Semisimplicity and finite groups

Michielsen, J.R.

Joost Michielsen

Semisimplicity and finite groups

Bachelor thesis

Date: 10-06-2008

Thesis advisor: Hendrik Lenstra

Mathematisch Instituut, Universiteit Leiden

Contents

1 Introduction

This thesis deals with some group theoretic questions that can be solved using the theory of so called semisimplicity. In this introduction we will state the theorems to be proved. We will first give the definitions which are essential for these theorems.

1.1. Definition. For any ring R, a left R-module M is called semisimple if every short exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

of R-modules splits.

1.2. Definition. Let G be a group. A G-module is an abelian group M equipped with a group homomorphism $G \to \mathrm{End}_{\mathbb{Z}} M$.

Note that a module over a group is a module over a ring in a natural way, since we can extend the group homomorphism $G \to \mathrm{End}_{\mathbb{Z}} M$ to a ring homomorphism $\mathbb{Z}[G] \to \mathrm{End}_{\mathbb{Z}} M$. So all the definitions and theorems about modules over rings can also be used for modules over groups.

Now the theorems can be formulated.

1.3. Theorem. *Let G be a finite group and let M be a simple G-module. Then* $\mathrm{im}(\mathbb{Z}[G] \to \mathrm{End}_{\mathbb{Z}} M)$ *is (as a ring) isomorphic to a matrix ring over a finite field.*

1.4. Theorem. *Let G be a finite group and let $A \triangleleft G$ be cyclic such that A is a maximal abelian normal subgroup of G. Let C be the centralizer of A in G. Let N be normal in G. Then, for any $B \triangleleft G$ with $A \subset B \subset C$ such that B/A is abelian, B/A is a semisimple N-module with $N \to \mathrm{End}_{\mathbb{Z}} B/A$ given by $n \mapsto (x \mapsto nxn^{-1})$.*

To prove these theorems, the theory of semisimplicity, which is worked out in the second chapter, will be essential. The third and the fourth chapter are devoted to the proofs of the theorems.

This thesis has been written as a result of the course 'Permutation groups' taught by Hendrik Lenstra in the fall of 2007 ([6]). The aim of this course was to give an upper bound for the size of a solvable permutation group in terms of the number of elements being permuted. It turned out that it is sufficient to look at a smaller class of solvable groups G, namely solvable groups G together with a faithful primitive G-module (see [6] for the definition of 'primitive'). Solvable groups with a primitive module have some special and interesting properties, which make it is possible to give a strong bound on the size of a solvable permutation group in terms of the number of elements being permuted. The theorems that are proved in this thesis apply to these kind of groups, but we will not go into the specific consequences for this special case.

2 Semisimplicity

This section deals with the theory of semisimplicity, e.g. semisimple modules and semisimple rings. For any ring R, by an R-module we shall mean a left R-module.

2.1 Semisimple modules

We recall the definition from the introduction.

2.1. Definition. An R-module M is called semisimple if every short exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

of R-modules splits.

2.2. Theorem. *Let M be a semisimple R-module, and let $0 \longrightarrow M' \xrightarrow{f} M \longrightarrow M'' \longrightarrow 0$ be an exact sequence of R-modules. Then M' and M'' are semisimple. Also, if $M \neq 0$, then M contains a simple submodule.*

Proof. First we prove the semisimplicity of M'. Let $0 \longrightarrow A \xrightarrow{g} M' \longrightarrow B \longrightarrow 0$ be exact. If f is the map in the theorem, then we know that $h = fg$ is injective. So we can construct the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{g} & M' & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle f} & & & & \\ 0 & \longrightarrow & A & \xrightarrow{h} & M & \longrightarrow & M/A & \longrightarrow & 0. \end{array}$$

By the definition of M we see that the lower sequence splits, so there is a retraction $s : M \to A$. Now sf is a retraction of the upper sequence.
The proof of the second assertion is easy now: we know that $M \cong M' \oplus M''$, so we can just swap M' and M'' in the sequence.

