R.H. Eggermont
reggermo@math.leidenuniv.nl

Generalizations of a theorem by Brauer and Nesbitt

Master thesis, defended on September 26, 2011

Thesis advisors:
prof. dr. H.W. Lenstra
and
dr. L.D.J. Taelman

Mathematisch Instituut, Universiteit Leiden

Contents

1 Introduction **2**

2 Algebra **4**

3 Witt rings **10**

4 Witt power sums **19**
4.1 Definition and properties of Witt power sums 19
4.2 The isomorphism $W(A) \to W_p(A)^{\mathbb{Z}_{>0} \setminus p\mathbb{Z}_{>0}}$ for commutative $\mathbb{Z}_{(p)}$-algebras 22

5 Brauer-Nesbitt **25**
5.1 Definitions and notations 25
5.2 The Brauer-Nesbitt Theorem 26
5.3 Generalizations 31
5.3.1 Replacing $\Lambda(k)^B$ by $W_p(k)^B$ 31
5.3.2 Replacing $G_k(A)$ by $G_k(A) \bigotimes_{\mathbb{Z}} W_p(k)$. 36
5.3.3 The injection $G_k(A) \bigotimes_{\mathbb{Z}} W(k) \hookrightarrow W(k)^B$ 40
5.3.4 A different way of generalization 43

1 Introduction

The following is a theorem by Richard Brauer and Cecil Nesbitt, as found in [6].

Quotation 1.1 (Brauer-Nesbitt, 1937) *Let G be a group and let k be an algebraically closed field. Let A and B be two representations of a group G which associate the matrices A_Q and B_Q with the element Q of G. If both A_Q and B_Q have the same characteristic roots for every Q in G, then A and B have the same irreducible constituents.*

Let k be a field and A a k-algebra. Let B be a subset of A that generates A as a k-vectorspace, for example a k-basis of A. For $a \in A$ and a (left) A-module M that is finite-dimensional over k, denote by $\chi_M(a)$ the characteristic polynomial of left multiplication by a, which can be viewed as an element of the multiplicative group $\Lambda(k) = 1 + Tk[[T]]$ for a suitable definition of the characteristic polynomial (see Definition 5.3). Denote by $G_k(A)$ the Grothendieck group of A-modules that are finite-dimensional over k (see Definition 2.14 for the precise definition). Defining $\phi(M) = (\chi_M(b))_{b \in B}$ induces a group homomorphism $G_k(A) \to \Lambda(k)^B$.

One can rephrase Quotation 1.1 as follows.

Theorem 1.2 *Let G be a group and let k be an algebraically closed field. Then the group homomorphism $\phi : G_k(k[G]) \to \Lambda(k)^G$ defined by $[M] \mapsto (\chi_M(g))_{g \in G}$ is injective.*

This is Theorem 5.21 in this thesis. This theorem is not the strongest form one can have. For example, we can replace the group algebra $k[G]$ with k-vector space basis G by any algebra A with a subset B of A that generates A as a k-vector space, and one can omit the requirement that k is algebraically closed. However, the map ϕ from the theorem will never be surjective, and it suffices to know certain coefficients of the characteristic polynomials to determine the isomorphism class of a module. To be somewhat more precise, if the field k has characteristic 0, it suffices to know the traces of the action of the elements of B. If k has positive characteristic p, let $\Lambda_p(k) \subset \Lambda(k)$ be $1+\sum_{i=1}^{\infty} T^{p^i}k$ and let π be the surjective map $\Lambda(k) \to \Lambda_p(k)$ obtained by sending $1+a_1T+a_2T^2+a_3T^3+\ldots$ to $1 + a_1T + a_pT^p + a_{p^2}T^{p^2} + \ldots$. Then the map $\pi \circ \phi$ is injective. The latter was shown in [1], and a comparable result can be found in [2]. These results originally inspired this thesis.

Observe that $\Lambda_p(k)$ is not even a group, so the map $\pi \circ \phi$ is not even a group homomorphism.

The idea of somehow replacing the mentioned map $\pi \circ \phi$ by a group homomorphism that gives the same information leads to the study of Witt rings; see section 3. If A is a commutative ring, then there is a commutative ring $W(A)$, isomorphic as a set to $A^{\mathbb{Z}_{>0}}$, such that there is a group isomorphism $W(A) \to \Lambda(A) = 1 + TA[[T]]$. In particular, addition in $W(A)$ corresponds with multiplication in $\Lambda(A)$, and in Theorem 1.2, one may replace $\Lambda(k)$ by $W(k)$. More importantly, if k is a field of characteristic p, there is a ring $W_p(k)$ that behaves like $\Lambda_p(k)$ (or like k if p equals 0) in the way that we want; as a set it is isomorphic to $k^{\{1,p,p^2,\ldots\}}$ if $p > 0$ and to $k^{\{1\}}$ if $p = 0$ and there is a natural surjective ring homomorphism $\pi : W(k) \to W_p(k)$ by componentwise projection. We have the following theorem.

Theorem 1.3 *Let k be a field of characteristic p, let A be a k-algebra and let B be a subset of A that generates A as a k-vector space. Let π be the projection $W(k) \to W_p(k)$. If $a \in A$ and if M is an A-module, denote by $\psi_M(a)$ the element of $W(k)$ that corresponds with the characteristic polynomial $\chi_M(a) \in \Lambda(k)$ via the correspondence of $\Lambda(k)$ and $W(k)$.*

Then the group homomorphism $G_k(A) \to W_p(k)^B$ that is defined by $[M] \mapsto (\pi(\psi_M(b)))_{b\in B}$ is injective.

The definitions of $W(k)$ and $W_p(k)$ can be found in Definition 3.5 and Notation 3.8. The above theorem is Theorem 5.22 in this thesis. There is a stronger version of this theorem; Theorem 5.43 in this thesis.

Theorem 1.4 *Let k be a field of characteristic p, let A be a k-algebra and let B be a subset of A that generates A as a k-vector space. Let π be the projection $W(k) \to W_p(k)$. If $a \in A$ and if M is an A-module, denote by $\psi_M(a)$ the element of $W(k)$ that corresponds with the characteristic polynomial $\chi_M(a) \in \Lambda(k)$ via the correspondence of $\Lambda(k)$ and $W(k)$.*

Then the group homomorphism $G_k(A) \bigotimes_{\mathbb{Z}} W_p(k) \to W_p(k)^B$ that is defined by $[M] \otimes w \mapsto (\pi(\psi_M(b)) \cdot w)_{b\in B}$ is injective.

There is a deeper relation between $W(k)$ and $W_p(k)$. We have the following theorem.

Theorem 1.5 *Let $p \in \mathbb{Z}_{>0}$ be a prime number and let A be a commutative ring such that for each $n \in \mathbb{Z}$ with $p \nmid n$, one has n is invertible (in other words, A is a commutative $\mathbb{Z}_{(p)}$-algebra). Then there is a ring isomorphism $P : W(A) \to W_p(A)^{\mathbb{Z}_{>0} \setminus p\mathbb{Z}_{>0}}$.*

The mentioned ring isomorphism is functorial in the category of commutative $\mathbb{Z}_{(p)}$-algebras. To effectively compute it, it would be useful if we can efficiently calculate in Witt rings. In many practical cases, this is not a problem, but if A is an abstract ring, the number of computations required seems to be polynomial in p even if we only look at the first two components of $W_p(A)$, which limits the size of the possible characteristic of A.

If we can calculate efficiently in Witt rings, if $a \in A$, suppose one is given $(\pi(\psi_M(a^n)))_{n \in \mathbb{Z}_{>0} \setminus p\mathbb{Z}_{>0}}$, where π and $\psi_M(a)$ are as in Theorem 1.3. Then one can compute $\psi_M(a)$ efficiently using the theorem above. If one is given $(\pi(\psi_M(b)))_{b \in B}$ for a subset B of A that generates A as a k-vector space, one may compute $\psi_M(a)$ as well, but possibly not as efficiently.

There are more generalizations of Theorem 1.2. In the end, we will prove the following theorem. It is Theorem 5.54 in this thesis.

Theorem 1.6 *Let k be a field, let A be a k-algebra and let B be a subset of A that generates A as a k-vector space. Then the group homomorphism $G_k(A) \bigotimes_{\mathbb{Z}} W(k) \to W(k)^B$ defined by $[M] \otimes w \mapsto (\chi_M(b)w)_{b \in B}$ is injective.*

Finally, there is a generalization of Theorem 1.2 not by replacing $G_k(A)$ by some larger ring or by replacing $\Lambda(k)$ by some smaller ring in the statement of the theorem, but by replacing the set B that generates A as a k-vector space by a set C such that $\{c^n : c \in c, n \in \mathbb{Z}_{>0}\}$ generates A as a k-vector space. This is Theorem 5.62 in this thesis.

Theorem 1.7 *Let k be a field, let A be a k-algebra and let C be a subset of A such that $\sum_{c \in C} k[c]c = A$. Then the group homomorphism $G_k(A) \to W(k)^C$ defined by $[M] \mapsto (\psi_M(c))_{c \in C}$ is injective.*

Here is a summary of the thesis. In section 2, some basic algebra is found that is useful in the later sections. Section 3 defines Witt rings and gives some basic properties. Section 4 essentially describes the isomorphism mentioned in the theory above. Section 5 describes the theorem of Brauer and Nesbitt, and shows some generalizations of it.

2 Algebra

In the context of this thesis, a ring is defined to be an abelian group equipped with an associative, bilinear multiplication and a unit element with respect to multiplication. If not explicitly mentioned, a module over a ring is assumed to

be a left module. An algebra A over a ring R is a ring A together with a ring homomorphism $f : R \to A$ such that $f(R) \subseteq \mathrm{Z}(A)$ (where $\mathrm{Z}(A)$ denotes the center of A); in particular, any algebra is assumed to be associative and unital. Let R be a ring.

Definition 2.1 Let M be an R-module. We call M *simple* (as an R-module) if it has precisely two submodules, being 0 and M. We call M *semisimple* (as an R-module) if every short exact sequence $0 \to M' \to M \to M'' \to 0$ of R-modules splits. We call R a *semisimple* ring if any R-module is semisimple.

Remark 2.2 Note that an R-module is semisimple if and only if it is isomorphic to some direct sum of simple modules. Furthermore, any submodule of a semisimple module is semisimple and a direct sum of semisimple modules is semisimple. Moreover, R is a semisimple ring if and only if it is semisimple as a left R-module, hence we may just call R semisimple. Proofs of these remarks can be found in chapter 9 of [3].

Definition 2.3 We call R a *simple* ring if R has precisely two two-sided ideals, being 0 and R.

Note that if R is a simple ring, it isn't necessarily simple as an R-module.

Definition 2.4 We call R *left* respectively *right Artinian* if it satisfies the descending chain condition on left respectively right ideals

Definition 2.5 The *Jacobson radical* of R is the intersection of all maximal left ideals of R. It is denoted by $\mathrm{J}(R)$.

Lemma 2.6 *The Jacobson radical annihilates any simple R-module. It is a two-sided ideal of R.*

Proof Let M be a simple R-module. For any $m \in M \setminus \{0\}$, one has $Rm = M$ since M is simple. The R-linear map $R \to M$ that maps $r \in R$ to rm is therefore surjective, and as M is simple, its kernel $\mathfrak{m}$ is a maximal left ideal. As $\mathrm{J}(R)$ is contained in $\mathfrak{m}$, one has $\mathrm{J}(R)m = 0$. This holds for any $m \in M \setminus \{0\}$, hence for all $m \in M$, hence $\mathrm{J}(R)M = 0$.

