C$. Thus the short exact sequence is split. □

The following lemma is very trivial, but I still use it a few times. Also it shows the usefulness of lemma 2.2.

Lemma 2.5. *Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence. If any of the three groups A, B or C is the trivial group, then the short exact sequence splits.*

Proof. Suppose $A = \{e\}$. Take $r : B \to A, x \mapsto e$. It is clear that r is a homomorphism and $r \circ f = \mathrm{id}_A$. Thus, using lemma 2.2, the sequence is split.

Suppose $B = \{e\}$. We know $\mathrm{im}\,(f) = \{e\}$. But f is injective, so $A = \{e\}$. This is exactly the first scenario, thus the sequence is split.

Suppose $C = \{e\}$. We know $\ker(g) = B$ so $\mathrm{im}\,(f) = B$. So f is surjective, thus an isomorphism. So f^{-1} is a retract of f. Thus, using lemma 2.2, the sequence is split. □

3 Half-projective groups

Definition 3.1. *A group G is called half-projective iff every short exact sequence $0 \to A \to B \to G \to 0$ is half-split.*

Definition 3.2. *Let G be a group, X a set and $f : X \to G$ a function. Then f is called universal iff for every group H and every function $g : X \to H$ holds: $\exists!$ homomorphism $h : G \to H : h \circ f = g$.*

The property in the definition above is often called the universal property. I will define when a group is free based on this universal property.

Definition 3.3. *Let G be a group. Then G is called free iff there exist a set X and a function $f : X \to G$ such that f is universal.*

Before we prove that half-projective groups are free groups, we need some fundamental theorems for free groups.

Theorem 3.4. *Let X be a set. Then there exist a group G and a function $f : X \to G$ such that f is universal.*

Proof. The proof can be found in the reference [2]. □

If we take an arbitrary set X, we denote $F(X)$ a group with $f : X \to F(X)$ universal. The theorem above states that $F(X)$ and f exist. It is true that $F(X)$ is unique, up to isomorphism, but this is not needed for this thesis and therefore will be left out.

Theorem 3.5. *Let G be a group. Then is G half-projective iff G is free with a basis $X \subset G$.*

Proof. ($\Rightarrow$). Denote $\overline{G}$ as the set of elements of G. Take $F(\overline{G})$ the free group and take $u : \overline{G} \to F(\overline{G})$ universal.

Now consider the function $\mathrm{id} : \overline{G} \to G, x \mapsto x$. Because u is universal, there exists a unique homomorphism $h : F(\overline{G}) \to G$ such that $h \circ u = \mathrm{id}$. Take this h. We know that id is surjective, so h is as well. Now consider the following sequence:

$$0 \to \ker(h) \xrightarrow{f} F(\overline{G}) \xrightarrow{h} G \to 0.$$

Let f be the inclusion. Now holds: $\mathrm{im}\,(f) = \ker(h)$. Also f is injective and h is surjective. Thus the sequence is a short exact sequence.

We know that G is half-projective, thus this sequence is half-split. Let $s : G \to F(\overline{G})$ be a section. We know $h \circ s = \mathrm{id}$, thus s is injective. So G is a subgroup of $F(\overline{G})$.

According to the Nielsen-Schreier Theorem [3], every subgroup of a free group is free. So G is free.

($\Leftarrow$). Let $0 \to A \xrightarrow{f} B \xrightarrow{g} G \to 0$ be a short exact sequence. Take X a set and $u : X \to G$ universal. This is possible because G is free.

Define $i : X \to B$ such that holds $g \circ i = u$. This i exists because g is surjective. The following diagram commutes:

$$\begin{array}{ccc} B & \xrightarrow{g} & G \\ {\scriptstyle i}\uparrow & & {\scriptstyle u}\uparrow \\ X & = & X \end{array}$$

Because u is universal, there exists a unique homomorphism $h : G \to B$ such that holds $h \circ u = i$. We know that holds:

$$g \circ h \circ u = g \circ i = u.$$

Thus must hold $g \circ h = \mathrm{id}_G$. Therefore h is a section and the sequence is half-split. □

4 Projective groups

Definition 4.1. *A group G is called projective iff every short exact sequence $0 \to A \to B \to G \to 0$ is split.*

Theorem 4.2. *Let G be a group. Then is G projective iff G is the trivial group.*

Proof. ($\Leftarrow$) This is proven by lemma 2.5.

($\Rightarrow$). In this proof I will create a specific short exact sequence that is half-split. Then I will show that no section of that sequence has a normal image. This gives, with lemma 2.4, a contradiction.

Suppose $G \neq \{e\}$. Let A be an abelian group with $\mathrm{Aut}(A) \neq \{e\}$. This group exists, because $\mathbb{Z}/3\mathbb{Z}$ is an example. I will leave it to the reader to verify this.

First note that G is free because G is also half-projective. Let $\psi : G \to \mathrm{Aut}(A)$ be a non-trivial homomorphism. This ψ exists because $\mathrm{Aut}(A) \neq \{e\}$, $G \neq \{e\}$ and G is free. Take the following short exact sequence:

$$0 \to A \xrightarrow{f} A \rtimes_\psi G \xrightarrow{g} G \to 0.$$

We take $f(a) = (a, e)$ and g the homomorphism the projection. It is clear that holds $\mathrm{im}(f) = \ker(g)$, thus the sequence is indeed exact.

Let s be a section and suppose $s(G) \lhd A \rtimes_\psi G$. I will now show that this gives a contradiction.

We know $A \cap s(G) = \{e\}$. From lemma 2.3 follows $[A, s(G)] = \{e\}$. Thus $s(G) \subset \mathrm{C}_{A \rtimes_\psi G}(A)$. Because A is abelian we know $A \subset \mathrm{C}_{A \rtimes_\psi G}(A)$. Therefore must hold $A \rtimes_\psi G = \mathrm{C}_{A \rtimes_\psi G}(A)$.