To prove the last assertion, take $x \in M$ not equal to 0, and consider the left ideal $\mathfrak{a} = \mathrm{Ann}(x) \subset R$. Because $1 \cdot x = x \neq 0$ we know that $\mathfrak{a} \subsetneq R$. So there is a maximal left ideal $\mathfrak{m}$ such that $\mathfrak{a} \subset \mathfrak{m} \subset R$. Since $R/\mathfrak{a} \cong Rx$ as R-modules, we know by the second statement that $R/\mathfrak{a}$ is semisimple. Therefore, the exact sequence

$$0 \longrightarrow \mathfrak{m}/\mathfrak{a} \longrightarrow R/\mathfrak{a} \longrightarrow R/\mathfrak{m} \longrightarrow 0$$

splits, so we find $Rx \cong R/\mathfrak{a} \cong \mathfrak{m}/\mathfrak{a} \oplus R/\mathfrak{m}$. Now the image of $R/\mathfrak{m}$ in Rx is a simple submodule of M. □

2.3. Theorem. *For every R-module M the following assertions are equivalent:*
(1) *M is semisimple.*
(2) *For every submodule $N \subset M$ there exists $N' \subset M$ such that $M = N \oplus N'$.*
(3) *M is the sum of a family of simple submodules of M.*
(4) *M is the direct sum of a family of simple submodules of M.*

Proof. (1) $\Leftrightarrow$ (2): Trivial.

(2) $\Rightarrow$ (3): Let M_0 be the sum of all simple submodules of M. We have $M = M_0 \oplus N$ for a certain $N \subset M$. Because N cannot have a simple submodule, we know by 2.2 that $N = 0$. Hence we have $M_0 = M$, so M is the sum of a family of simple submodules of M.

Now the following lemma is useful.

2.4. Lemma. *Let $\{M_i\}_{i\in I}$ be a family of simple R-modules and let M be an R-module. Let $f : \bigoplus_{i\in I} M_i \to M$ be an R-homomorphism. Then there is a subset $J \subset I$ such that the restriction map $g = f|_{\bigoplus_{j\in J} M_j}$ is injective and* $\operatorname{im} f = \operatorname{im} g$.

Proof. Let $\{M_i\}_{i\in I}$ and f be as in the theorem. Take with Zorn's lemma a maximal subset $J \subset I$ such that $g = f|_{\bigoplus_{j\in J} M_j}$ given by summation is injective. We are going to prove that $\operatorname{im} g = \operatorname{im} f$. We know for any $i \in I$ that $\operatorname{im} g \cap M_i = 0$ or $\operatorname{im} g \cap M_i = M_i$ because of the simplicity of M_i. If $\operatorname{im} g \cap M_i = 0$ we can add M_i to our direct sum and the map is still injective, contradicting the maximality of J. So for any $i \in I$, we see that $\operatorname{im} g \cap M_i = M_i$. This shows that $\operatorname{im} g = \operatorname{im} f$. □

The rest is easy now:

(3) $\Rightarrow$ (4): In this case the map $f : \bigoplus_{i\in I} M_i \to M$ given by summation is a surjective R-homomorphism, so by 2.4 there is a $J \subset I$ such that the map $f|_{\bigoplus_{j\in J}}$ is an R-isomorphism, showing that $\bigoplus_{j\in J} M_j = M$.

(4) $\Rightarrow$ (2): Let N be an arbitrary submodule of $M = \bigoplus_{i\in I} M_i$ with M_i simple. Now consider the natural map $f : \bigoplus_{i\in I} M_i \to M/N$. By 2.4 we know a $J \subset I$ exists such that $f|_{\bigoplus_{j\in J} M_j}$ is an R isomorphism. This immediately implies that $M = N \oplus (\bigoplus_{j\in J} M_j)$. □

To give an example, we will look at the case $R = \mathbb{Z}$. We know that the simple $\mathbb{Z}$-modules are the groups $\mathbb{Z}/p\mathbb{Z}$ for a prime number p. We see that a $\mathbb{Z}$-module is semisimple if and only if it is of the form $\bigoplus_{i\in I} \mathbb{Z}/p_i\mathbb{Z}$ with all p_i prime.

2.2 Semisimple rings

Next to semisimple modules, we have semisimple rings.

2.5. Definition. A ring R is called semisimple if R is semisimple as an R-module.

The following lemma enables us to prove an interesting theorem about semisimple rings.