Consequently, for any maximal left ideal $\mathfrak{m}$ of R, one has $\mathrm{J}(R)(R/\mathfrak{m}) = 0$, hence $\mathrm{J}(R)R$ is contained in $\mathfrak{m}$ for any maximal left ideal $\mathfrak{m}$ of R and therefore in the intersection of the maximal left ideals of R, which is $\mathrm{J}(R)$. ∎

As the maximal left ideals in $R/\mathrm{J}(R)$ correspond naturally to the maximal left ideals in R containing $\mathrm{J}(R)$, which are all of them by definition, it follows that $R/\mathrm{J}(R)$ has Jacobson radical 0.

Lemma 2.7 *If R is semisimple, then $\mathrm{J}(R) = 0$. Suppose there are finitely many maximal left ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ such that $\mathrm{J}(R) = \bigcap_{i=1}^{n} \mathfrak{m}_i$. Then R is semisimple if and only if $\mathrm{J}(R)$ equals 0.*

PROOF Suppose R is semisimple. Using Remark 2.2, one has R is a finite direct sum of simple R-modules, say $R = \bigoplus_{i=1}^{n} S_i$. For each $i \in \{1, 2, \ldots, n\}$, the projection $\pi_i : R \to S_i$ has kernel $\bigoplus_{j=1, j\neq i}^{n} S_i$, which is a maximal left ideal in R since S_i is simple. Clearly, the intersection of the kernels of π_i for each $i \in \{1, 2, \ldots, n\}$ is 0, hence one has $\mathrm{J}(R) = 0$.

For the second part, suppose $\mathrm{J}(R) = 0$ and there are finitely many maximal left ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ such that $\mathrm{J}(R) = \bigcap_{i=1}^{n} \mathfrak{m}_i$. We have an injective R-linear map $R/\bigcap_{i=1}^{n} \mathfrak{m}_i \hookrightarrow \bigoplus_{i=1}^{n} R/\mathfrak{m}_i$, induced by the quotient maps $\phi_i : R \to R/\mathfrak{m}_i$. As $R/\bigcap_{i=1}^{n} \mathfrak{m}_i = R/\mathrm{J}(R) = R$, it follows that we can view R as a submodule of the semisimple module $\bigoplus_{i=1}^{n} R/\mathfrak{m}_i$, hence R is semisimple. ∎

Corollary 2.8 *If R is a finite ring, it is semisimple if and only if $\mathrm{J}(R) = 0$.*

Corollary 2.9 *If k is a field and A is a k-algebra that is finite-dimensional over k, it is semisimple if and only if $\mathrm{J}(A) = 0$.*

PROOF The first implication follows directly from Lemma 2.7. Suppose $\mathrm{J}(A) = 0$. Since the dimension of any finite intersection of maximal left ideals can only take values in $\{0, 1, \ldots, \dim_k(A)\}$, there is some finite intersection $M = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_l$ of maximal left ideals of minimal dimension d. Since $\mathrm{J}(A) = 0$, if d is positive, there is some non-zero $x \in M$ and hence some maximal ideal $\mathfrak{m}$ that does not contain x. It follows that $M \cap \mathfrak{m} \subsetneq M$ and hence $\dim_k(M \cap \mathfrak{m}) < d$, a contradiction. Hence d equals 0 and thus M equals $\mathrm{J}(A)$. Then by Lemma 2.7, it follows that A is semisimple. ∎

Notation 2.10 Let R be a ring and M an R-module. Then the annihilator of M over R is denoted $\mathrm{Ann}_R(M)$.

Lemma 2.11 *Let k be a field and A a k-algebra. Let M be a semisimple A-module that is finite-dimensional over k. Then $A/\mathrm{Ann}_A(M)$ is finite-dimensional over k and semisimple.*

PROOF Since M is finite-dimensional over k, so is $\mathrm{End}_k(M)$, and as one has $A/\mathrm{Ann}_A(M) \subseteq \mathrm{End}_k(M)$, it follows that $A/\mathrm{Ann}_A(M)$ is finite-dimensional over k.

As M is semisimple, there are $S_1, \ldots, S_t$ such that $M \cong \bigoplus_{i=1}^{t} S_i$ as an A-module, and hence it follows that $\mathrm{Ann}_A(M) = \bigcap_{i=1}^{t} \mathrm{Ann}_A(S_i) \supseteq \mathrm{J}(A)$. Thus $\mathrm{J}(A/\mathrm{Ann}_A(M)) = 0$ and hence $A/\mathrm{Ann}_A(M)$ is semisimple by Corollary 2.9. ∎

Definition 2.12 Let R be a ring and let M and N be R-modules.

1 A *chain* for M is a finite sequence $0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_t = M$ of R-submodules of M, with $t \in \mathbb{Z}_{\geq 0}$. A chain $0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_t = M$ for M is called a *composition series* for M if for each $i \in \{1, 2, \ldots, t\}$, the quotient M_i/M_{i-1} is simple (as an R-module). If a composition series for M exists, M is said to be of *finite length*.

2 If $0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_t = M$ is a chain for M and $0 = N_0 \subsetneq N_1 \subsetneq \ldots \subsetneq N_s = N$ is a chain for N, these chains are called *isomorphic* if is a bijection $\rho : \{1, 2, \ldots, t\} \to \{1, 2, \ldots, s\}$ such that for each $i \in \{1, 2, \ldots, t\}$, one has $M_i/M_{i-1} \cong N_{\rho(i)}/N_{\rho(i)-1}$.

3 If M and N have isomorphic chains, M and N are called *Jordan-Hölder isomorphic* as R-modules, denoted $M \cong_{\mathrm{JH}R} N$ or just $M \cong_{\mathrm{JH}} N$ if it is clear which ring R we are using.

4 Suppose $0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_t = M$ is a composition series for M. Then the *semisimplification* of M is the R-module $M_{\mathrm{ss}} = \bigoplus_{i=1}^{t} M_i/M_{i-1}$.

Remark 2.13 Jordan-Hölder isomorphism is in fact an equivalence relation. Moreover, a composition series for an R-module M is unique up to isomorphism of chains if it exists, hence the semisimplification of an R-module M of finite length is well-defined up to isomorphism. Moreover, if M has finite length, M_{ss} is semisimple, as it is a direct sum of simple modules. Proofs of these statements can be found in [3].

Note that if k is a field, A a k-algebra and M an A-module that is finite-dimensional over k, any proper submodule of M has dimension strictly smaller than $\dim_k(M)$. It immediately follows that M is of finite length.

Definition 2.14 Let k be a field and A a k-algebra. Let $\mathcal{M}_k(A)$ be the set of isomorphism classes of A-modules that are finite-dimensional over k. We denote the isomorphism class of a finite-dimensional A-module M by M. We define $F_k(A)$ to be the free group generated by $\mathcal{M}_k(A)$ and denote by $R_k(A)$ the subgroup of $F_k(A)$ generated by elements of the form $M' + M'' - M$, where M', M'' and M are elements of $\mathcal{M}_k(A)$ such that there exists an exact sequence $0 \to M' \to M \to M'' \to 0$ of A-modules. Then the *Grothendieck group* of A-modules that are finite-dimensional over k is $G_k(A) = F_k(A)/R_k(A)$. The class of an element M of $F_k(A)$ modulo $R_k(A)$ is denoted by $[M]$.

Note that $G_k(A)$ is abelian and has zero element $[0]$.

Definition 2.15 Let k be a field and A a k-algebra. Let X be an abelian group. A map $f : \mathcal{M}_k(A) \to X$ is called *additive* if for every exact sequence $0 \to M' \to M \to M'' \to 0$ of A-modules with $M', M, M'' \in \mathcal{M}_k(A)$, one has $f(M) = f(M') + f(M'')$. The set of additive functions from $\mathcal{M}_k(A)$ to X is denoted $\mathrm{Add}(\mathcal{M}_k(A), X)$.

Proposition 2.16 *Let k be a field and A a k-algebra. Let X be an abelian group. Denote by π the map $\mathcal{M}_k(A) \to G_k(A)$ defined by sending $M \in \mathcal{M}_k(A) \subseteq F_k(A)$ to $[M] = M + R_k(A)$.*

There is a canonical bijection $g : \mathrm{Hom}(G_k(A), X) \to \mathrm{Add}(\mathcal{M}_k(A), X)$ given by $g(f)(M) = f(\pi(M))$ for any $f \in \mathrm{Hom}(G_k(A), X)$ and $M \in \mathcal{M}_k(A)$.

This proposition is a special case of Theorem 8.5 in [3]. It is trivially true.

Proposition 2.17 *Let k be a field and A a k-algebra. Let $M, N \in \mathcal{M}_k(A)$. Then one has $[M] = [N]$ if and only if $M \cong_{\mathrm{JH}A} N$.*

This proposition is a special case of Corollary 8.9 in [3].

Theorem 2.18 *Let k be a field and A a k-algebra. Let X be an abelian group. Let g be the map from Proposition 2.16. Let $f \in \mathrm{Hom}(G_k(A), X)$. Then the following are equivalent.*

1 *The group homomorphism f is injective.*

2 *For any two elements M, $N \in \mathcal{M}_k(A)$, one has $g(f)(M) = g(f)(N)$ if and only if $M \cong_{\mathrm{JH}} N$.*

Proof Suppose f is injective. Let M, $N \in \mathcal{M}_k(A)$. Then one has $g(f)(M) = g(f)(N)$ if and only if $f([M]) = f([N])$, which holds if and only $[M] = [N]$ since f is injective. One has $[M] = [N]$ if and only if $M \cong_{\mathrm{JH}} N$ by Proposition 2.17, hence one has $g(f)(M) = g(f)(N)$ if and only if $M \cong_{\mathrm{JH}} N$.

Conversely, suppose f is not injective. Then there is a non-zero $x \in G_k(A)$ with $f(x) = 0$. Let $\sum_{i=1}^{n} d_i M_i \in F_k(A)$ be a representative of x with $d_i \in \mathbb{Z}$ and $M_i \in \mathcal{M}_k(A)$ for each $i \in \{1, 2, \ldots, n\}$. Assume without loss of generality that none of the d_i is equal to 0 and that there is $j \in \{0, 1, 2, \ldots, n\}$ such that d_i is positive if $1 \leq i < j+1$ and that d_i is negative if $j+1 \leq i \leq n$. Note that if $M', M'' \in \mathcal{M}_k(A)$, one has $M' + M'' - M' \bigoplus M'' \in R_k(A)$. Then defining $M_+ = \bigoplus_{i=1}^{j} M_i^{d_i}$ and $M_- = \bigoplus_{i=j+1}^{n} M_i^{-d_i}$, we find that $M_+ - M_-$ is also a representative of x.

Since $f(x) = 0$, one has $g(f)(M_+) = g(f)(M_-)$. Since $x \neq 0$ by assumption, one has $[M_+] \neq [M_-]$ and hence $M_+ \ncong_{\mathrm{JH}} M_-$. This shows the other implication. ∎

Notation 2.19 Let k be a field and A a k-algebra. Let X be an abelian group. Suppose $f : \mathcal{M}_k(A) \to X$ is an additive map. Let g be the map from Proposition 2.16 and let $h = g^{-1}(f)$. Then we say that h is the *group homomorphism* $h : G_k(A) \to X$ *defined by* $[M] \mapsto f(M)$.