But now holds $G \subset \mathrm{C}_{A \rtimes_\psi G}(A)$. If we write out the product of two elements, we see that every element of G and every element of A only commute if ψ is the trivial homomorphism. This is a contradiction because ψ is a non-trivial homomorphism.

So no section can have a normal image. From lemma 2.4 follows that the sequence cannot be split. But G is projective so it has to be split. This is a contradiction, so G is the trivial group. □

5 Half-semisimple groups

Definition 5.1. *A group G is called half-semisimple iff every short exact sequence $0 \to A \to G \to C \to 0$ is half-split.*

Theorem 5.2. *Let G be a group. Then holds: G is half-semisimple iff every normal subgroup of G has a complement.*

Proof. ($\Rightarrow$). Let $N \lhd G$ en denote $H = G/N$. Take the following short exact sequence, with f the inclusion and g the canonical projection:

$$0 \to N \xrightarrow{f} G \xrightarrow{g} H \to 0.$$

Now follows, because G is half-semisimple: $G \cong N \rtimes_\psi H$ with a homomorphism $\psi : H \to \mathrm{Aut}\,(N)$. This is equivalent to: $G = NH$ and $N \cap H = \{e\}$. Therefore H is a complement of N.

($\Leftarrow$). Let $0 \to A \xrightarrow{f} G \xrightarrow{g} C \to 0$ be a short exact sequence. We know $A \lhd G$ so A has a complement in G. Take a complement of A and call this H. We know $G = AH$ and $A \cap H = \{e\}$, from which follows $G \cong A \rtimes_\psi H$ with a homomorphism $\psi : H \to \mathrm{Aut}\,(A)$.

With the second isomorphism theorem easily follows: $G/A \cong H$. We already know $G/A \cong C$ from the first isomorphism theorem. Therefore $C \cong H$.

Now follows $G \cong A \rtimes_\theta C$ with a homorphism $\theta : C \to \mathrm{Aut}\,(A)$. Thus G is half-semisimple. □

Theorem 5.3. *Let $n \in \mathbb{Z}_{\geq 1}$. Then S_n is half-semisimple.*

Proof. In the whole proof I will not note the possibility that the first group in the short exact sequence (most of the time denoted by A) is the trivial group. In this scenario the sequence always splits, see lemma 2.5.

Also the possibility where the first group is equal to the second group ($A = B$), will not be noted. In this case the third group is the trivial group, so the sequence also always splits, see lemma 2.5.

Let $n \geq 5$ and $0 \to A \xrightarrow{f} S_n \xrightarrow{g} C \to 0$ a short exact sequence. We know $A \lhd S_n$. The only non-trivial normal subgroup of S_n for $n \geq 5$ is A_n, see [4]. So $A = A_n$. We know: $C \cong S_n/A_n \cong C_2$. Write $C = \{e, a\}$ with $a^2 = e$.

Define $s : C \to S_n$ with $s(e) = e$ and $s(a) = (1, 2)$. From $s(a^2) = s(a)^2 = e$ follows that s is a homomorphism. Note $(1, 2) \notin A_n$ so $g(s(a)) = g((1, 2)) = a$. Also $g(s(e)) = e$. Thus $g \circ s = \mathrm{id}_C$. Thus the sequence is half-split and S_n is half-semisimple for $n \geq 5$.

Let $n = 4$ and $0 \to A \xrightarrow{f} S_4 \xrightarrow{g} C \to 0$ a short exact sequence. The only non-trivial normal subgroups of S_4 are V_4 and A_4. If $A = A_4$ the above proof still works. So we only have to check that the sequence is half-split for $A = V_4$.

Consider the short exact sequence $0 \to V_4 \xrightarrow{f} S_4 \xrightarrow{g} C \to 0$, where we consider f the inclusion. Let $h : S_3 \to S_4$ be the inclusion. Denote $i = g|_{S_3}$. I will prove that i is an isomorphism. Consider the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V_4 & \xrightarrow{f} & S_4 & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & & & \uparrow{\scriptstyle h} & & \uparrow{\scriptstyle i} & & \\ & & & & S_3 & = & S_3 & & \end{array}$$

Note: $S_3 \cap V_4 = \{e\}$. It is clear that holds $\ker(i) \subset S_3$. Also $\ker(i) \subset \ker(g) = \mathrm{im}\,(f) = V_4$. So $\ker(i) \subset S_3 \cap V_4 = \{e\}$. Thus i is injective.

We know that $S_4/V_4 \cong C$, by the first isomorphism theorem. Also, S_4 has 24 elements and V_4 has 4 elements. Therefore C must have 6 elements. But S_3 also has 6 elements. Therefore, because i is injective, i is surjective. This makes i an isomorphism.

Then $i^{-1} \circ g = \mathrm{id}_C$, thus i is a section. The sequence is split, so S_4 is half-semisimple.

Let $n = 3$ and $0 \to A \xrightarrow{f} S_n \xrightarrow{g} C \to 0$ a short exact sequence. The only non-trivial normal subgroup of S_3 is A_3. The above proof still works.

We know: $S_1 = \{e\}$ and $S_2 \cong C_2$. So I only have to prove that C_2 is half-semisimple.

It is clear that C_2 is even semisimple, because all proper normal subgroups are trivial. Therefore, using lemma 2.5, we get that C_2 is semisimple and thus also half-semisimple.

I've gone through all possibilities of n, therefore I can now conclude that S_n is half-semisimple for given n. □

6 Semisimple groups

Definition 6.1. *A group G is called semisimple iff every short exact sequence $0 \to A \to G \to C \to 0$ is split.*

I've given all definitions needed to understand the main theorem of this section. But to understand the proof, one more definition is needed.