2.6. Lemma. *Every direct sum of semisimple modules is again semisimple.*

Proof. A direct sum of semisimple modules is still a sum of simple modules, so it is semisimple. □

2.7. Theorem. *A ring R is semisimple if and only if every R-module is semisimple.*

Proof. The "$\Longleftarrow$"-implication is trivial. To prove "$\Longrightarrow$", recall that every R-module is a quotient of a free R-module. Every free R-module is semisimple by 2.6. Because every quotient of a semisimple module is semisimple, the desired result follows. □

As an example, we will give the proof of a theorem which is fundamental in representation theory. We will not be using it in this thesis.

2.8. Theorem. *Let G be a finite group and k be a field such that the characteristic of k does not divide $\#G$. Then the group ring $k[G]$ is semisimple.*

Proof. Assume

$$0 \longrightarrow M' \longrightarrow M \xrightarrow{p} M'' \longrightarrow 0$$

to be an exact sequence of $k[G]$-modules. Then a k-linear map $q : M'' \to M$ exists such that $pq = \mathrm{id}_{M''}$. If we can construct a $k[G]$-linear map $q' : M'' \to M$ such that $pq' = \mathrm{id}_{M''}$ we are done. We assert that

$$q' = \frac{1}{\#G} \sum_{\sigma \in G} \sigma q \sigma^{-1},$$

where the σ's are considered to be maps, is such a map. It is immediately clear that this map q' is a k-homomorphism. Moreover,

$$pq' = \frac{1}{\#G} \sum_{\sigma \in G} p(\sigma q \sigma^{-1}) = \frac{1}{\#G} \sum_{\sigma \in G} \sigma \, \mathrm{id}_{M''} \, \sigma^{-1} = \mathrm{id}_{M''}$$

because p is a $k[G]$-homomorphism. This shows that q' also gives a section of the exact sequence above. Furthermore, for all $\tau \in G$ we have

$$\tau q' = \frac{1}{\#G} \sum_{\sigma \in G} \tau \sigma q \sigma^{-1} = \left(\frac{1}{\#G} \sum_{\sigma \in G} \tau \sigma q \sigma^{-1} \tau^{-1} \right) \tau = q' \tau$$

This proves that q' is also $k[G]$-linear. We conclude that every short exact sequence of $k[G]$-modules splits. □

2.3 The classification of semisimple rings

For rings, it turns out that being semisimple is quite a strong condition. In fact, the semisimple rings can be classified.

2.9. Theorem. *A ring R is semisimple if and only if it is isomorphic to a finite direct product of matrix rings over division rings.*

The aim of this paragraph is to prove this theorem, which will turn out to be surprisingly elementary. We will make use of the following important lemmas. By R^{opp} we mean the ring R together with the ring multiplication $*$ such that $x * y = yx$.

2.10. Lemma. *For any ring R, we have a ring isomorphism $R \xrightarrow{\sim} (\mathrm{End}_R R)^{\mathrm{opp}}$ given by $r \mapsto (x \mapsto xr)$.*

Proof. Trivial. □

2.11. Lemma. *Let R be an arbitrary ring, let $\{M_i\}_{i\in I}$ be a collection of pairwise non-isomorphic simple R-modules, and let $m_i \in \mathbb{Z}_{\geq 0}$ for all $i \in I$. Then there is a ring isomorphism*

$$\begin{aligned} \mathrm{End}_R\left(\bigoplus_{i\in I} M_i^{m_i}\right) &\xrightarrow{\sim} \prod_{i\in I} \mathrm{End}_R(M_i^{m_i}) \\ f &\longmapsto \bigoplus_{i\in I} f|_{M_i} \end{aligned}$$

Proof. Note that every homomorphism of simple R-modules is either the zero map or an isomorphism. □

By $M(n, R)$ we mean the ring of $n \times n$ matrices over a ring R. We assume n to be finite.

2.12. Lemma. *Let R be an arbitrary ring and E an R-module. Fix $n \in \mathbb{Z}_{>0}$. For every $\varphi \in \mathrm{End}_R(E^n)$ we say (denoting E^n as $\bigoplus_{i\leq n} E_i$) that $\varphi_{ij} = \pi_i \circ (\varphi|_{E_j})$ where π_i is the restriction of the projection map $E^n \mapsto E_i$ to $\varphi(E_j)$. Then we have a ring isomorphism $\mathrm{End}_R E^n \to M(n, \mathrm{End}_R(E))$ given by*

$$\varphi \longmapsto \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & & \vdots \\ \varphi_{n1} & \cdots & \varphi_{nn} \end{pmatrix}$$

Proof. Trivial. □

Now we are ready to prove the 'only if' part of Theorem 2.9.