Corollary 2.20 *Let k be a field and A a k-algebra. Then $G_k(A)$ is torsion-free as an abelian group.*

Proof For any $n \in \mathbb{Z}_{>0}$ the map $f_n : \mathcal{M}_k(A) \to G_k(A)$ defined by $M \mapsto n[M]$ is well-defined. It is additive by the commutativity of direct sums. Moreover, it is easily seen that $f_n(M) = f_n(N)$ if and only if $[M^n] = [N^n]$. One has $[M^n] = [N^n]$ if and only if $M^n \cong_{\mathrm{JH}} N^n$. By uniqueness of decomposition chains up to chain isomorphisms, the latter holds if and only if $M \cong_{\mathrm{JH}} N$. Thus it follows that the group homomorphism $h_n : G_k(A) \to G_k(A)$ defined by $[M] \mapsto n[M]$ is injective for each $n \in \mathbb{Z}_{>0}$, hence $G_k(A)$ is torsion-free. ∎

Notation 2.21 Let $n \in \mathbb{Z}_{>0}$ and let R be a ring. Then $M(n, R)$ denotes the n by n matrix ring with coefficients in R.

Lemma 2.22 *Let k be a field and A a k-algebra that is finite-dimensional over k and that is semisimple as a ring. Then there are $t \in \mathbb{Z}_{\geq 0}$, $n_1, n_2, \ldots, n_t \in$*

$\mathbb{Z}_{>0}$ *and division rings* $D_1, \ldots, D_t$ *that are* k*-algebras, finite-dimensional over* k*, such that* $A \cong \prod_{i=1}^{t} M(n_i, D_i)$*. The integer* $t \in \mathbb{Z}_{\geq 0}$ *is unique and the pairs* $(n_1, D_1), \ldots, (n_t, D_t)$ *are unique up to ordering and* k*-algebra isomorphism classes of the* D_i*.*

Moreover, if k *is algebraically closed, one has* $D_i \cong k$ *for all* $i \in \{1, 2, \ldots, t\}$*.*

Furthermore, one has the following. For each $i \in \{1, 2, \ldots, t\}$*, denote* $S_i = D_i^{n_i}$*. Each* S_i *is an* $M(n_i, D_i)$*-module, and defining* $M(n_j, D_j)S_i = 0$ *if* $i, j \in \{1, 2, \ldots, t\}$ *with* $i \neq j$*, one has each* S_i *is an* A*-module. Then* S_1,S_2,...,S_t *are pairwise non-isomorphic simple* A*-modules and every simple* A*-module is isomorphic to* S_i *for some unique* $i \in \{1, 2, \ldots, t\}$*.*

PROOF This follows from theorems 9.10 and 9, 11 from [3]. ∎

We assume the basic definition of the tensor product is known.

Definition 2.23 Let R, S be rings and let $f : R \to S$ a ring homomorphism. Let V be an R-module. We denote $V_{R,S} = S \bigotimes_R V$. Here, we consider S to be a right R-module by $s \cdot r = s \cdot f(r)$ for $s \in S$ and $r \in R$. If it is clear what ring we take the tensor product over, we may denote $V_S = V_{R,S}$.

We recall a few facts about the tensor product.

Lemma 2.24 *Let* R *and* S *be rings. Let* $f : R \to S$ *be a ring homomorphism. Then the following hold.*

1 *If* V *is an* R*-module,* V_S *can be given an* S*-module structure in a canonical way such that for all* $\alpha, \beta \in S$ *and* $v \in V$*, one has* $\alpha \cdot (\beta \otimes v) = (\alpha\beta) \otimes v$*. The* S*-module* V_S *can be given an* R*-module structure in a canonical way such that for all* $\alpha \in R$*,* $\beta \in S$ *and* $v \in V$*, one has* $\alpha \cdot (\beta \otimes v) = (f(\alpha)\beta) \otimes v$*. In this way,* V_S *is an* R*-module as well, and with this structure, the map* $V \to V_S$ *given by* $v \mapsto 1 \otimes v$ *is* R*-linear.*

Any set $\{v_i\}_{i \in I}$ *that generates* V *as an* R*-module gives rise to a set* $\{1 \otimes v_i\}_{i \in I}$ *that generates* V_S *as an* S*-module. Moreover, if* V *is a free* R*-module, any free subset of* V *that generates* V *as an* R*-module gives rise to a free subset of* V_S *that generates* V_S *as an* S*-module.*

2 *Suppose* $f(R) \subseteq \mathrm{Z}(S)$ *and* A *is an* R*-algebra with defining ring homomorphism* $g : R \to A$*. Then* A_S *has a unique ring structure such that for all* $\alpha, \beta \in S$ *and all* $a, b \in A$*, one has* $(\alpha \otimes a) \cdot (\beta \otimes b) = (\alpha\beta) \otimes (ab)$*. The canonical maps* $A \to A_S$ *and* $S \to A_S$*, given by* $a \mapsto 1 \otimes a$ *and* $s \mapsto s \otimes 1$ *respectively, are ring homomorphisms with respect to this multiplication.*

With this structure, A_S *is canonically an* R*-algebra, with defining ring homomorphism* $r \mapsto f(r) \otimes 1 = 1 \otimes g(r)$*.*

Suppose the canonical ring homomorphism $h : S \to A_S$*, given by* $s \mapsto s \otimes 1$*, satisfies* $h(S) \subseteq \mathrm{Z}(A_S)$*. Then* A_S *is also an* S*-algebra.*

3 *Suppose $f(R) \subseteq \mathrm{Z}(S)$, let A be an R-algebra and let M be an A-module. Then M is also an R-module via the homomorphism $R \to A$. Then $M_{R,S} = S \bigotimes_R M$ can be given the structure of an A_S-module via the canonical isomorphism $M_{R,S} = S \bigotimes_R M \cong S \bigotimes_R (A \bigotimes_A M) \cong (S \bigotimes_R A) \bigotimes_A M = A_S \bigotimes_A M = M_{A,A_S}$ given by the correspondence $s \otimes m \leftrightarrow (s \otimes 1) \otimes m$ for $s \in S$, $m \in M$.*

4 *The functor $S \bigotimes_R -$ from the category of R-modules to the category of S-modules is right exact.*

Checking these properties is straightforward. It is left as an exercise for the reader.

Definition 2.25 Let R be a commutative ring and T an R-module. Then T is called *flat* if for any injective R-module homomorphism $f : M \to N$, the induced map $f \otimes \mathrm{Id} : M \bigotimes_R T \to N \bigotimes_R T$ is injective as well.

Lemma 2.26 *Suppose R is a principal ideal domain and T an R-module. Then T is flat if and only if it is torsion-free as an R-module.*

A proof of this lemma can be found in [7]. The lemma is given as proposition 3.2 in chapter XVI of [5] without proof, and it easily follows from proposition 3.7 in the same chapter of [5].

Proposition 2.27 *Suppose R is a principal ideal domain and let T be a torsion-free R-module. Let B be some index set. Then the R-linear map $R^B \bigotimes_R T \to T^B$ given by $(r_b)_{b \in B} \otimes t \mapsto (r_b t)_{b \in B}$ is injective.*

Proof Let S be a finitely generated submodule of T. Since R is a principal ideal domain and since T is torsion-free as an R-module, there is $s \in \mathbb{Z}_{\geq 0}$ such that $S \cong R^s$.

Observe that $R^B \bigotimes_R S \cong S^B$ since S is a direct sum of copies of R, since direct sums commute with tensors and since $R^B \otimes_R R \cong R^B$ canonically.

One has $T = \varinjlim S$, where S ranges over the finitely generated R-submodules of T. Moreover, one has $R^B \bigotimes_R T = R^B \bigotimes_R \varinjlim S \cong \varinjlim (R^B \bigotimes_R S) \cong \varinjlim (S^B) \subseteq T^B$. Here, we use that direct limits commute with tensor products; see exercise 12 on page 639 in [5]. This map is given by $(r_b)_{b \in B} \otimes t \mapsto (r_b t)_{b \in B}$. ∎

3 Witt rings

Definition 3.1 Let A be a commutative ring. Let $w = (w_1, w_2, \ldots) \in A^{\mathbb{Z}_{>0}}$. Let $n \in \mathbb{Z}_{>0}$. Then the n-th *ghost component* of w is $w^{(n)} = \sum_{d|n} d w_d^{n/d}$.

Lemma 3.2 *For each $n \in \mathbb{Z}_{>0}$, denote by $\mathbb{Q}[z_d]_{d|n}$ the polynomial ring in the variables z_d with d dividing n. Then there are unique polynomials $g_n \in \mathbb{Q}[z_1, z_2, \ldots]$ such that the following holds.*

Let A be a commutative ring that is torsion-free as an abelian group and let $w_1, w_2, \ldots \in A$. We denote $w = (w_1, w_2, \ldots) \in A^{\mathbb{Z}_{>0}}$. Then for each $n \in \mathbb{Z}_{>0}$, one has $g_n((w^{(d)})_{d|n})$ exists in A and is equal to w_n.

Furthermore, for each $n \in \mathbb{Z}_{>0}$, one has $g_n \in \mathbb{Q}[z_d]_{d|n} \subset \mathbb{Q}[z_1, z_2, \ldots]$.

PROOF We apply induction to n. For $n = 1$, the result is trivial; one has $g_1 = z_1$. For $N \in \mathbb{Z}_{>1}$, assume g_n exists as in the statement of the lemma if $n < N$. Define $g_N = \frac{1}{N}(z_N - \sum_{d|N \wedge d \neq N} d g_d^{N/d}) \in \mathbb{Q}[z_1, z_2, \ldots]$.

Let A be a torsion-free commutative ring and let $w_1, w_2, \ldots \in A$. Denote $w = (w_1, w_2, \ldots) \in A^{\mathbb{Z}_{>0}}$. One has $w^{(N)} = \sum_{d|N} d w_d^{N/d}$, hence $N w_N = w^{(N)} - \sum_{d|N \wedge d \neq N} d w_d^{N/d}$. Since A is torsion-free, $\frac{1}{N}(w^{(N)} - \sum_{d|N \wedge d \neq N} d w_d^{N/d})$ is well-defined in A and is equal to w_N. Then $g_N((w^{(d)})_{d|N})$ exists in A and is equal to w_N. Uniqueness of g_N is easily seen by taking for A the polynomial ring over $\mathbb{Q}$ in the variables $x_1, x_2, \ldots$ and taking $w_1 = x_1, w_2 = x_2, \ldots$.

By induction, the result holds for all $n \in \mathbb{Z}_{>0}$. By induction, one easily sees that $g_n \in \mathbb{Q}[z_d]_{d|n}$ for each $n \in \mathbb{Z}_{>0}$. ∎

Let A be a torsion-free commutative ring and let $w = (w_1, w_2, \ldots) \in A^{\mathbb{Z}_{>0}}$. We define

$$f_w = \prod_{n \in \mathbb{Z}_{>0}} (1 - w_n T^n)^{-1} \in 1 + TA[[T]].$$

Note that it is well-defined as for any $M \in \mathbb{Z}_{>0}$ and any $m \in \mathbb{Z}_{\geq M}$, one has $\prod_{n=1}^{M}(1 - w_n T^n)^{-1} \equiv \prod_{n=1}^{m}(1 - w_n T^n)^{-1} \bmod T^M$ and hence $f_w = \lim_{m \to \infty} \prod_{n=1}^{m}(1 - w_n T^n)^{-1}$ exists in $1 + TA[[T]]$.