Definition 6.2. *Let G be a group and $N \subset G$ a subgroup. We call N a minimal normal subgroup iff $N \lhd G$ and $\#\{M \subset N : M \lhd G\} = 2$.*

Theorem 6.3. *Let G be a group. The following statements are equivalent:*

(i) G is generated by a collection of simple subgroups that centralize each other.

(ii) G is generated by a collection of simple normal subgroups that centralize each other.

(iii) $G \cong \bigoplus_{i \in I} S_i$ with every S_i simple and I some set.

(iv) G is semisimple.

In this theorem, some parts of the proof are used several times. Therefore I will create two lemmas for that purpose.

Lemma 6.4. *Let G be a group such that $G = \langle \bigcup_{i \in I} G_i \rangle$ with G_i simple subgroups such that all G_i centralize each other. Then $\forall i \in I : G_i \lhd G$.*

Proof. If I is empty or $|I| = 1$, then the statement is clear. Suppose $|I| > 1$. Let $i, j \in I$ with $i \neq j$. The following are always true: $G_i \subset \mathrm{N}_G(G_i)$ and $\mathrm{C}_G(G_i) \subset \mathrm{N}_G(G_i)$. We know $G_j \subset \mathrm{C}_G(G_i)$ because G_i and G_j centralize each other. Therefore $G_j \subset \mathrm{N}_G(G_i)$ for each $j \in I$. So $\mathrm{N}_G(G_i) = G$, which implies $G_i \lhd G$. □

Lemma 6.5. *Let G be a group such that $G = \langle \bigcup_{i \in I} G_i \rangle$ with G_i simple subgroups such that all G_i centralize each other. Then there exists a subset $J \subset I$ such that $G = \bigoplus_{j \in J} G_j$.*

Proof. Let $\phi : \bigoplus_{i \in I} G_i \to G, (g_i)_{i \in I} \mapsto \prod_{i \in I} g_i$. Note that ϕ is well-defined because all G_i centralize each other. Because of the same reason, ϕ is a homomorphism.

Let $\mathcal{J} = \{J \subset I : \phi|_{\bigoplus_{j \in J} G_j} \text{ is injective }\}$. Note that $\mathcal{J}$ is not empty because $\varnothing \in \mathcal{J}$. For elements in $\mathcal{J}$ holds the following: $J \in \mathcal{J}$ iff for all finite subsets $D \subset J$ holds $D \in \mathcal{J}$.

Let $\mathcal{K} \subset \mathcal{J}$ be a chain. Then holds: $\bigcup_{K\in\mathcal{K}} K \in \mathcal{J}$ iff every finite subset $D \subset \bigcup_{K\in\mathcal{K}} K$ is contained in $\mathcal{J}$.

A finite subset D itself is contained in a finite union of elements of $\mathcal{K}$. Thus there exists a $K \in \mathcal{K}$ such that $D \subset K$, because $\mathcal{K}$ is a chain. From which follows $D \in \mathcal{J}$. So now we know that holds $\bigcup_{K\in\mathcal{K}} K \in \mathcal{J}$. Therefore the chain $\mathcal{K}$ has an upper bound in $\mathcal{J}$. From Zorn's Lemma follows that $\mathcal{J}$ has a maximal element.

Let $J \in \mathcal{J}$ be a maximal element and $N = \langle \bigcup_{j\in J} G_j \rangle$. It is enough to show that $G_i \subset N$ for each $i \in I$.

From lemma 6.4, we know that every G_i is normal in G. But even stronger holds: for every $J' \subset I$ holds $\langle \bigcup_{j\in J'} G_j \rangle$ is normal in G. So N is also normal in G.

From this fact follows $N \cap G_i \lhd G_i$. But every G_i is simple, so $N \cap G_i$ is either G_i or $\{e\}$. Suppose it is $N \cap G_i = G_i$. Then we are done, because $G_i \subset N$. Suppose $N \cap G_i = \{e\}$, thus $G_i \not\subset N$. We can now take a new set: $J' = J \cup \{i\}$. I claim that $J' \in \mathcal{J}$. It is clear that N and G_i centralize each other, because $i \notin J$. It is also clear that holds: $\langle N, G_i \rangle = NG_i$. These two facts combined with $N \cap G_i = \{e\}$, show that $\langle N, G_i \rangle = N \times G_i = N \oplus G_i$. Therefore holds $J' \in \mathcal{J}$. But J was a maximal element and we found a strictly larger element. This is a contradiction with our assumption $N \cap G_i = \{e\}$. So $N \cap G_i = G_i$. Thus $G_i \subset N$ for each $i \in I$. □

Now with this lemma done, we can prove the theorem.

Proof. (Theorem 6.3) $(i) \Rightarrow (ii)$. This is clear from lemma 6.4.

$(ii) \Rightarrow (iii)$. This is clear from lemma 6.5.

$(iii) \Rightarrow (iv)$. Let $0 \to A \xrightarrow{f} G \xrightarrow{g} C \to 0$ be a short exact sequence. Consider the following exact sequence, with $i \in I$ and $h = g|_{S_i}$:

$$S_i \xrightarrow{h} g(S_i) \to 0$$

We already know that $\ker(h) \lhd S_i$. But S_i is simple, so $\ker(h)$ is either S_i or $\{e\}$. Suppose $\ker(h) = \{e\}$, then $S_i \cong g(S_i)$. I am only interested in these S_i. Therefore I make the following set: $I' = \{i \in I : g(S_i) \neq \{e\}\}$. Because the function g is surjective on C, we can say: $\langle g[G] \rangle = C$. But we can even be more specific: $C = \langle g(S_i) : i \in I' \rangle$ because $g(S_i) = \{e\}$ for $i \notin I$. Note: all $g(S_i)$ centralize each other because the S_i centralise each other in G. Therefore we can now use lemma 6.5. Let $J' \subset I'$ such that holds $C = \bigoplus_{j\in J'} g(S_j)$. Because we chose $g(S_j)$ such that it is isomorphic

to S_j, we can write: $\bigoplus_{j\in J'} S_j \cong C$ with the following isomorphism:

$$\phi : \bigoplus_{j\in J'} S_j \to C, (x_j)_{j\in J'} \mapsto \prod_{j\in J'} g(x_j)$$

This is extremely helpful to define our section. Let $\alpha : C \to \bigoplus_{j\in J'} S_j$ be the isomorphism and $\beta : \bigoplus_{j\in J'} S_j \to G$ the embedding. Define the function $s : C \to G, x \mapsto (\beta \circ \alpha)(x)$. Note that α and β are homomorphism, so the composition, s, is a homomorphism as well. It is clear that $g \circ s = \mathrm{id}_C$.