2.13. Theorem. *Let R be a semisimple ring. Then R is isomorphic to a finite product of matrix rings over division rings.*

Proof. Let R be semisimple. This means that R is, when viewed as an R-module, isomorphic to the direct sum of simple R-modules. Because R is finitely generated as an R-module, this sum will be finite. So we can say $R \cong_R \bigoplus_{i \leq n} M_i^{m_i}$ with $M_i \ncong M_j$ if $i \neq j$. Using 2.10 and 2.11 we see

$$R \cong (\operatorname{End}_R R)^{\text{opp}} \cong (\operatorname{End}_R \bigoplus_{i \leq n} M_i^{m_i})^{\text{opp}} \cong \prod_{i \leq n} (\operatorname{End}_R M_i^{m_i})^{\text{opp}}.$$

Using lemma 2.12, we have

$$R \cong \prod_{i \leq n} M(m_i, D_i)^{\text{opp}}$$

where the D_i are the division rings $\operatorname{End}_R(M_i)$. Furthermore, for any matrix ring $M(n, D)$, we have a ring isomorphism $(M(n, D))^{\text{opp}} \to M(n, D^{\text{opp}})$ given by $A \mapsto A^T$. Because D^{opp} is clearly also a division ring, we are done. □

We still have to prove the converse.

2.14. Theorem. *Let R be a ring and M a faithful simple R-module that is finitely generated as an $\operatorname{End}_R M$-module. Then R is semisimple.*

Proof. Let $S = \{s_1, \ldots, s_n\} \subset M$ be a set of generators for M over $\operatorname{End}_R M$. Then we know by 2.6 that M^S is a semisimple module. Moreover, the R-homomorphism

$$\begin{array}{ccc} R & \longrightarrow & M^S \\ r & \longmapsto & (rs_1, \ldots, rs_n) \end{array}$$

is injective: Suppose $rs_i = 0$ for all generators of R as an $\operatorname{End}_R M$-module. Then we can write every $x \in M$ as $\varphi_1(s_1) + \ldots + \varphi_n(s_n)$ for $\varphi_i \in \operatorname{End}_R M$. So we have

$$rx = r(\varphi_1(s_1) + \ldots + \varphi_n(s_n)) = \varphi_1(rs_1) + \ldots + \varphi_n(rs_n) = 0.$$

So we see that $rx = 0$ for all $x \in M$. By the faithfulness of M, we conclude that $r = 0$. This shows that R is (as an R-module) isomorphic to a submodule of M^S, hence R is semisimple. □

2.15. Lemma. *For any matrix ring $M(n, D)$ with $n > 0$ and D a division ring, the $M(n, D)$-module D^n is faithful and simple. Also, D^n is finitely generated as $\operatorname{End}_{M(n,D)}(D^n)$-module.*

Proof. From linear algebra we know that $M(n, D)x = D^n$ for any $x \in D^n$ with $x \neq 0$. This shows that D^n is simple. Also, we know that the only matrix A such that $Ax = 0$

for all $x \in D^n$ is the zero matrix. This shows that D^n is faithful. We easily see that D^n is finitely generated as a $\mathrm{End}_{M(n,D)}(D^n)$-module, because if we view $S \subset \mathrm{End}_{M(n,D)}(D^n)$ as the ring consisting of the maps $\{(x \mapsto xd) : d \in D\}$ then D^n can be generated by n elements as an S-module. $\square$

2.16. Theorem. *Any finite product of matrix rings over division rings is semisimple.*

Proof. We know by 2.14 and 2.15 that any matrix ring over a division ring is semisimple. Since by 2.6 any finite product of semisimple rings is semisimple, the statement follows. $\square$

This concludes the 'if' part of the proof of 2.9, hence the whole theorem has been proved.