Lemma 3.3 *One has $T\frac{f'_w}{f_w} = \sum_{n \in \mathbb{Z}_{>0}} w^{(n)} T^n$, where f'_w is the formal derivative of f_w with respect to T.*

PROOF If $f, g \in 1 + TA[[T]]$, one has $\frac{(fg)'}{fg} = \frac{f'}{f} + \frac{g'}{g}$. Hence one has $T\frac{f'_w}{f_w} = T\sum_{n \in \mathbb{Z}_{>0}} n w_n T^{n-1}(1 - w_n T^n)^{-1} = \sum_{n \in \mathbb{Z}_{>0}} \sum_{r \in \mathbb{Z}_{>0}} n (w_n T^n)^r$. It is easily seen that the n-th coefficient of the latter is indeed $\sum_{d|n} d w_d^{n/d} = w^{(n)}$ as was to be shown. ∎

Let $w_1, w_2, \ldots$ and $v_1, v_2, \ldots$ be algebraically independent elements over $\mathbb{Z}$ and let $w = (w_1, w_2, \ldots)$, $v = (v_1, v_2, \ldots)$. By Lemma 3.2, for each $i \in \mathbb{Z}_{>0}$ there are unique elements $s_i(w, v)$ and $m_i(w, v) \in \mathbb{Q}[w_1, w_2, \ldots, v_1, v_2, \ldots]$ such that for $s(w, v) = (s_1(w, v), s_2(w, v), \ldots)$, $m(w, v) = (m_1(w, v), m_2(w, v), \ldots)$ and $n \in \mathbb{Z}_{>0}$, one has $s(w, v)^{(n)} = w^{(n)} + v^{(n)}$ and $m(w, v)^{(n)} = w^{(n)} \cdot v^{(n)}$. Moreover, for each $n \in \mathbb{Z}_{>0}$, one has $m_n(w, v)$ and $s_n(w, v)$ can be expressed as polynomials in terms of w_d and v_d for $d|n$ with coefficients in $\mathbb{Q}$ (namely, one has $s_n(w, v) = g_n((w^{(d)} + v^{(d)})_{d|n})$ and $m_n(x, y) = g_n((w^{(d)} v^{(d)})_{d|n})$, where the g_n are the polynomials of Lemma 3.2). The following proposition shows that these rational coefficients are in fact integers.

Proposition 3.4 *Let $w_1, w_2, \ldots$ and $v_1, v_2, \ldots$ be algebraically independent elements over $\mathbb{Z}$ and let $w = (w_1, w_2, \ldots)$, $v = (v_1, v_2, \ldots)$. Then the following hold.*

1 *The power series $f_w \cdot f_v$ satisfies $T\frac{(f_w f_v)'}{f_w(T) f_v(T)} = \sum_{n \in \mathbb{Z}_{>0}} (w^{(n)} + v^{(n)}) T^n$.*

2 *The power series $g = \prod_{d,e \in \mathbb{Z}_{>0}} (1 - w_d^{e/\gcd(d,e)} v_e^{d/\gcd(d,e)} T^{de/\gcd(d,e)})^{-\gcd(d,e)}$ satisfies $T\frac{g'}{g} = \sum_{n \in \mathbb{Z}_{>0}} w^{(n)} v^{(n)} T^n$.*

3 *For each $n \in \mathbb{Z}_{>0}$, the n-th coefficient of $f_w \cdot f_v$ is $s_n(w, v)$ and the n-th coefficient of h is $m_n(w, v)$.*

4 *For each $n \in \mathbb{Z}_{>0}$, both $s_n(w, v)$ and $m_n(w, v)$ are elements of $\mathbb{Z}[w_d, v_d]_{d|n} \subset \mathbb{Q}[w_1, w_2, \ldots, v_1, v_2, \ldots]$.*

PROOF One has $T\frac{(f_w f_v)'}{f_w f_v} = T\frac{f_w'}{f_w} + T\frac{f_v'}{f_v}$; the first result holds by Lemma 3.3.

Denote $m = \gcd(d, e)$ for convenience. One has

$$T\frac{g'}{g} = T \sum_{d,e \in \mathbb{Z}_{>0}} \frac{-m(1 - w_d^{e/m} v_e^{d/m} T^{de/m})^{-m-1} \cdot (-\frac{de}{m}) w_d^{e/m} v_e^{d/m} T^{de/m-1}}{(1 - w_d^{e/m} v_e^{d/m} T^{de/m})^{-m}}$$
$$= \sum_{d,e \in \mathbb{Z}_{>0}} \frac{dew_d^{e/m} v_e^{d/m} T^{de/m}}{1 - w_d^{e/m} v_e^{d/m} T^{de/m}}.$$

Expanding and writing out, we find that the n-th coefficient of the latter equals

$$\sum_{d,e,r \in \mathbb{Z}_{>0} : r\frac{de}{m} = n} dew_d^{re/m} v_e^{rd/m} = \sum_{d,e \in \mathbb{Z}_{>0} : \frac{de}{\gcd(d,e)} | n} dw_d^{n/d} ev_e^{n/e}$$
$$= \sum_{d|n, e|n} dw_d^{n/d} ev_e^{n/e} = w^{(n)} v^{(n)}.$$

This shows the second result.

For $n \in \mathbb{Z}_{>0}$, let σ_n be the n-th coefficient of $f_w f_v$ and let μ_n be the n-th coefficient of g. Clearly, one has $\sigma_n, \mu_n \in \mathbb{Z}[w_1, w_2, \ldots, v_1, v_2, \ldots]$. Let $\sigma = (\sigma_1, \sigma_2, \ldots)$ and let $\mu = (\mu_1, \mu_2, \ldots)$. By Lemma 3.3, one has $\sigma^{(n)} = w^{(n)} + v^{(n)} = s(w, v)^{(n)}$ for each $n \in \mathbb{Z}_{>0}$ and $\mu^{(n)} = w^{(n)} v^{(n)} = m(w, v)^{(n)}$ for each $n \in \mathbb{Z}_{>0}$.

Then by Lemma 3.2, one has $\sigma_n = g_n((w^{(d)} + v^{(d)})_{d|n}) = s_n(w, v)$ and likewise, one has $\mu_n = m_n(w, v)$, hence $s_n(w, v)$ and $m_n(w, v)$ are elements of $\mathbb{Z}[w_1, w_2, \ldots, v_1, v_2, \ldots] \bigcap \mathbb{Q}[w_d, v_d]_{d|n}$, hence both are elements of $\mathbb{Z}[w_d, v_d]_{d|n}$. ■

Definition 3.5 Let A be a commutative ring.

1 We define $W(A) = A^{\mathbb{Z}_{>0}}$ as a set. An element $w = (w_1, w_2, \ldots)$ of $W(A)$ is called a *Witt vector*. For $w, v \in W(A)$, we define $w + v = s(w, v) = (s_1(w, v), s_2(w, v), \ldots)$ and $w \cdot v = m(w, v) = (m_1(w, v), m_2(w, v), \ldots)$. With this addition and multiplication, we call $W(A)$ the *Witt ring* of A. For $w \in W(A)$ and $n \in \mathbb{Z}_{>0}$, the n-th component of w is denoted w_n.

2 We define $\Lambda(A) = 1 + TA[[T]]$. We have a bijection $W(A) \to \Lambda(A)$ given by $(w_1, w_2, \ldots) \mapsto \prod_{n \in \mathbb{Z}_{>0}} (1 - w_n T^n)^{-1}$. For $f = \prod_{n \in \mathbb{Z}_{>0}} (1 - w_n T^n)^{-1} \in \Lambda(A)$, we say that $(w_1, w_2, \ldots)$ is the *Witt vector associated to* f.

3 Suppose B is also a commutative ring. A map $f : W(A) \to W(B)$ is called *continuous* if for each $n \in \mathbb{Z}_{>0}$ there is some $m \in \mathbb{Z}_{>0}$ such that for all $w, v \in W(A)$ with $w_i = v_i$ for $i \in \{1, 2, \ldots, m\}$, one has $f(w)_j = f(v)_j$ for each $j \in \{1, 2, \ldots, n\}$.

Remark 3.6 Here are some remarks about Definition 3.5.

1 Note that for $w_1, w_2, \ldots, v_1, v_2, \ldots, u_1, u_2, \ldots$ algebraically independent over $\mathbb{Z}$, the fact that componentwise addition and multiplication on the ghost components are commutative, bilinear and associative, it follows easily that $s(s(w, v), u) = s(w, s(v, u))$, that $s(w, v) = s(v, w)$, that $m(w, s(v, u)) = s(m(w, v), m(w, u))$ and that $m(m(w, v), u) = m(w, m(v, u))$. Hence the addition and multiplication defined on $W(A)$ are commutative, bilinear and associative. The Witt vector $(0, 0, \ldots) \in W(A)$ is the zero element, and the Witt vector $(1, 0, 0, \ldots) \in W(A)$ is the unit element. So the Witt ring of a commutative ring A is indeed a ring.

2 The bijection between $W(A)$ and $\Lambda(A)$ also makes $\Lambda(A)$ into a commutative ring. By Proposition 3.4, $\Lambda(A)$ has its standard multiplication as addition. It has zero element 1 and unit element $(1 - T)^{-1}$.

3 Let $w \in W(A)$. Then the maps $s, m : W(A) \to W(A)$ defined by $s(v) = w + v$ and $m(v) = w \cdot v$ are continuous, since for each positive integer n, the n-th coefficient of $s(v)$ (respectively $m(v)$) depends only on those v_d for which d divides n.

4 We could have used different identifications of $W(A)$ and $\Lambda(A)$. For example, we could use the correspondence $(w_1, w_2, \ldots) \leftrightarrow \prod_{n \in \mathbb{Z}_{>0}} (1 - w_n T^n)$ or $(w_1, w_2, \ldots) \leftrightarrow \prod_{n \in \mathbb{Z}_{>0}} (1 + w_n T^n)^{-1}$. The identification we use is the one used in [4].

Proposition 3.7 *Let $S \subseteq \mathbb{Z}_{>0}$ be a set such that for all $n \in S$ and all $d \in \mathbb{Z}_{>0}$ with $d|n$, one has $d \in S$. Then the projection $\pi : W(A) \mapsto A^S$ given by projecting an element $(w_1, w_2, \ldots)$ to $(w_n)_{n \in S}$ induces a unique ring structure on A^S such that π is a ring homomorphism.*

Proof This follows directly from Proposition 3.4, using that $(w + v)_n$ and $(w \cdot v)_n$ only depend on the w_d and v_d with $d|n$. ∎

Notation 3.8 Let A be a commutative ring and let $S \subset \mathbb{Z}_{>0}$ be a set that is closed under division, meaning that for all $n \in S$ and all $d \in \mathbb{Z}_{>0}$ with $d|n$, one has $d \in S$. Then $W_S(A)$ is the set A^S with the ring structure induced by the ring structure of $W(A)$ as in Proposition 3.7. We denote by π_S the projection $W(A) \to W_S(A)$. For an element $w \in W(A)$, we denote $w_S = \pi_S(x) \in W_S(A)$.

If $p \in \mathbb{Z}_{>0}$ is a prime and $P = \{1, p, p^2, p^3, \ldots\}$, we denote $W_p(A) = W_P(a)$. We denote $\pi_p = \pi_P$. We define $W_0(A) = W_{\{1\}}(A) \cong A$ and denote $\pi_0 = \pi_{\{1\}}$.

Abusing notation, if $S \subseteq T$ are both closed under division, we denote by π_S the projection $W_T(A) \to W_S(A)$ induced by the projection $\pi_S : W(A) \to W_S(A)$. Similarly, if $S = \{1, p, p^2, p^3, \ldots\}$, we denote by π_p the projection $W_T(A) \to W_S(A)$ induced by the projection $\pi_p : W(A) \to W_S(A)$ and if $S = \{1\}$, we denote by π_0 the projection $W_T(A) \to W_S(A)$ induced by the projection $\pi_0 : W(A) \to W_S(A)$.

Example 3.9 For $S = \{1\}$, one has $W_S(A) \cong A$, since for all $w, v \in W(A)$, one has $(w + v)_1 = w_1 + v_1$, $(w \cdot v)_1 = w_1 \cdot v_1$ and $\pi_0(1) = 1$.

Notation 3.10 Let A be a commutative ring.