From lemma 6.4 follows $s[C] \lhd G$. From lemma 2.4 follows that the sequence is split.

$(iv) \Rightarrow (i)$. First I treat a lemma that I will use in the proof.

Lemma 6.6. *Let $G \neq \{e\}$ be a group that is semisimple. Then the group G has a minimal normal subgroup.*

Proof. Let $a \in G$ with $a \neq e$. Let $N = \langle gag^{-1} : g \in G\rangle$. Note: $N \lhd G$.

Let $\mathcal{J} = \{M \lhd G : M \subset N, a \notin M\}$. I claim that $\mathcal{J}$ has a maximal element. Let $\mathcal{K} \subset \mathcal{J}$ be a chain. Then holds $\bigcup_{K\in\mathcal{K}} K$ is normal in G. Also the union is contained in N because all K are. Also a is not contained in any K, so a is also not contained in the union. Therefore holds $\bigcup_{K\in\mathcal{K}} K \in \mathcal{J}$. Thus the chain has an upper bound in $\mathcal{J}$. From Zorn's Lemma follows that $\mathcal{J}$ has a maximal element.

Choose $M \lhd G$ with $M \subset N$ and $a \notin M$ maximal. Consider the following short exact sequence:

$$0 \to M \to G \to G/M \to 0.$$

This sequence is split because G is semisimple. Therefore $G = M \times K$ for some $K \lhd G$. Also: $N = M \times (K \cap N)$. We know $K \cap N \neq \{e\}$ because $a \notin M$.

I claim that $K \cap N$ is a minimal normal subgroup of G. First note: $K \cap N \lhd G$. Let $L \lhd G$, $L \neq \{e\}$ and $L \subset K \cap N$. Note: $M \subsetneq M \times L \subset N$. But M is maximal so $a \in M \times L$. Note that $M \times L \lhd G$, so all conjugates of a (which generate N) are contained in $M \times L$. Thus $N \subset M \times L$. The other inclusion was already given. Therefore holds: $N = M \times L$ and $L = K \cap N$. This proves that $K \cap N$ is a minimal normal subgroup of G. □

Let $\mathcal{N}$ be the set of all minimal normal subgroups of G. Take the following subgroup generated by the elements of $\mathcal{N}$: $H = \langle N : N \in \mathcal{N}\rangle$. It is clear that one has $H \lhd G$. Therefore: $G \cong H \oplus (G/H)$. Denote $R = G/H$.

I claim that $R = \{e\}$. Suppose $R \neq \{e\}$. I will show that R is semisimple and therefore has a minimal normal subgroup (lemma 6.6), which is a contradiction.

Consider the following two short exact sequences, with A and C groups such that the first sequence is short and exact:

$$0 \to A \xrightarrow{f} R \xrightarrow{g} C \to 0$$
$$0 \to H \oplus A \xrightarrow{f'} H \oplus R \xrightarrow{g'} C \to 0$$

Take $f'(h, a) = (h, f(a))$ and $g'(b, c) = g(c)$. It is clear that holds $\operatorname{im}(f') = \ker(g')$. Thus the second sequence is also a short exact sequence.

Note: $G = H \oplus R$ and G is semisimple, thus the second sequence splits. Take $r : G \to H \oplus A$ a retract. Then holds $r \circ f' = \mathrm{id}_{H \oplus A}$. Now I want a retract that gives the identity on A. Define $\pi_A : H \oplus A \to A, (x, y) \mapsto y$. Act π_A on the equation to get: $\pi_A \circ r \circ f' = \pi_A \circ \mathrm{id}_{H \oplus A}$. If I write out the function $\pi_A \circ r \circ f'$ we get:

$$(h, a) \mapsto f'(h, a) \mapsto (h, a) \mapsto a$$

If I restrict the domain of f' to A and r to R, it is clear that the resulting function is the identity. Thus we get $\pi_A \circ r|_R \circ f'|_A = \mathrm{id}_A$. Also $f'|_A = f$. Denote $r' = \pi_A \circ r|_R$. It is now clear that r' is a retract of the first short exact sequence. Thus, using lemma 2.2, the sequence is split. So R is semisimple.

Because $R \neq \{e\}$ follows, with lemma 6.6, that R has a minimal normal subgroup. But H contained all minimal normal subgroups of G so R cannot contain any. This is a contradiction. Thus $R = \{e\}$.

Thus we know $G = H$. To finish the proof of theorem 6.3, I only have to show that every minimal normal subgroup is simple.

Let $M \in \mathcal{N}$ and $K \lhd M$. Let $L \in \mathcal{N}$ with $L \neq M$, then the following 4 statements hold:

1. $M \subset \mathrm{N}_G(K)$ because K is normal in M.
2. $L \subset \mathrm{C}_G(M)$ because M and L centralize each other (follows from lemma 2.3).
3. $\mathrm{C}_G(M) \subset \mathrm{C}_G(K)$ because $K \subset M$.
4. $\mathrm{C}_G(K) \subset \mathrm{N}_G(K)$, this is always true.