2.4 Left and right semisimplicity

The theorem that has just been proved has a surprising consequence. We know that left and right R-modules are different things, and the notion of a semisimple ring is a priori asymmetric: there does not appear to be any reason for a left semisimple ring to be right semisimple (definition clear), and vice versa. But they turn out to be the same! It is clear that any left-semisimple ring R gives rise to a right semisimple ring R^{opp}, and we know that for any finite product of matrix rings over division rings $\prod_{i \leq n} M(n_i, D_i)$, the ring $(\prod_{i \leq n} M(n_i, D_i))^{\mathrm{opp}}$ is also a finite product of matrix rings over division rings. So, the notions of left semisimplicity and right semisimplicity are equivalent.

Note that not all the theorems in this section have been stated in the sharpest and most general way possible, we basically just chose the steps which we use in the next two section. For a more detailed treatment of semisimplicity, see [2], chapter XVIII or [3], chapter 9.

3 The ring generated by a finite group with a simple module

3.1 The first theorem

The goal of this section is to give a proof of Theorem 1.3. For the proof, the following famous theorem is essential. The proof we give is due to Witt, 1931 ([7]).

3.1. Theorem. *(Wedderburn) Every finite division ring is a field.*

To prove the theorem, we will make use of some lemma's.

3.2. Lemma. *Consider $a \in \mathbb{Z}_{>1}$ and $d, m \in \mathbb{Z}_{>0}$. Then we have $a^d - 1 \mid a^m - 1$ if and only if $d \mid m$.*

Proof. "$\Longleftarrow$": If $d \mid m$, then $\frac{a^m-1}{a^d-1} = \sum_{i=0}^{\frac{m}{d}} a^{id}$.
"$\Longrightarrow$": We know that a has order d in $\mathbb{Z}/(a^d-1)\mathbb{Z}$, because $a^d \equiv 1 \mod a^d - 1$ and $a^r - 1 < a^d - 1$ for $0 < r < d$. Also we see that $a^m \equiv 1 \mod a^d - 1$. By group theory, this implies that $d \mid m$. □

Recall that the cyclotomic polynomial $\Phi_n(X) \in \mathbb{Z}[X]$ is defined as $\prod_{k \in \mathbb{Z}/n\mathbb{Z}^*}(X - \zeta_n^k)$ with $\zeta_n \in \mathbb{C}$ a primitive n-th root of unity. See [5] for example.

3.3. Lemma. *Let $n \in \mathbb{Z}_{>0}$. Then for any $d \mid n, d \neq n$, we have that $\Phi_n(X) \mid \frac{X^n-1}{X^d-1}$.*

Proof. We have $X^n - 1 = \prod_{k \in \mathbb{Z}/n\mathbb{Z}}(X - \zeta_n^k)$ and $X^d - 1 = \prod_{k \in \frac{n}{d}(\mathbb{Z}/n\mathbb{Z})}(X - \zeta_n^k)$, and because $\frac{n}{d} \notin (\mathbb{Z}/n\mathbb{Z})^*$ we immediately see that dividing $X^n - 1$ out by $X^d - 1$ will not remove any zero ζ_n^k with $k \in (\mathbb{Z}/n\mathbb{Z})^*$. □.

Proof of 3.1. Let D be a finite division ring, and let $F \subset D$ be the center of D. It follows immediately that F is a field and D is a vector space over F, so D has q^n elements for q a prime power and $n \in \mathbb{Z}_{>0}$. Now we are going to count the sizes conjugacy classes of the group D^*.

By [4] we know that the size of any conjugacy class of D^* divides the order of D^*, and that the sum of the sizes of the conjugacy classes of D^* is equal to D^*. Also, the size of the conjugacy class of an element x is equal to $\frac{\#D^*}{\#\mathcal{C}(x)}$ with $\mathcal{C}(x)$ the centralizer of x in D^*. In our case, this means

$$\#D^* = \sum_{x \in \mathcal{B}} \frac{\#D^*}{\#\mathcal{C}(x)}$$

where $\mathcal{B}$ is a set of representatives for the conjugacy classes of D^*.