For $a \in A$ we denote by $\{a\} \in W(A)$ the Witt vector associated to $(1-aT)^{-1}$, i.e. the Witt vector $(a, 0, 0, \ldots) \in W(A)$.

For $n \in \mathbb{Z}_{\geq 0}$, we define $V_n : W(A) \to W(A)$ by letting $V_n((w_1, w_2, \ldots))$ be the Witt vector associated to $\prod_{m \in \mathbb{Z}_{>0}} (1 - w_m T^{nm})^{-1}$. As the first m components of w determine the first nm components of $V_n(w)$, it follows immediately that V_n is continuous (if $n = 0$, continuity of V_n is trivial). Clearly, if $n \in \mathbb{Z}_{>0}$, one has V_n is injective.

Note that for any commutative ring A, any $a \in A$ and any $n \in \mathbb{Z}_{>0}$, one has that $V_n(\{a\})$ is the Witt vector associated to $\frac{1}{1-aT^n}$. Note moreover that for any $n, m \in \mathbb{Z}_{\geq 0}$, one has $V_n \circ V_m = V_{nm}$.

Lemma 3.11 *Let A, B be commutative rings and $f : A \to B$ a ring homomorphism. Then f induces a natural ring homomorphism $W(f) : W(A) \to W(B)$ given by $(w_n)_{n \in \mathbb{Z}_{>0}} \mapsto (f(w_n))_{n \in \mathbb{Z}_{>0}}$.*

Moreover, if f is injective, surjective or bijective respectively, then $W(f)$ is injective, surjective or bijective respectively.

Furthermore, one has $W(f) \circ V_n = V_n \circ W(f)$ for each $n \in \mathbb{Z}_{>0}$.

Proof One has $W(f)(1) = (f(1), f(0), f(0), \ldots) = (1, 0, 0, \ldots) = 1$. For $w, v \in W(A)$, one has $W(f)(w + v) = (f(s_1(w, v)), f(s_2(w, v)), \ldots) = (s_1(W(f)(w), W(f)(v)), s_2(W(f)(w), W(f)(v)), \ldots) = W(f)(w) + W(f)(v)$ and similarly $W(f)(w \cdot v) = W(f)(w) \cdot W(f)(v)$.

The last parts of the lemma are trivial. ∎

Proposition 3.12 *Let A be a commutative ring and let a,$b \in A$. Let n,$m \in \mathbb{Z}_{>0}$ and denote $g = \gcd(n, m)$. Then one has*

$$V_n(\{a\}) \cdot V_m(\{b\}) = g \cdot V_{nm/g}(\{a^{m/g} b^{n/g}\}).$$

Proof By Proposition 3.4, one has that $V_n(\{a\}) \cdot V_m(\{b\})$ is the Witt vector associated to $(1 - a^{m/g} b^{n/g} T^{nm/g})^{-g}$. Then $V_n(\{a\}) \cdot V_m(\{b\})$ is indeed equal to $g \cdot V_{nm/g}(\{a^{m/g} b^{n/g}\})$. ∎

Proposition 3.13 *Let A be a commutative ring, let $w, v \in W(A)$. Then for all $n \in \mathbb{Z}_{>0}$, one has*

$$n(w+v)_n = n(w_n + v_n) + \sum_{d|n \wedge d \neq n} d(w_d^{n/d} + v_d^{n/d} - (w+v)_d^{n/d})$$

and

$$n(w \cdot v)_n = \sum_{d,e|n} dw_d^{n/d} \cdot ev_e^{n/e} - \sum_{d|n \wedge d \neq n} d(w \cdot v)_d^{n/d}.$$

PROOF Denote the operations by $\circ$. Note that $(w \circ v)^{(n)} = w^{(n)} \circ v^{(n)}$ for all $n \in \mathbb{Z}_{>0}$. Let $n \in \mathbb{Z}_{>0}$.

One has $(w \circ v)^{(n)} = \sum_{d|n} d(w \circ v)_d^{n/d}$, hence it immediately follows that $n(w \circ v)_n = (w \circ v)^{(n)} - \sum_{d|n \wedge d \neq n} d(w \circ v)_d^{n/d} = w^{(n)} \circ v^{(n)} - \sum_{d|n \wedge d \neq n} d(w \circ v)_d^{n/d}$. Writing out $w^{(n)} = \sum_{d|n} dw_d^{n/d}$, the equalities in the lemma follow. ∎

Corollary 3.14 *Let A be a commutative ring and let $w = (w_1, w_2, \ldots)$, $v = (v_1, v_2, \ldots) \in W(A)$. Let $n \in \mathbb{Z}_{>0}$. Suppose $w_d = 0 = v_d$ for all $d|n$, $d \neq n$. Then one has $(w+v)_n = w_n + v_n$ and $(w \cdot v)_n = nw_n v_n$.*

Moreover, suppose for all $d|n$, $d \neq n$, at least one of w_d, v_d equals 0. Then $(w+v)_n = w_n + v_n$ as well.

Corollary 3.15 *Let A be a commutative ring and let $m \in \mathbb{Z}_{\geq 0}$. Then $V_m : W(A) \to W(A)$ is a continuous group homomorphism.*

PROOF It suffices to show this in a torsion-free ring, so assume A is torsion-free. Let $w, v \in W(A)$. It follows by Corollary 3.14 and induction that for any $n \in \mathbb{Z}_{>0}$, one has $V_m(w+v)_n = 0 = (V_m(w) + V_m(v))_n$ if $n \nmid m$. So it suffices to show $V_m(w+v)_{nm} = (V_m(w) + V_m(v))_{nm}$ for each $n \in \mathbb{Z}_{>0}$. One has $V_m(w+v)_{nm} = (w+v)_n$. On the other hand, one has

$$nm(V_m(w) + V_m(v))_{nm}$$

$$= nm(V_m(w)_{nm} + V_m(v)_{nm}) + \sum_{d|nm, d \neq nm} d(V_m(w)_d^{\frac{nm}{d}} + V_m(v)_d^{\frac{nm}{d}} - V_m(w+v)_d^{\frac{nm}{d}})$$

$$= nm(w_n + v_n) + \sum_{d|n, d \neq n} md(w_d^{\frac{nm}{dm}} + v_d^{\frac{nm}{dm}} - (w+v)_d^{\frac{nm}{dm}}) = nm(w+v)_n$$

and hence $V_m(w)_{nm} + V_m(v)_{nm} = (w+v)_n = V_m(w+v)_{nm}$ for each $n \in \mathbb{Z}_{>0}$. ∎

Proposition 3.16 *Let A be a commutative ring and let m be a non-negative integer. Then $V_m(W(A))$ is an ideal in $W(A)$.*

PROOF Let $S = \mathbb{Z}_{>0} \setminus m\mathbb{Z}_{>0}$. It is easily seen that S is closed under division. Then π_S is a ring homomorphism, and it is easily seen that $\mathrm{Ker}(\pi_S) = V_m(W(A))$, hence $V_m(W(A))$ is an ideal. ∎

Proposition 3.17 *Suppose A and B are commutative rings and $f : W(A) \to W(B)$ is a continuous group homomorphism. Let $w \in W(A)$ and suppose there are $w_1, w_2, \ldots \in W(A)$ such that $\sum_{i=1}^{\infty} w_i$ exists and is equal to w. Then the sum $\sum_{i=1}^{\infty} f(w_i) \in W(B)$ is well-defined and equal to $f(w)$.*

PROOF Let $w \in W(A)$ and let $w_1, w_2, \ldots \in W(A)$ such that $\sum_{i=1}^{\infty} w_i$ exists and is equal to a.

Note that since f is continuous, for each $l \in \mathbb{Z}_{>0}$ there is some $n \in \mathbb{Z}_{>0}$ such that if $v \in W(A)$ has first n components equal to zero, the first l components of $f(v)$ are equal to the first l components of $f(0) = 0$. Moreover, for each $n \in \mathbb{Z}_{>0}$, there is $M \in \mathbb{Z}_{>0}$ such that for each $m \in \mathbb{Z}_{\geq M}$, the first n components of $w - \sum_{i=1}^{m} w_i$ are equal to 0 by the continuity of addition.

Then for each $l \in \mathbb{Z}_{>0}$ there is $M \in \mathbb{Z}_{>0}$ such that for all $m \in \mathbb{Z}_{\geq M}$, the first l components of $f(w - \sum_{i=1}^{m} w_i)$ are equal to 0. Hence the first l components of $f(w)$ and $f(\sum_{i=1}^{m} w_i)$ are equal if m is sufficiently large.

In particular, one has $f(\sum_{i=1}^{m} w_i) = \sum_{i=1}^{m} f(w_i)$ since f is a group homomorphism and hence $\sum_{i=1}^{\infty} f(w_i)$ exists and is equal to $f(w)$. ∎

Theorem 3.18 *Suppose one is given for each commutative ring A a map $f_A : W(A) \to W(A)$ such that the following hold.*

1 *The map f_A is a group homomorphism.*

2 *The map f_A is continuous.*

3 *For each $a, b \in A$, one has $f_A(\{a\} \cdot \{b\}) = f_A(\{a\}) \cdot f_A(\{b\})$ and $f_A(1) = 1$.*

4 *If A and B are commutative rings and $g : B \to A$ is a group homomorphism, then the following diagram is commutative.*

$$\begin{array}{ccc} W(B) & \xrightarrow{f_B} & W(B) \\ \downarrow{\scriptstyle W(g)} & & \downarrow{\scriptstyle W(g)} \\ W(A) & \xrightarrow{f_A} & W(A) \end{array}$$

Then for each commutative ring A, the map f_A is a ring homomorphism.

PROOF Let A be a commutative ring, let $w = (w_1, w_2, \ldots), v = (v_1, v_2, \ldots) \in W(A)$. Note that one has $w \cdot v = \sum_{n,m=1}^{\infty} V_n(\{w_n\}) \cdot V_m(\{v_m\})$ using continuity of addition and multiplication. Hence one has $f_A(w \cdot v) = \sum_{n,m=1}^{\infty} f_A(V_n(\{w_n\}) \cdot V_m(\{v_m\}))$ and $f_A(w) \cdot f_A(v) = \sum_{n,m=1}^{\infty} f_A(V_n(\{w_n\})) \cdot f_A(V_m(\{v_m\}))$ by Proposition 3.17, using that f_A is a continuous group homomorphism by assumption. Thus it suffices to show that for each $n, m \in \mathbb{Z}_{>0}$, one has $f_A(V_n(\{w_n\}) \cdot V_m(\{v_m\})) = f_A(V_n(\{w_n\})) \cdot f_A(V_m(\{v_m\}))$.

Let $n, m \in \mathbb{Z}_{>0}$. Let $B = \mathbb{Z}[X^n, Y^m]$ be the polynomial ring in the variables X^n and Y^m. Let ζ_n and ζ_m be primitive n-th and m-th roots of unity respectively, and let $C = \mathbb{Z}[\zeta_m, \zeta_n, X, Y]$. Let $\iota : B \to C$ be the natural inclusion. Since

one has $\frac{1}{1-X^nT^n} = \prod_{i=1}^n \frac{1}{1-\zeta_n^i XT}$ in $\Lambda(C)$, one has $V_n(\{X^n\}) = \sum_{i=1}^n \{\zeta_n^i X\}$ in $W(C)$ and likewise $V_m(\{Y^m\}) = \sum_{j=1}^m \{\zeta_m^j Y\}$ in $W(C)$.