Combining these 4 we get the following:

$$\forall L \in \mathcal{N} : L \subset \mathrm{N}_G(K).$$

We know that G is generated by all minimal normal subgroups, so $\mathrm{N}_G(K) = G$. Therefore $K \lhd G$. We know that M is a minimal normal subgroup, thus $K = M$ or $K = \{e\}$. Thus M is simple. $\square$

7 Half-injective groups

Definition 7.1. *A group G is called half-injective iff every short exact sequence $0 \to G \to B \to C \to 0$ half-splits.*

Definition 7.2. *Let R be a ring and I a set. Denote the following additive groups: $R^{(I)} = \bigoplus_{i \in I} R$ and $R^I = \prod_{i \in I} R$.*

The difference between $R^{(I)}$ and R^I lies in the case that I is infinite. The group R^I has every element possible in infinite sequences with elements of R, but in $R^{(I)}$ only sequences are allowed with only finitely many elements unequal to zero.

Before proving the main theorem I need the following lemma.

Lemma 7.3. *Let H be a non-trivial cyclic group and I a set. Then there exists a group A with the following properties:*
(i) $\#A > \#I$.
(ii) $\mathrm{Z}(A) \cong H$.
(iii) $[A, A] \subset \mathrm{Z}(A)$.

Proof. I will prove this lemma by showing an example of such a group and prove that all requirements are met.

Let $m \in \mathbb{Z}_{\geq 0}$ such that $H \cong \mathbb{Z}/m\mathbb{Z}$. Let $R = \mathbb{Z}/m\mathbb{Z}$ the ring with addition and multiplication. Before defining the group A, I need the following inner product:

$$\langle \cdot, \cdot \rangle : R^{(I)} \times R^I \to R, \langle (a_i)_{i \in I}, (b_i)_{i \in I} \rangle = \sum_{i \in I} a_i b_i.$$

Note that this inner product does not give us an infinite sum because there are only finitely many a_i unequal to zero. Define $A = R \times R^{(I)} \times R^I$ with operation $*$ as follows:

$$(r, a, b) * (s, c, d) = (r + s + \langle c, b \rangle, a + c, b + d).$$

I will prove that $(A, *)$ is a group by showing it is the same as a semi-direct product.

Let $A' = (R \times R^{(I)}) \rtimes_\phi R^I$ with the following function:

$$\phi : R^I \to \mathrm{Aut}\left((R \times R^{(I)}, +)\right), b \mapsto ((r, a) \mapsto (r + \langle a, b \rangle, a))$$

Note that I take the automorphism group of the group $R \times R^{(I)}$ with componentwise addition. I will leave it to the reader to verify that ϕ is a homomorphism. Because A' is a semidirect product, it has the following operation:

$$((r, a), b)((s, c), d) = ((r, a) + \phi(b)(s, c), b + d).$$

I claim that A and A' are the same groups, up to notation. The elements of the groups are the same, so I only have to show that the operations are identical:

$$\begin{aligned}((r,a),b)((s,c),d) &= ((r,a)+\phi(b)(s,c),b+d) = ((r,a)+(s+\langle c,b\rangle,c)\\ &= ((r+s+\langle c,b\rangle,a+c),b+d),\\ (r,a,b)*(s,c,d) &= (r+s+\langle c,b\rangle,a+c,b+d).\end{aligned}$$

The above shows that the operations are indeed identical. Thus $(A,*)$ is a group.

Requirement 1. Note that holds: $\#R \geq 2$ thus $\#A \geq 2^{\#I}$. Cantor has proven that holds: $2^{\#I} > \#I$. A proof can be found in the reference [5]. Thus holds $\#A > \#I$.

Requirement 2. To show that $\mathrm{Z}(A)$ is isomorphic to H, I will first determine $\mathrm{Z}(A)$.

Denote $\overline{R} = R \times \{0\} \times \{0\}$. Let $(s,0,0) \in \overline{R}$ and $(r,a,b) \in A$. Then holds:

$$\begin{aligned}(s,0,0)*(r,a,b) &= (s+r+\langle a,0\rangle,0+a,0+b) = (s+r,a,b)\\ (r,a,b)*(s,0,0) &= (r+s+\langle 0,b\rangle,a+0,b+0) = (s+r,a,b)\end{aligned}$$

From this follows that every element in $\overline{R}$ commutes with every other element of A. Thus $\overline{R} \subset \mathrm{Z}(A)$.

With writing out the operation of left and right multiplication, the following statement holds:

$$(r,a,b) \in \mathrm{Z}(A) \Leftrightarrow \forall c \in R^{(I)}, d \in R^I : \langle c,b\rangle = \langle a,d\rangle$$

Let $(r,a,b) \in \mathrm{Z}(A)$ and $k \in I$. Take $c \in R^{(I)}$ with $c_i = 0$ for $i \in I\backslash\{k\}$, $c_k = 1$ and $d \in R^I$ with $d = 0$. Then follows: $b_k = \langle c,b\rangle = \langle a,d\rangle = 0$. So $b_k = 0$. This holds for every $k \in I$, thus $b = 0$.

In an analogous manner to this proof (by switching c and d) follows $a = 0$. Thus $\mathrm{Z}(A) \subset \overline{R}$.

I have proven both inclusions, therefore we now know $\mathrm{Z}(A)$ equals $\overline{R}$. I've chosen R such that holds $R \cong H$ as a group. Also it is clear that holds $\overline{R} \cong R$. Thus $\mathrm{Z}(A) \cong H$.

Requirement 3. Let $f : A \to (R^{(I)} \times R^I, +), (r,a,b) \mapsto (a,b)$. Note that f is a homomorphism because the operation $*$ on the second and third coordinates is equal to componentwise addition. Note: $\overline{R} = \mathrm{Z}(A) \lhd A$.

Also note: $A/\overline{R} \cong R^{(I)} \times R^I$. From Algebra 1 we know that holds: $A/\overline{R}$ is abelian iff $[A,A] \subset \overline{R}$. It is clear that $R^{(I)} \times R^I$ is abelian thus holds $[A,A] \subset \overline{R}$. We know $\overline{R} = \mathrm{Z}(A)$ thus $[A,A] \subset \mathrm{Z}(A)$.