Take an arbitrary $x \in D$. Now $\mathcal{C}(x)$ is also a division ring, so it must have q^d elements for some $d \in \mathbb{Z}_{>0}$. Since $\mathcal{C}(x)^*$ is a subgroup of D^*, it follows that $q^d - 1 \mid q^n - 1$ and by 3.2 that $d \mid n$. So we have

$$\#D^* = q^n - 1 = q - 1 + \sum_{i \in I} \frac{q^n - 1}{q^{d_i} - 1}$$

with I a certain finite sequence of divisors of n that are not equal to n. The $q - 1$ comes from $\mathbb{F}_q^*$, we know that $\mathbb{F}_q^*$ is central in D^* and conjugation classes of central elements consist of a single element. Since $i \mid n$ and $i \neq n$ for all $i \in I$, Lemma 3.3 tells us that $\Phi_n(q)$ is a divisor of $\frac{q^n-1}{q^i-1}$ for all i. Because $\Phi_n(q) \mid q^n - 1$, this implies that $\Phi_n(q) \mid q - 1$. This is impossible if $n > 1$, since $|q - \zeta_n^k| > q - 1$ for all $k \in (\mathbb{Z}/n\mathbb{Z})^*$ if $n > 1$. We conclude that $n = 1$, so D must be a one-dimensional vector space over F. Hence D is a field itself. □

The theorem of Wedderburn has the following interesting corollary.

3.4. Corollary. *Let R be a finite ring and let M be a faithful simple R-module. Then R is a matrix ring over a finite field.*

Proof. Because R is finite, every simple module over R is finite. This means we can apply theorem 2.14 to show that R is semisimple. By 2.9 and 3.1 we know that R is the finite product of matrix rings over finite fields. If we can show that $Z(R)$, the center of R, has no zero divisors we are done. Note that for any $r \in Z(R)$, the map $M \to M$ given by $r \mapsto rx$ is an R-linear map. This implies that $Z(R) \subset \operatorname{End}_R M$, which is by Schur's lemma a division ring. This shows that R is a matrix ring over a finite field. □

3.5. Lemma. *Let G be a finite group and let M be a simple G-module. Then M is finite.*

Proof. Because G is finite, we know that M is finitely generated as a $\mathbb{Z}$-module. If M is infinite, then the rank of M (as an abelian group) must be greater than zero. This implies that $2M \subsetneq M$ is a non-trivial submodule of M, which contradicts the simplicity of M. This shows that M must be finite. □

Note that this statement is not generally true if G is not finite. For example, $\mathbb{Q}$ is a simple $\mathbb{Z}$-module that is not finite.

3.6. Theorem. *(First theorem of the introduction) Let G be a finite group and let M be a simple G-module. Then* $\operatorname{im}(\mathbb{Z}[G] \to \operatorname{End}_{\mathbb{Z}} M)$ *is (as a ring) isomorphic to a matrix ring over a finite field.*

Proof. Let R be the ring $\operatorname{im}(\mathbb{Z}[G] \to \operatorname{End}_{\mathbb{Z}} M)$. Then it follows immediately that M is a faithful simple R-module. By lemma 3.5 we know that $R \subset \operatorname{End}_{\mathbb{Z}} M$ is a finite ring. Now 3.4 immediately gives the desired result. □

4 Semisimple modules inside finite groups

4.1 The second theorem

In this section we consider a finite group G and let $A \triangleleft G$ be cyclic such that A is a maximal abelian normal subgroup of G. Then, for any $B \triangleleft G$ such that $A \subset B$ and B is contained in the centralizer of A, we try to use the theory of semisimplicity to understand the group B/A.
The first lemma can also be found in [6].

4.1. Lemma. *Let G be a finite group and let $A \triangleleft G$ be cyclic such that A is a maximal abelian normal subgroup of G. Let $B \triangleleft G$ such that $A \subset B$ and B is contained in the centralizer of A in G and B/A is abelian. Then we have a group isomorphism $B/A \longrightarrow \mathrm{Hom}(B/A, A)$ given by $\beta A \longmapsto (\delta \mapsto \beta\delta\beta^{-1}\delta^{-1})$.*

Proof. The group B/A is abelian, giving us that $[B, B] \subset A \subset Z(B)$ (since B is contained in the centralizer of A). Now it is easy to see that $B \times B \longrightarrow A$, given by $(\beta, \delta) \mapsto \beta\delta\beta^{-1}\delta^{-1}$, is a bilinear map. This already gives us the homomorphism

$$\begin{array}{rcl} \psi : B & \longrightarrow & \mathrm{Hom}(B, A) \\ \beta & \longmapsto & (\delta \mapsto \beta\delta\beta^{-1}\delta^{-1}). \end{array}$$