Then one has $f_C(V_n(\{X^n\}) \cdot V_m(\{Y^m\})) = \sum_{i=1}^n \sum_{j=1}^m f_C(\{\zeta_n^i X\} \cdot \{\zeta_m^j Y\})$ since f_C is a group homomorphism. By property **3**, one has $f_C(\{\zeta_n^i X\} \cdot \{\zeta_m^j Y\}) = f_C(\{\zeta_n^i X\}) \cdot f_C(\{\zeta_m^j Y\})$ and hence one concludes $f_C(V_n(\{X^n\}) \cdot V_m(\{Y^m\})) = f_C(V_n(\{X^n\})) \cdot f_C(V_m(\{Y^m\}))$.

By property **4**, one also has $f_B(V_n(\{X^n\}) \cdot V_m(\{Y^m\})) = f_B(V_n(\{X^n\})) \cdot f_B(V_m(\{Y^m\}))$, using that $W(\iota)$ is injective.

Now, define a ring homomorphism $g : B \to A$ by $X^n \mapsto w_n$ and by $Y^m \mapsto v_m$. By property **4**, we conclude that $f_A(V_n(\{w_n\}) \cdot V_m(\{v_m\})) = f_A(V_n(\{w_n\})) \cdot f_A(V_m(\{v_m\}))$. This concludes our proof. ∎

Theorem 3.19 *Suppose one is given for each commutative ring A maps $f_A, g_A : W(A) \to W(A)$ such that the following hold.*

1 *Both f_A and g_A are group homomorphisms.*

2 *Both f_A and g_A are continuous.*

3 *For each $a \in A$, one has $f_A(\{a\}) = g_A(\{a\})$.*

4 *If A and B are commutative rings and $h : B \to A$ is a group homomorphism, then the following diagram is commutative if one has $e_A = f_A$ and $e_B = f_B$ or if one has $e_A = g_A$ and $e_B = g_B$.*

$$\begin{array}{ccc} W(B) & \xrightarrow{e_B} & W(B) \\ \downarrow{\scriptstyle W(h)} & & \downarrow{\scriptstyle W(h)} \\ W(A) & \xrightarrow{e_A} & W(A) \end{array}$$

Then one has $f_A = g_A$ for each commutative ring A.

Proof Analogously to the proof of Theorem 3.18, it suffices to show that for each commutative ring A, for each $a \in A$ and for each $n \in \mathbb{Z}_{>0}$, one has $f_A(V_n(\{a\})) = g_A(V_n(\{a\}))$ since both f_A and g_A are continuous group homomorphisms.

Let $n \in \mathbb{Z}_{>0}$. Let $B = \mathbb{Z}[X^n]$ be the polynomial ring in the variables X^n and Y^m. Let ζ_n and ζ_m be primitive n-th and m-th roots of unity respectively, and let $C = \mathbb{Z}[\zeta_m, \zeta_n, X, Y]$. Let $\iota : B \to C$ be the natural inclusion.

Then analogously to the proof of Theorem 3.18, one finds $f_C(V_n(\{X^n\})) = \sum_{i=1}^n f_C(\{\zeta_n^i X\}) = \sum_{i=1}^n g_C(\{\zeta_n^i X\}) = g_C(V_n(\{X^n\}))$ using properties **1** and **3**. By property **4**, one concludes $f_B(V_n(\{X^n\})) = g_B(V_n(\{X^n\}))$ as well.

Now, define a ring homomorphism $g : B \to A$ by $X^n \mapsto a$. By property **4**, we conclude that $f_A(V_n(\{a\})) = g_A(V_n(\{a\}))$. This concludes our proof. ∎

Lemma 3.20 *Let A be a commutative ring of characteristic p, where $p \in \mathbb{Z}_{>0}$ is prime. For $n \in \mathbb{Z}_{\geq 0}$, let $Q_n = \{1, p, \ldots, p^n\}$.*

Then for $w = (w_1, w_2, \ldots) \in W(A)$, one has $p \cdot w = V_p((w_1^p, w_2^p, \ldots))$. Also, p^{n+1} annihilates $W_{Q_n}(A)$ and $W_{Q_n}(A)$ is a ring of characteristic p^{n+1}.

PROOF Note that for any element $w \in W(A)$, we have $p \cdot w$ is the Witt vector associated to $(\prod_{n \in \mathbb{Z}_{>0}}(1 - w_n T^n)^{-1})^p = \prod_{n \in \mathbb{Z}_{>0}}(1 - w_n^p T^{pn})^{-1}$, which is $V_p((w_1^p, w_2^p, \ldots))$. In particular, one has $p^{n+1} \cdot a_{Q_n} = 0$ and for $1 \in W_{Q_n}(A)$, one has $p^n \cdot 1 = (0, 0, \ldots, 0, 1) \neq 0$, so indeed $W_{Q_n}(A)$ is a ring of characteristic p^{n+1}. ∎

We end this section with an example.

Example 3.21 Let $p \in \mathbb{Z}_{>0}$ be prime and let A be a commutative ring. Let $S = \{1, p\}$ and consider the ring $W_S(A)$. An element w of $W_S(A)$ is denoted by (w_1, w_p) with $w_1, w_p \in A$. Let $w, v \in W_S(A)$. Then the following hold:

1 $w+v = (w_1+v_1, w_p+v_p-\sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} w_1^i v_1^{p-i})$, where $\frac{\binom{p}{i}}{p}$ is computed in $\mathbb{Z}$ as it may not be well-defined in A. This just follows by writing out the formal equality $p(x+y)_p = px_p + py_p + x_1^p + y_1^p - (x_1 + y_1)^p$ in characteristic 0 and dividing by p.

2 $w \cdot v = (w_1 v_1, pw_p v_p + w_1^p v_p + w_p v_1^p)$. This one follows by writing out $p(x \cdot y)_p = p^2 x_p y_p + p x_1^p y_p + p x_p y_1^p + x_1^p y_1^p - (x_1 y_1)^p$ in characteristic 0 and dividing by p.

3 For any $n \in \mathbb{Z}$, one has $n \cdot w = (nw_1, nw_p - \frac{n^p - n}{p} w_1^p)$, where $\frac{n^p - n}{p}$ is computed in $\mathbb{Z}$. This follows from the fact that for any $n, m \in \mathbb{Z}$, one has
$(nw_1, nw_p - \frac{n^p-n}{p} w_1^p) + (mw_1, mw_p - \frac{m^p - m}{p} w_1^p) =$
$((n+m)w_1, (n+m)w_p - \frac{n^p + m^p - n - m}{p} w_1^p + \frac{(nw_1)^p + (mw_1)^p - (nw_1 + mw_1)^p}{p}) =$
$((n+m)w_1, (n+m)w_p - \frac{(n+m)^p - (n+m)}{p} w_1^p)$ and induction.

4 As a direct corollary of 3, one has $-w = (-w_1, -w_p - \frac{(-1)^p + 1}{p} w_1^p)$. In particular, if $p = 2$, one has $-w = (-w_1, -w_2 - w_1^2)$ and if p is odd, one has $-w = (-w_1, -w_p)$.

5 Suppose A has characteristic p. Then for any $n \in \mathbb{Z}_{\geq 0}$, one has $w^n = (w_1^n, nw_1^{(n-1)p} w_p)$. This can easily be shown by induction, since it is true for $n = 1$, and for any $m, n \in \mathbb{Z}$, provided that w_1 is invertible if either $m < 0$ or $n < 0$, one has $(w_1^n, nw_1^{(n-1)p} w_p) \cdot (w_1^m, mw_1^{(m-1)p} w_p) =$
$(w_1^{m+n}, (w_1^n)^p (mw_1^{(m-1)p} w_p) + (nw_1^{(n-1)p} w_p)(w_1^m)^p) =$
$(w_1^{m+n}, (m+n) w_1^{(m+n-1)p} w_p)$.

In particular, one has $(w_1, w_p)^p = (w_1^p, 0)$.

Moreover, if w is invertible, one has $w^n = (w_1^n, nw_1^{(n-1)p} w_p)$ for all $n \in \mathbb{Z}$.

6 Suppose A has characteristic p. Then $w = (w_1, w_p)$ is invertible if and only if w_1 is invertible; in this case, the inverse of w is $(w_1^{-1}, -w_1^{-2p} w_p)$. This is a direct consequence of 5.

4 Witt power sums

Notation 4.1 Let $p \in \mathbb{Z}_{\geq 0}$ be a prime (possibly 0). We denote $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} | a, b \in \mathbb{Z}, p \nmid b\}$. In particular, one has $\mathbb{Z}_{(0)} = \mathbb{Q}$.

Remark 4.2 It is easily verified that $\mathbb{Z}_{(p)}$ is a subring of $\mathbb{Q}$ for each prime p, and that any $n \in \mathbb{Z}_{>0}$ with $p \nmid n$ is invertible in $\mathbb{Z}_{(p)}$.

Moreover, a ring A is a $\mathbb{Z}_{(p)}$-algebra if and only if any $n \in \mathbb{Z}$ that is not divisible by p is invertible. In particular, any $\mathbb{Z}_{(p)}$-algebra has characteristic either 0 or some power of p.

Let A be a commutative ring and let $n \in \mathbb{Z}_{>0}$. Recall that $V_n : W(A) \to W(A)$ is the map defined by letting $V_n((w_1, w_2, \ldots))$ be the Witt vector associated to the element $\prod_{m=1}^{\infty}(1 - w_m T^{nm})^{-1}$ of $\Lambda(A)$. We showed in Corollary 3.15 and Proposition 3.16 that V_n is a continuous group homomorphism and that $V_n(W(A))$ is an ideal of $W(A)$. Moreover, V_n is injective. We are going to use these properties to define certain ring homomorphisms $P_n : W(A) \to W(A)$. If there is some prime $p \in \mathbb{Z}_{\geq 0}$ (possibly 0) such that $W(A)$ is a $\mathbb{Z}_{(p)}$-algebra, then the ring homomorphisms P_n will allow us to find a ring isomorphism of $W(A)$ with the product $\prod_{n \in \mathbb{Z}_{>0}, p \nmid n} W_p(A)$.

4.1 Definition and properties of Witt power sums

Definition 4.3 Let A be a commutative ring. Let $n \in \mathbb{Z}_{>0}$. We define $P_n : W(A) \to W(A)$, by $V_n(P_n(w)) = V_n(1) \cdot w$. We call P_n the n-th *Witt power sum.*

Remark 4.4 Since $V_n(W(A))$ is an ideal, one has $V_n(1) \cdot w \in V_n(W(A))$. As V_n is injective for any $n \in \mathbb{Z}_{>0}$, the element $P_n(w)$ is well defined for each $w \in W(A)$.

Recall that if A is a commutative ring and if $a \in A$, one denotes by $\{a\}$ the Witt vector associated to $\frac{1}{1-aT}$, i.e. the Witt vector $(a, 0, 0, \ldots)$.

Theorem 4.5 *Let A be a commutative ring and let $n \in \mathbb{Z}_{>0}$. Then one has the following.*

1 *The map P_n is a group homomorphism.*

2 *The map P_n is continuous.*

3 *For all $a \in A$ and $m \in \mathbb{Z}_{>0}$, letting $g = \gcd(n, m)$, one has*

$$P_n(V_m(\{a\})) = g V_{m/g}(\{a^{n/g}\}).$$

4 *For all $a \in A$, one has $P_n(\{a\}) = \{a^n\}$.*

5 *For all $a, b \in A$, one has $P_n(\{a\} \cdot \{b\}) = P_n(\{a\}) \cdot P_n(\{b\})$ and one has $P_n(1) = 1$.*

6 *Let B be a commutative ring and suppose $g : B \to A$ is a ring homomorphism. Then the following diagram commutes.*

$$\begin{array}{ccc} W(B) & \xrightarrow{P_n} & W(B) \\ \downarrow{\scriptstyle W(g)} & & \downarrow{\scriptstyle W(g)} \\ W(A) & \xrightarrow{P_n} & W(A) \end{array}$$

7 *The map P_n is a ring homomorphism.*

PROOF Properties **1** and **2** follow from the fact that V_n is an injective, continuous group homomorphism. Property **6** follows from Lemma 3.11. For all $a, b \in A$, one has $\{a\} \cdot \{b\} = \{ab\}$, this means that property **4** implies property **5**. Clearly property **3** implies property **4**.