The lemma is proven, but a stronger version of requirement 3 is true: $\mathrm{Z}(A) = [A, A]$. It will not be needed in this thesis, therefore I will not prove it. If interested, the reader can verify this. $\square$

Theorem 7.4. *Let G be a group. Then holds: G is half-injective iff $0 \to G \xrightarrow{i} \mathrm{Aut}(G) \xrightarrow{j} \mathrm{Out}(G) \to 0$ with $i : G \to \mathrm{Aut}(G), \alpha \mapsto (x \mapsto \alpha x \alpha^{-1})$ and j the canonical homomorphism is a half-split short exact sequence.*

Proof. ($\Rightarrow$). Suppose $\mathrm{Z}(G) = \{e\}$. The short exact sequence as given in the theorem is indeed a short exact sequence because $\ker(i) = \mathrm{Z}(G) = \{e\}$. Also the sequence is half-split because G is half-injective.

Suppose $\mathrm{Z}(G) \neq \{e\}$. To obtain a contradiction takes some huge effort. This part of the proof will be very long, hence I will give some guidelines for the proof to make it more understandable. But first some notations and notes.

Take $x \in \mathrm{Z}(G)$ with $H = \langle x \rangle$ such that holds $H \neq \{e\}$. Let A be a group as in lemma 7.3 with $I = G$ and $H = H$. Let $\psi : H \to \mathrm{Z}(A)$ be an isomorphism, which exists according to lemma 7.3. Define $N = \{(\psi(h), h) \in A \times G : h \in H\}$. Note: $N \lhd A \times G$ because $N \subset \mathrm{Z}(A \times G)$. Denote $B = (A \times G)/N$.

I will find a contradiction in three steps:

1. Find a complement of G in $A \times G$ that contains N.
2. Make a homomorphism $\phi : A \to G$ for which holds: $\forall h \in H : \phi(\psi(h)) = h$.
3. Show that ϕ is injective.

Step 1. Define the sequence $0 \to G \xrightarrow{f} B \xrightarrow{g} A/\mathrm{Z}(A) \to 0$ as follows: $f(\alpha) = (e, \alpha)N$ and $g((a, b)N) = a\mathrm{Z}(A)$. I claim that this sequence is a short exact sequence.

First I need to prove that g is well-defined. Let $(x_1, y_1)N, (x_2, y_2)N \in B$ such that $(x_1, y_1)N = (x_2, y_2)N$. I need to show that holds $x_1\mathrm{Z}(A) = x_2\mathrm{Z}(A)$.

Let $\pi : A \times G \to A, (a, b) \mapsto a$. Note: $\pi(N) = \psi(H) = \mathrm{Z}(A)$. Then holds: $\pi((x_1, y_1)N) = \pi(x_1, y_1)\psi(N) = x_1\mathrm{Z}(A)$. From $\pi(x_1, y_1)N = \pi(x_2, y_2)N$ follows $x_1\mathrm{Z}(A) = x_2\mathrm{Z}(A)$. Therefore g is well-defined.

It is clear that f and g are homomorphisms. I will now show that f is injective. Let $x \in \ker(f)$. We know $f(x) = (e, x)N = N$. Thus follows $(e, x) \in N$. There exists precisely one element with e on the first coordinate in N because ψ is an isomorphism. This element is (e, e), thus $(e, e) = (e, x)$ so $x = e$. We now know $\ker(f) = \{e\}$ so f is injective.

Every element $a\mathrm{Z}(A) \in A/\mathrm{Z}(A)$ can be reached by the element $(a, e)N \in B$ so g is surjective. Also holds $\forall x \in G : (g \circ f)(x) = \mathrm{Z}(A)$ thus $\mathrm{im}(f) \subset \ker(g)$.

Let $(a,b)N \in \ker(g)$. From this follows $a\mathrm{Z}(A) = \mathrm{Z}(A)$, from which follows $a \in \mathrm{Z}(A)$. Thus $(a, \psi^{-1}(a)) \in N$. We can now rewrite:

$$(a,b)N = (e, b \cdot \psi^{-1}(a^{-1}))N = f(b \cdot \psi^{-1}(a^{-1}))N \in \mathrm{im}(f)$$

Thus $\ker(g) \subset \mathrm{im}(f)$.

Both inclusions have been proven so $\mathrm{im}(f) = \ker(g)$. All requirements for the sequences to be short exact are met.

Let $s : A/\mathrm{Z}(A) \to B$ be a section of the short exact sequence. This section exists because G is half-injective. Denote $I = \mathrm{im}(s)$. It holds that I is a complement of $f(G)$ in B. I will find a complement of G in $A \times G$ using I.

Define $c : A \times G \to B$ the quotient homomorphism. Note that holds: $c|_G = f$ so $c|_G$ is injective.

Denote $J = c^{-1}(I)$. I claim that J is a complement of G in $A \times G$.

Let $z \in A \times G$. To prove that J is a complement of G it suffices to prove that there exist unique $\alpha \in J$ and $\beta \in G$ such that holds $z = \alpha\beta$. This is equivalent to saying there exists a unique $\gamma \in G$ such that holds $z\gamma^{-1} \in J$.

We know that I is a complement of $f(G) = c(G)$ so there exists a unique $(e,g)N \in c(G)$ such that holds: $c(z)(e,g)^{-1}N \in I$. Now I want to act c^{-1} on this equation, but c is not an isomorphism. However, we do know that $c|_G$ is an injection. Let $x \in G$ such that $c(x) = (e,g)^{-1}N$. This x exists because $(e,g)^{-1}N \in \mathrm{im}(c|_G)$. Also the element x is the only element for which holds $c(x) = (e,g)^{-1}N$. So we get $zx \in J$. The element x is unique so J is a complement of G in $A \times G$.