Note that $\ker\psi = Z(B)$. Since $A \subset Z(B)$ and $Z(B)$ is normal in G (it is a characteristic subgroup of the normal subgroup B), the maximality of A tells us that $A = Z(B)$. This means that $A = \ker\psi$, and we have a natural injection

$$\begin{array}{rcl} \varphi : B/A & \longrightarrow & \mathrm{Hom}(B/A, A) \\ \beta A & \longmapsto & (\delta A \mapsto \beta\delta\beta^{-1}\delta^{-1}) \end{array}$$

making the following diagram commutative, with i the natural inclusion:

$$\begin{array}{ccc} B & \xrightarrow{\psi} & \mathrm{Hom}(B, A) \\ \downarrow & & \uparrow{\scriptstyle i} \\ B/A & \xrightarrow{\varphi} & \mathrm{Hom}(B/A, A). \end{array}$$

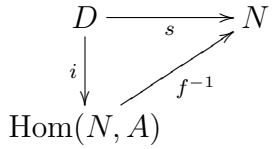
Now we claim that φ is an isomorphism.
We only have to show surjectivity. We immediately see that there are at least $\#(B/A)$ homomorphisms $B/A \to A$. By just counting all possible homomorphisms between an abelian group and a cyclic group, using the structure theorem for finite abelian groups, we see that $\#\mathrm{Hom}(B/A, A) \leq \#(B/A)$, which proves surjectivity. This shows that φ is an isomorphism. □

4.2. Definition. Let D be an abelian group and let A be an abelian group. We call a bilinear map map $[\,,\,] : D \times D \to A$ non-degenerate if the map $f : D \to \mathrm{Hom}(D, A)$ given by $d \mapsto (x \mapsto [d, x])$ is an isomorphism.

4.3. Definition. Let D be an abelian group, A a cyclic group and $[\,,\,] : D \times D \to A$ a bilinear map. Then, for any subgroup $N \subset D$, we define $N^{\perp}$ to be the set $\{d \in D : [d, n] = 0 \text{ for all } n \in N\}$.

4.4. Lemma. *Let D be a finite abelian group, A an abelian group and $[\,,\,] : D \times D \to A$ a bilinear map. Let $N \subset D$ be a subgroup such that $[\,,\,]|_{N\times N}$ is non-degenerate. Then $D = N \oplus N^{\perp}$.*

Proof. Let $f^{-1} : \mathrm{Hom}(N, A) \to N$ the inverse map of 4.2 given by $(x \mapsto nx) \mapsto n$. We have the following diagram



with i the natural map and s the map making the diagram commutative.
Now we consider the following exact sequence (with the natural maps):

$$0 \longrightarrow N \longrightarrow D \longrightarrow D/N \longrightarrow 0.$$

It is clear that the map $s : D \to N$ is a retraction. Moreover, $\ker s = \ker f^{-1} \circ i = \ker i = \{d \in D : dnd^{-1}n^{-1} = 0 \text{ for all } n \in N\} = N^{\perp}$. This immediately implies that $D = N \oplus N^{\perp}$, concluding the proof. □

4.5. Lemma. *Let A, B as in 4.1. Then the map $G \to \mathrm{End}_{\mathbb{Z}}(B/A)$ given by $\sigma \mapsto \sigma x \sigma^{-1}$ makes B/A into a semisimple G-module.*

Proof. The commutator map $[\,,\,] : B/A \times B/A \to A$ is clearly bilinear, and in 4.1 was proved that $[\,,\,]|_{N\times N}$ is non-degenerate for any $A \subset N \subset B$ such that N is normal in G, so the conditions of 4.4 are satisfied. The G-submodules of B/A are precisely the groups N/A such that $A \subset N \subset B$ and $N/A \triangleleft G/A$, or, equivalently, the groups N such that $A \subset N \subset B$ and $N \triangleleft G$. By 4.1 we know that $(N/A) \xrightarrow{\sim} \mathrm{Hom}((N/A), A)$ given by $\beta A \mapsto [\beta, \delta]$. Now 4.4 tells us that $B/A = N/A \oplus (N/A)^{\perp}$. Moreover, it is clear that $(N/A)^{\perp}$ is a sub-G-module of B/A, since $(N/A)^{\perp} = \mathcal{C}_B(N)/A$, with $\mathcal{C}_B(N)$ the centralizer of N in B, which is normal in G. Now the conditions of 2.3(2) are satisfied, so the lemma has been proved. □