Let $a \in A$ and $m \in \mathbb{Z}_{>0}$. Let $g = \gcd(n, m)$. One has $V_n(1) \cdot V_m\{a\} = gV_{nm/g}(\{a^{n/g}\}) = V_{nm/g}(g\{a^{n/g}\})$ by Proposition 3.12. Hence one has $P_n(a) = V_n^{-1}(V_{nm/g}(g\{a^{n/g}\})) = V_{m/g}(g\{a^{n/g}\}) = gV_{m/g}(\{a^{n/g}\})$. This shows property **3**.

Property **7** now holds by Theorem 3.18. ∎

Corollary 4.6 *Let $n, m \in \mathbb{Z}_{>0}$. Then $P_n \circ P_m = P_{nm}$ for each commutative ring A.*

PROOF Let A be a commutative ring and let $a \in A$. Then one has $P_n \circ P_m(\{a\}) = P_n(\{a^m\}) = \{a^{nm}\} = P_{nm}(\{a\})$. As both $P_n \circ P_m$ and P_{nm} are continuous ring homomorphisms that satisfy property **4** from Theorem 3.19, one has by Theorem 3.19 that they are equal. ∎

Proposition 4.7 *Let $m, n \in \mathbb{Z}_{>0}$. Let $g = \gcd(m, n)$. Let m', $n' \in \mathbb{Z}_{>0}$ such that $m = gm'$ and $n = gn'$. For a commutative ring A, denote by ϕ_g the group homomorphism $W(A) \to W(A)$ given by $\phi_g(w) = gw$ for each $w \in W(A)$.*

Then one has $P_n \circ V_m = V_{m'} \circ \phi_g \circ P_{n'}$.

PROOF Observe that both $P_n \circ V_m$ and $V_{m'} \circ \phi_g \circ P_{n'}$ are continuous group homomorphisms that satisfy property **4** from Theorem 3.19. Then by Theorem 3.19 it suffices to show that for each commutative ring A and for each $a \in A$, one has $P_n \circ V_m(\{a\}) = V_{m'} \circ \phi_g \circ P_{n'}(\{a\})$. Let A be a commutative ring and let $a \in A$. One has $P_n(V_m(\{a\})) = gV_{m/g}(\{a^{n/g}\}) = V_{m'}(g\{a^{n'}\}) = V_{m'}(\phi_g(P_{n'}(\{a\})))$ using properties **3** and **4** from Theorem 4.5. This completes the proof. ∎

Corollary 4.8 *Let $m, n \in \mathbb{Z}_{>0}$ be coprime. Then one has $P_n \circ V_m = V_m \circ P_n$ for each commutative ring A.*

Corollary 4.9 *Let A be a commutative ring and let $n \in \mathbb{Z}_{>0}$. Then for each $w \in W(A)$, one has $P_n(V_n(w)) = nw$.*

Proposition 4.10 *Let A be a commutative ring and let $w = (w_1, w_2, \ldots) \in W(A)$. Let $n \in \mathbb{Z}_{>0}$. Then the first component of $P_n(w)$ is equal to $w^{(n)}$.*

PROOF Let $m \in \mathbb{Z}_{>0}$. Let $g = \gcd(n, m)$. Then by Theorem 4.5, the first component of $P_n(V_m(\{w_m\}))$ is the first component of $gV_{m/g}(\{w_m^{n/g}\})$. If one has $g \neq m$, this component is zero. One has $\gcd(n, m) = m$ if and only if $m|n$. If this is the case, the first component of $P_n(V_m(\{w_m\}))$ is equal to the first component of $mV_1(\{w_m^{n/m}\})$, which is $mw_m^{n/m}$. Since P_n is a continuous group homomorphism, one has $P_n(w) = \sum_{i=1}^{\infty} P_n(V_i(\{w_i\}))$ and hence the first component of $P_n(w)$ is equal to the first component of $\sum_{d|n} P_n(V_d(\{w_d\}))$, which is $\sum_{d|n} dw_d^{n/d} = w^{(n)}$. ∎

Theorem 4.11 *Let A be a commutative ring, let $m \in \mathbb{Z}_{>0}$, let $n \in \mathbb{Z}_{>0}$ such that $\gcd(m, n) = 1$ and let $w = (w_1, w_2, \ldots) \in W(A)$. Then one has $P_n(V_m(w)) \in V_m(W(A))$ and the m-th component of $P_n(V_m(w))$ is equal to $w^{(n)}$.*

PROOF Since n and m are coprime, one has $P_n(V_m(w)) = V_m(P_n(w))$. The m-th component of $P_n(V_m(w))$ is therefore equal to the first component of $P_n(w)$, which is $w^{(n)}$ by Proposition 4.10. ∎

Theorem 4.12 *Let A be a commutative ring, let $m \in \mathbb{Z}_{>0}$, let $n \in \mathbb{Z}_{>0}$ such that $\gcd(m, n) = 1$ and let $w = (w_1, w_2, \ldots) \in W(A)$. If one has $w_k = 0$ for each divisor k of nm, then the e-th coefficient of $P_d(w)$ is equal to 0 for each $d|n$ and each $e|m$.*

Suppose that n is invertible in A. If the e-th coefficient of $P_d(w)$ is equal to 0 for each $d|n$ and each $e|m$, then one has $w_k = 0$ for each divisor k of nm.

PROOF Let $l \in \mathbb{Z}_{>0}$. Suppose $k \in \mathbb{Z}_{>0}$ is not a divisor of nm. Let d be a divisor of n and let $g = \gcd(k, d)$. One has $P_d(V_k(\{w_k\})) = gV_{k/g}(\{w_k^{d/g}\})$. Since k/g does not divide m (as this would imply that k divides mg and hence that k divides mn), the e-th coefficient of $P_d(V_k(\{w_k\}))$ is zero for each divisor e of m. Hence for each divisor d of n and for each divisor e of m, one has the e-th component of $P_d(w)$ is the e-th component of $\sum_{k|nm} P_d(V_k(\{w_k\}))$, which is 0 if $w_k = 0$ for all $k|nm$.

Suppose n is invertible. Suppose there is a divisor $k = de$ of nm with $w_k \neq 0$. There is a minimal divisor e of m such that there is $d|n$ with $w_{de} \neq 0$. Let e be such a minimal divisor of m, and let d be the minimal divisor of n with $w_{de} \neq 0$. Then d and e are coprime, and for each divisor k of de, one has $w_k = 0$. Hence one has $\sum_{k|de} P_d(V_k(\{w_k\})) = P_d(V_{de}(\{w_{de}\}))$ and by the previous argument, the e-th component of $P_d(w)$ is the e-th component of $P_d(V_{de}(\{w_{de}\}))$. One has $P_d(V_{de}(\{w_{de}\})) = dV_e(\{w_{de}\})$, which has e-th component $dw_{de} \neq 0$ since d is invertible. ∎

Definition 4.13 Let k be a field and A a k-algebra. Let M be an A-module that is finite-dimensional over k. Let $a \in A$ and denote by a_M the k-linear map $M \to M$ given by $m \mapsto am$. The *characteristic polynomial* of a with respect to M is $\chi_M(a) = \det(I - Ta_M)^{-1} \in \Lambda(k)$. We denote by $\psi_M(a) \in W(k)$ the Witt vector associated to $\chi_M(a)$ and we denote by $\mathrm{Tr}_M(a)$ the trace of a_M.

We will repeat these definitions in section 5.

Lemma 4.14 *Let k be an algebraically closed field and let A be a k-algebra. Let M be an A-module that is finite-dimensional over k. Let $a \in A$ and let $n \in \mathbb{Z}_{>0}$. Then one has $P_n(\psi_M(a)) = \psi_M(a^n) \in W(k)$.*

Proof Note that the action of a on M has eigenvalues $\lambda_1, \ldots, \lambda_d \in k$, counted with multiplicity. Then one has $\chi_M(a) = \prod_{i=1}^{d} \frac{1}{1-\lambda_i T}$, hence one has $\psi_M(a) = \sum_{i=1}^{n} \{\lambda_i\}$. By property **4** of Theorem 4.5, one has $P_n(\psi_M(a)) = \sum_{i=1}^{d} \{\lambda_i^n\}$. As the action of a^n on M has eigenvalues $\lambda_1^n, \ldots, \lambda_d^n$ counted with multiplicity, one finds $\psi_M(a^n) = P_n(\psi_M(a))$ as was to be shown. ∎

Proposition 4.15 *Let k be a field and let A be a k-algebra. Let M be an A-module that is finite-dimensional over k. Let $a \in A$ and let $n \in \mathbb{Z}_{>0}$. Then one has $P_n(\psi_M(a)) = \psi_M(a^n)$.*

Proof Replace k by some algebraic closure $\bar{k}$, replace A by $A_{\bar{k}}$, replace M by $M_{\bar{k}}$ and replace a by $1 \otimes a \in A_{\bar{k}}$.

Observe that under the natural inclusion $W(k) \to W(\bar{k})$ induced by the inclusion $k \subseteq \bar{k}$, one has $\psi_M(a) \mapsto \psi_{M_{\bar{k}}}(1 \otimes a)$ and $\psi_M(a^n) \mapsto \psi_{M_{\bar{k}}}(1 \otimes a^n)$. Applying Lemma 4.14, the statement of the lemma follows immediately. ∎

Corollary 4.16 *Let k be a field and let A be a k-algebra. Let M be an A-module that is finite-dimensional over k. Let $a \in A$ and let $n \in \mathbb{Z}_{>0}$. Then one has $\mathrm{Tr}_M(a^n) = \psi_M(a)^{(n)}$.*

Proof One has $\mathrm{Tr}_M(a^n)$ is the first component of $\psi_M(a^n)$. The latter is equal to $P_n(\psi_M(a))$ by Proposition 4.15 and hence $\mathrm{Tr}_M(a^n) = \psi_M(a)^{(n)}$ by Proposition 4.10. ∎

4.2 The isomorphism $W(A) \to W_p(A)^{\mathbb{Z}_{>0} \setminus p\mathbb{Z}_{>0}}$ for commutative $\mathbb{Z}_{(p)}$-algebras

Proposition 4.17 *Let $p \in \mathbb{Z}_{\geq 0}$ be a prime, possibly 0, and let A be a commutative $\mathbb{Z}_{(p)}$-algebra. Let S be a subset of $\mathbb{Z}_{\geq 0} \setminus p\mathbb{Z}_{\geq 0}$ that is closed under division, meaning that if $n \in S$ and $d \in \mathbb{Z}_{>0}$ with $d|n$, then $d \in S$. Recall that π_0 is the projection $W(A) \to W_0(A)$. The ring homomorphism $g : W(A) \to W_0(A)^S$ defined by $g(w)_n = \pi_0(P_n(w)) = w^{(n)}$ for $n \in S$ induces a ring isomorphism $W_S(A) \to W_0(A)^S$ given by $w + \mathrm{Ker}(\pi_S) \mapsto g(w)$ for each $w \in W(A)$.*

PROOF Let $w = (w_1, w_2, \ldots) \in \mathrm{Ker}(\pi_S)$ and let $n \in S$. Then for each $d|n$, one has $d \in S$ and hence $w^{(n)} = \sum_{d|n} dw_d^{n/d} = 0$. Hence $\mathrm{Ker}(\pi_S) \subseteq \mathrm{Ker}(g)$. Then there is a unique ring homomorphism $g_S : W_S(A) \to W_0(A)^S$ such that $g_S \circ \pi_S = g$.