From this follows: $z \cdot c|_G^{-1}((e,g)^{-1}N) \in J$. Because $c|_G^{-1} = f^{-1}$ is injective and $(e,g)^{-1}N \in \mathrm{im}(f)$ follows that the element $c|_G^{-1}((e,g)^{-1}N)$ exists and is unique. Thus J is a complement of G in $A \times G$.

We also know $N \subset J$ because $(e,e) \in I$ and $c^{-1}(e,e) = N$.

Step 2. Define $\phi : A \to G$ such that holds $J = \{(x, \phi(x)) : x \in A\}$. I will prove that ϕ is well-defined, a homomorphism and that holds $\forall h \in H : \phi(\psi(h)) = h$.

Let $x \in A$. The element $(x,e) \in A \times G$ is a product of an element in $\overline{G}$ and an element in J. Every element in $\overline{G}$ is of the form (e,γ). Let $(\alpha,\beta) \in J$ such that holds $(x,e) = (e,\gamma)(\alpha,\beta)$. Then must follow $\alpha = x$ and $\beta = \gamma^{-1}$. Thus J contains an element with an x on the first coordinate.

We know that x is sent to at least one element with ϕ. To be well-defined, ϕ has to send x to at most one element.

Let $(x,y),(x,z) \in J$. Suppose $y \neq z$. We know $(e,y^{-1}),(e,z^{-1}) \in \overline{G}$ so $(x,e) = (x,y)(e,y^{-1}) = (x,z)(e,z^{-1})$. But if J is a complement of G the

product should be unique. This is a contradiction so $y = z$. Thus ϕ is well-defined.

Let $x, y \in A$. Then holds: $(x, \phi(x))(y, \phi(y)) = (xy, \phi(x)\phi(y)$. But we know $(xy, \phi(x)\phi(y)) \in J$. Using the definition of ϕ we know $\phi(xy) = \phi(x)\phi(y)$. Thus ϕ is a homomorphism.

We know $(\psi(h), h) \in J$ for each $h \in H$ because $N \subset J$. Thus holds $\phi(\psi(h)) = h$.

Step 3. To show that ϕ is injective, I will show that holds $\ker(\phi) = \{e\}$. I will do this with the following lemma:

Lemma 7.5. *Let G be a group and $N \lhd G$ for which holds: $N \cap \mathrm{Z}(G) = \{e\}$ and $[G, G] \subset \mathrm{Z}(G)$. Then holds $N = \{e\}$.*

Proof. Let $g \in G$ and $n \in N$. Then holds $gng^{-1} \in N$ because N is normal. So we also know $gng^{-1}n^{-1} \in N$. This holds for every g and n so $[G, N] \subset N$. It is also clear that holds $[G, N] \subset [G, G] \subset \mathrm{Z}(G)$. From this follows $[G, N] \subset N \cap \mathrm{Z}(G) = \{e\}$.

Therefore holds $gn = ng$. Thus $n \in \mathrm{Z}(G)$, from which follows $n \in N \cap \mathrm{Z}(G)$. Therefore $n = e$ and $N = \{e\}$. □

We know $[A, A] \subset \mathrm{Z}(A)$, so we only need to prove $\ker(\phi) \cap \mathrm{Z}(A) = \{e\}$ to use lemma 7.5.

Let $x \in \ker(\phi) \cap \mathrm{Z}(A)$. Take $h \in H$ such that holds $\psi(h) = x$. This h exists because $x \in \mathrm{Z}(A)$. Then holds, $\phi(\psi(h)) = h$. But x is in the kernel of ϕ, we also know $\phi(\psi(h)) = \phi(x) = e$. Thus $h = e$, from which follows $x = e$. Thus $\ker(\phi) \cap \mathrm{Z}(A) = \{e\}$.

Using lemma 7.5 follows $\ker(\phi) = \{e\}$. Thus ϕ is injective. But we know, from lemma 7.3, that holds $\#A > \#G$. There cannot exist any injective function from A to G, so this is a contradiction. Therefore holds $\mathrm{Z}(G) = \{e\}$, which finishes the proof.

($\Leftarrow$). Let $0 \to G \xrightarrow{f} B \xrightarrow{g} C \to 0$ be an arbitrary short exact sequence. Define $\phi : B \to \mathrm{Aut}(G), b \mapsto (bxb^{-1})$ and $s : \mathrm{Out}(G) \to \mathrm{Aut}(G)$ a section. Let $H = \phi^{-1}(s(\mathrm{Out}(G))) \subset B$. I claim that $g|_H$ is an isomorphism.

Let $x \in \ker(g|_H)$. We know $\ker(g) = G$ so $\ker(g|_H) \subset G$. Thus $x \in G$. Note: $\phi(x) \in i(G)$ because $\phi|_G = i$. Also note: $\phi(x) \in s(\mathrm{Out}(G))$ because this is how we defined H. Thus holds: $\phi(x) \in i(G) \cap s(\mathrm{Out}(G))$. But we already know that holds $i(G) \cap s(\mathrm{Out}(G)) = \{\mathrm{id}_G\}$ because s is a section.

From $\phi(x) = \mathrm{id}_G$ follows: $\forall y \in G : xyx^{-1} = y$, which is equivalent to $xy = yx$. Thus $x \in \mathrm{Z}(G)$. Thus $x = e$, from which follows $\ker(g|_H) = \{e\}$

and so $g|_H$ is injective.

Let $c \in C$. Choose $b \in B$ such that holds $g(b) = c$. Consider the elements $\phi(b)$ and $(s \circ j)(\phi(b))$. Both elements are sent to $j(\phi(b))$ with j, but the elements don't have to be the same element. There exists a $\gamma \in \ker(j)$ such that holds $\gamma \cdot \phi(b) = (s \circ j)(\phi(b))$. Thus holds $\gamma \cdot \phi(b) \in s(\mathrm{Out}\,(G))$.