4.6. Lemma. *Let G be a finite group and let M be a semisimple G-module. Then, for any $N \triangleleft G$, it follows that M is a semisimple N-module.*

Proof. We know that M is the direct sum of simple G-modules, so it is sufficient to restrict to the case that M is a simple G-module. Choose a simple N-submodule $L \subset M$. This is possible because M is finite by Lemma 3.5. Now, for any $\sigma \in G$, it is easy to see that σL is a simple $\sigma N \sigma^{-1}$-module, hence a simple N-module. We can write M as $\sum_{\sigma \in G} \sigma L$, the sum of simple N-modules, since $\sum_{\sigma \in G} \sigma L \subset M$ is a G-module and M is simple as a G-module. Now 2.3(3) shows that M is semisimple as an N-module. □

Now we have all the ingredients to prove Theorem 1.4.

4.7. Theorem. *(Second theorem of the introduction) Let G be a finite group together with a maximal abelian normal subgroup A that is cyclic. Let C be the centralizer of A in G. Let N be normal in G. Then, for any $B \lhd G$ with $A \subset B \subset C$ such that B/A is abelian, B/A is a semisimple N-module.*

Proof. From 4.1 it follows that B/A is a semisimple G-module, and by 4.6 we know that B/A must automatically be a semisimple N-module for any $N \lhd G$. □

4.2 Further remarks

The theorem just proved shows for example that B/A is a semisimple $\mathbb{Z}$-module, since the trivial group is normal in G. This means that every element of B/A has squarefree order, and B/A is the direct sum of vector spaces over finite fields. In fact, the map $B/A \times B/A \to A$ given by $(\beta A, \delta A) \mapsto [\beta, \delta]$ makes all of these vector spaces into so called symplectic vector spaces over finite fields. One of the consequences of this is that the order of B/A is a square (which was proved in a different way in [6]). The theory of symplectic vector spaces is worked out in [1], pp. 215–231.

In lemma 4.6, the condition that N must be normal in G is somewhat too strong. It is easy to see that it suffices for N to be subnormal in G, e.g. a subgroup such there is a finite chain of groups $N \lhd N_1 \lhd \ldots \lhd G$. So the theorem is also true if the condition 'normal' is slightly weakened.

However, Lemma 4.6 is no longer true if we allow N to be any subgroup of G. For example, if we take $G = S_4$, then the abelian normal subgroup $M = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ is a G-module in a natural way. Since M has no subgroups that are normal in G, we see that M is a simple G-module. However, M is not a semisimple (12)-module. This follows because both (13)(24) and (14)(23) generate M as a (12)-module. This implies that the group of order two generated by (12)(34) is the only simple sub-(12)-module of M, so M cannot be the sum of simple sub-(12)-modules.

Instead of the group B/A, the entire group B is also an object to study. Since B/A is abelian, we know that B is nilpotent (see [4], chapter 10). The nilpotency of B implies that B is the direct product of its Sylow-p-subgroups. These Sylow-p subgroups are interesting objects to study, see pp. 349–361 of [1] for example.

References

[1] B. Huppert: *Endliche Gruppen I*, Springer-Verlag, 1967

[2] S. Lang: *Algebra* (Revised third edition), Springer, 2002

[3] W.J. Palenstijn, J. Daems: *Representatietheorie*, http://websites.math.leidenuniv.nl/algebra/, 2003

[4] P. Stevenhagen: *Algebra 1*, http://websites.math.leidenuniv.nl/algebra/, 2008

[5] P. Stevenhagen: *Algebra 3*, http://websites.math.leidenuniv.nl/algebra/, 2008

[6] J. Weimar, J. Michielsen: *Permutation groups*, http://websites.math.leidenuniv.nl/algebra/, 2007

[7] E. Witt: *Über die Kommutativität endlicher Schiefkörper*, Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität 8 (1931), 413