Let $\gamma' \in G$ such that holds $i(\gamma') = \gamma$. From $\phi|_G = i$, and using that ϕ is a homomorphism, follows $i(\gamma')\phi(b) = \phi(\gamma' b)$. This is an element in $s(\mathrm{Out}\,(G))$ so, using the definition of H, we get $\gamma' b \in H$. Note $\gamma' \in \ker(g)$ so $g|_H(\gamma' b) = c$. Thus every element from C can be reached by an element in H, so $g|_H$ is surjective.

We now know that $g|_H$ is an isomorphism. It is clear that $g|_H^{-1}$ is a section, thus G is half-injective. □

8 Injective groups

Definition 8.1. *A group G is called injective iff every short exact sequence $0 \to G \to B \to C \to 0$ splits.*

Theorem 8.2. *Let G be a group. Then holds: G is injective iff G is complete.*

Proof. ($\Rightarrow$). We know that G is half-injective so $\mathrm{Z}\,(G) = \{e\}$ (7.4). Also the sequence sequence $0 \to G \xrightarrow{i} \mathrm{Aut}\,(G) \xrightarrow{j} \mathrm{Out}\,(G) \to 0$, as in theorem 7.4, is a short exact sequence. For G to be complete, I only have to show $\mathrm{Out}\,(G) = \{e\}$.

I will prove that holds $\mathrm{C}_{\mathrm{Aut}\,(G)}(\mathrm{Inn}\,(G)) = \{\mathrm{id}_G\}$. First I will show that holds $\forall \alpha \in G, \sigma \in \mathrm{Aut}\,(G) : \sigma \circ i(\alpha) \circ \sigma^{-1} = i(\sigma(\alpha))$. Let $x \in G$. Then:

$$\begin{aligned}(\sigma \circ i(\alpha) \circ \sigma^{-1})(x) &= (\sigma \circ i(\alpha))(\sigma^{-1}(x)) \\ &= \sigma(\alpha\sigma^{-1}(x)\alpha^{-1}) \\ &= \sigma(\alpha)x\sigma(\alpha)^{-1} \\ &= i(\sigma(\alpha))(x)\end{aligned}$$

Let $\phi \in \mathrm{C}_{\mathrm{Aut}\,(G)}(\mathrm{Inn}\,(G)) = \{\mathrm{id}_G\}$ and $\alpha \in G$. Then holds $\phi \circ i(\alpha) \circ \phi^{-1} = i(\alpha)$, because that is how I chose ϕ. But we also know, as proven above, $\phi \circ i(\alpha) \circ \phi^{-1} = i(\phi(\alpha))$. We know that i is injective, so $\phi(\alpha) = \alpha$. This is true for all $\alpha \in G$, thus $\phi = \mathrm{id}_G$. So $\mathrm{C}_{\mathrm{Aut}\,(G)}(\mathrm{Inn}\,(G)) = \{\mathrm{id}_G\}$.

The sequence $0 \to G \xrightarrow{i} \mathrm{Aut}\,(G) \xrightarrow{j} \mathrm{Out}\,(G) \to 0$ is split, because G is injective. Let $s : \mathrm{Out}\,(G) \to \mathrm{Aut}\,(G)$ be a section such that $s(\mathrm{Out}\,(G)) \lhd$

$\mathrm{Aut}\,(G)$. This section exists because of lemma 2.4. Also holds $\mathrm{Inn}\,(G) \lhd \mathrm{Aut}\,(G)$. This is always true, see [7].

We know $s(\mathrm{Out}\,(G)) \cap \mathrm{Inn}\,(G) = \{e\}$, thus $[s(\mathrm{Out}\,(G)), \mathrm{Inn}\,(G)] = \{e\}$ (lemma 2.3). Therefore $s(\mathrm{Out}\,(G)) \subset \mathrm{C}_{\mathrm{Aut}\,(G)}(\mathrm{Inn}\,(G)) = \{\mathrm{id}_G\}$. So $s(\mathrm{Out}\,(G)) = \{\mathrm{id}_G\}$. Because s is injective follows $\mathrm{Out}\,(G) = \{\mathrm{id}_G\}$.

($\Leftarrow$). Let $0 \to G \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence. Let $\phi : B \to \mathrm{Aut}\,(G), b \mapsto (x \mapsto bxb^{-1})$. Note that this function is well-defined because $G \lhd B$. Because f is injective, I consider $G \subset B$ with f the inclusion. Note: $\phi|_G$ is an isomorphism because G is complete. Consider the following diagram:

$$\begin{array}{ccc} G & \xrightarrow{f} & B \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle \phi} \\ \mathrm{Aut}\,(G) & = & \mathrm{Aut}\,(G) \end{array}$$

I will define a retract from B to G through $\mathrm{Aut}\,(G)$. Let $r = \phi|_G^{-1} \circ \phi$.

It is clear that holds $r \circ f = \mathrm{id}_G$. Also r is an homomorphism because ϕ is. Thus r is a retract and, using lemma 2.2, the sequence is split. $\square$

9 References

[1] `http://en.wikipedia.org/wiki/Projective_module`
`http://en.wikipedia.org/wiki/Semisimple_module`
`http://en.wikipedia.org/wiki/Injective_module`

[2] Serge Lang, *Algebra*, Springer, 2002

[3] `http://www.math.leidenuniv.nl/scripties/BachSluis_van_der.pdf`

[4] `http://planetmath.org/normalsubgroupsofthesymmetricgroups`

[5] Cantor theorem. B.A. Efimov, M.I. Voitsekhovskii (originator), Encyclopedia of Mathematics, Kluwer Academic Publishers, 2002

[6] R. Wilson, *The Finite Simple Groups*, Springer, 2009

[7] `http://www.proofwiki.org/wiki/Inner_Automorphisms_form_Normal_Subgroup`