Let $w \in W(A) \setminus \mathrm{Ker}(\pi_S)$. Then there is some minimal $n \in S$ such that $w_n \neq 0$. Then one has $w^{(n)} = nw_n \neq 0$ since n is invertible, hence $g(w) \neq 0$. So $\mathrm{Ker}(g) = \mathrm{Ker}(\pi_S)$. Hence one has $g(W(A)) \cong W_S(A)$ as rings.

Let $v = (v_n)_{n\in S}$. Define $w_1 = v_1$ and for $n \in S$, $n > 1$, define inductively $w_n = \frac{1}{n}(v_n - \sum_{d|n, d\neq n} dw_d^{n/d}) \in A$. As $p \nmid n$ for any $n \in S$, one has $\frac{1}{n} \in A$, hence w_n is well-defined for any $n \in S$.

Let $w \in \pi_S^{-1}((w_n)_{n\in S})$. Clearly, one has $w^{(n)} = \sum_{d|n} dw_d^{n/d} = v_n$ for each $n \in S$, showing g is surjective. Hence g induces a ring isomorphism $W_S(A) \to W_0(A)^S$ as was to be shown. ∎

Corollary 4.18 *Let A be a commutative $\mathbb{Q}$-algebra. Then the map $P : W(A) \to W_0(A)^{\mathbb{Z}_{>0}}$ defined by $P(w)_n = \pi_0(P_n(w))$ for any $n \in \mathbb{Z}_{>0}$ is a ring isomorphism.*

PROOF Take $S = \mathbb{Z}_{>0}$ in the previous proposition. ∎

Corollary 4.19 *Let $p \in \mathbb{Z}_{>0}$ be a prime number and let A be a commutative $\mathbb{Z}_{(p)}$-algebra. Let $S = \mathbb{Z}_{>0} \setminus p\mathbb{Z}_{>0}$. Then the ring homomorphism $g : W(A) \to W_0(A)^S$ defined by $g(w)_n = \pi_0(P_n(w))$ for any $n \in S$ has kernel $V_p(A) = \mathrm{Ker}(\pi_S)$ and induces a ring isomorphism $W_S(A) \to W_0(A)^S$.*

Proposition 4.20 *Let $p \in \mathbb{Z}_{>0}$ be a prime number and let A be a commutative $\mathbb{Z}_{(p)}$-algebra. Let $S = \mathbb{Z}_{\geq 0} \setminus p\mathbb{Z}_{\geq 0}$. For $l \in \mathbb{Z}_{\geq 0}$, denote by ${}_l\pi = \pi_{\{1,p,\ldots,p^l\}}$ the componentwise projection $W_p(A)^S \to W_{\{1,p,\ldots,p^l\}}(A)^S$. Denote by P the ring homomorphism $P : W(A) \to W_p(A)^S$ defined by $P(w)_n = \pi_p(P_n(w))$ for each $n \in S$. Then for each $l \in \mathbb{Z}_{\geq 0}$, the ring homomorphism ${}_l\pi \circ P$ has kernel $V_{p^{l+1}}(W(A))$ and is surjective.*

PROOF Let $l \in \mathbb{Z}_{>0}$. If $w \in V_{p^{l+1}}(W(A))$, Theorem 4.11 immediately gives ${}_l\pi(P(w)_n) = 0$ for each $n \in S$ and hence $w \in \mathrm{Ker}(f)$. Conversely, suppose $w \notin V_{p^{l+1}}(W(A))$. Then there is some minimal $i \in \mathbb{Z}_{>0}$ with $i < l+1$ such that there is some minimal $n \in S$ such that $w_{p^i n} \neq 0$. Writing $w = V_{p^i}(w')$, one has $P_n(w)_{p^i} = w'^{(n)} \neq 0$, hence $w \notin \mathrm{Ker}(P)$. This shows $\mathrm{Ker}({}_l\pi \circ P) = V_{p^{l+1}}(W(A))$ for each $l \in \mathbb{Z}_{>0}$.

Let $v = ({}_n v)_{n\in S} \in W_p(A)^S$. By Proposition 4.17, there is $w \in W(A)$ such that $({}_0\pi \circ P(w))_n = {}_n v_1$ for each $n \in S$. This shows ${}_0\pi \circ P$ is surjective.

Let $l \in \mathbb{Z}_{>0}$; assume ${}_{l-1}\pi \circ P$ is surjective. Then there is $\bar{w} \in W(A)$ such that $v - P(\bar{w}) \in \mathrm{Ker}({}_{l-1}\pi) = V_{p^l}(W_p(A)^S)$. Let $v' = ({}_n v)_{n\in S} \in W_p(A)^S$ such that $V_{p^l}(v') = v - P(\bar{w})$. By Proposition 4.17, there is $w' \in W(A)$ such that $({}_0\pi \circ P(w'))_n = {}_n v'_1$ for each $n \in S$.

Then one has $P(V_{p^l}(w')) = V_{p^l}(P(w')) = V_{p^l}(v') \in {}_l\pi(W_p(A)^S)$ since one has $V_{p^l} \circ P_n = P_n \circ V_{p^l}$ for all $n \in S$.

Let $w = \bar{w} + V_{p^l}(w')$. Then one has $v - P(w) = v - P(\bar{w}) - P(V_{p^l}(w')) = V_{p^l}(v') - P(V_{p^l}(w')) \in \mathrm{Ker}({}_l\pi)$ by construction, meaning ${}_l\pi(b) = {}_l\pi \circ P(a)$. Hence ${}_l\pi \circ P$ is surjective.

By induction, ${}_l\pi \circ P$ is surjective for each $l \in \mathbb{Z}_{\geq 0}$. ∎

Theorem 4.21 *Let $p \in \mathbb{Z}_{>0}$ be a prime number and let A be a commutative $\mathbb{Z}_{(p)}$-algebra. Let $S = \mathbb{Z}_{\geq 0} \setminus p\mathbb{Z}_{\geq 0}$. Then the ring homomorphism $P : W(A) \to W_p(A)^S$ defined by $P(w)_n = \pi_p(P_n(w))$ for any $n \in S$ is a ring isomorphism.*

Proof By Proposition 4.20, one has $\mathrm{Ker}(P) \subseteq \bigcap_{l \in \mathbb{Z}_{>0}} V_{p^l}(W(A)) = 0$, hence P is injective.

Let $v = ({}_nv)_{n \in S} \in W_p(A)^S$. For each $l \in \mathbb{Z}_{\geq 0}$, denote ${}_l\pi = \pi_{\{1,p,\ldots,p^l\}}$. For each $l \in \mathbb{Z}_{\geq 0}$, there is ${}_lw \in W(A)$ such that ${}_l\pi(v) = {}_l\pi \circ P({}_lw)$ by Proposition 4.20. For $l, m \in \mathbb{Z}_{>0}$ with $l \leq m$, one has ${}_l\pi(v) = {}_l\pi \circ P({}_mw)$ as well, hence ${}_lw - {}_mw \in V_{p^{l+1}}(W(A))$. It follows that there is $w \in W(A)$ such that for each $l \in \mathbb{Z}_{\geq 0}$, one has $w_s = ({}_lw)_s$ for each $s \in \mathbb{Z}_{>0}$ with $p^{l+1} \nmid s$. Namely, if $s = p^lu$ with $p \nmid u$, define $w_s = ({}_lw)_s$. Clearly, we have $w - {}_lw \in V_{p^{l+1}}(W(A))$ and hence ${}_l\pi \circ P(w) = {}_l\pi(v)$ for each $l \in \mathbb{Z}_{\geq 0}$. It immediately follows that $P(w) = v$, hence P is surjective. ∎

If $w = (w_1, w_2, \ldots) \in W(A)$, the proposition below essentially tells us that for given $n = p^lm \in \mathbb{Z}_{>0}$ with $p \nmid m$, we can reconstruct w_d for $d|n$ given the p^i-th coefficients of $P_e(w)$ for each divisor e of m and for each $i \in \{0, 1, \ldots, l\}$. It is more explicit than Proposition 4.20. In essence, it gives us a way to compute the inverse of the isomorphism P on a finite level. Provided one can calculate in $W(A)$ in an efficient manner, this computation can be performed in an efficient manner.

Proposition 4.22 *Let $p \in \mathbb{Z}_{>0}$ be a prime number and let A be a commutative $\mathbb{Z}_{(p)}$-algebra. Let $P : W(A) \to W_p(A)^{\mathbb{Z}_{>0} \setminus p\mathbb{Z}_{>0}}$ be the ring homomorphism defined by $P(w)_n = \pi_p(P_n(w))$ for all $a \in A$ and all $n \in \mathbb{Z}_{>0} \setminus p\mathbb{Z}_{>0}$. For $n \in \mathbb{Z}_{>0}$, denote $S_n = \{d \in \mathbb{Z}_{>0} : d|n\}$.*

Then for each $n \in \mathbb{Z}_{>0}$, one has the following. Write $n = qu$ with $q, u \in \mathbb{Z}_{\geq 0}$ such that $p \nmid u$ and q is a power of p. Then P induces an isomorphism $g_n : W_{S_n}(A) \to W_{S_q}(A)^{S_u}$.

Proof Let $n \in \mathbb{Z}_{>0}$. Write $n = qu$ with $q = p^l$ for some $l \in \mathbb{Z}_{>0}$ and $p \nmid u$. Let $w = (w_1, w_2, \ldots) \in W(A)$. One has $g_n(w) = 0$ if and only if the p^i-th coefficient of $P_d(w)$ is equal to 0 for each divisor d of u and each $i \in \{0, 1, \ldots, l\}$. Since u is invertible, by Theorem 4.12 this is the case if and only if the k-th coefficient of w is equal to 0 for each divisor k of qu. This shows $\mathrm{Ker}(g_n) = \mathrm{Ker}(\pi_{S_n})$.

Fix u. If $l = 0$, one has g_n is surjective by Proposition 4.17. We apply induction to l. Let $L \in \mathbb{Z}_{>0}$ and suppose g_{up^l} is surjective for every $l < L$. Write $N = up^L$. Note that g_N maps $V_{p^L}(W_{S_N}(A))$ surjectively to $V_{p^L}(W_{S_N}(A)^{S_u})$ by Proposition 4.17, using Corollary 4.8. Let $v \in W_{S_N}(A)^{S_u}$.

Let $w \in W_{S_N}(A)$ such that $\tilde{v} = v - g_N(w) \in V_{p^L}(W_{S_N}(A)^{S_u})$; such w exists by the induction hypothesis. Now let $\tilde{w} \in V_{p^L}(W(A))$ such that $g_N(\tilde{w}) = \tilde{v}$. Then one has $g_N(w + \tilde{w}) = v$, showing that g_N is surjective.

By induction, the proposition holds for any positive integer n. ∎

We can combine Corollary 4.18 and Theorem 4.21 in the following theorem.

Theorem 4.23 *Let $p \in \mathbb{Z}_{\geq 0}$ be a prime (possibly 0) and let A be a commutative $\mathbb{Z}_{(p)}$-algebra. Let $S = \mathbb{Z}_{\geq 0} \setminus p\mathbb{Z}_{\geq 0}$. Denote by π_p the componentwise projection $W(A)^S \to W_p(A)^S$. Then the ring homomorphism $P : W(A) \to W_p(A)^S$ defined by $P(w)_n = \pi_p(P_n(w))$ for any $n \in S$ is a ring isomorphism.*

Remark 4.24 Let $p \in \mathbb{Z}_{\geq 0}$ be a prime and let A be a commutative $\mathbb{Z}_{(p)}$-algebra. Using the ring isomorphism P from Theorem 4.23, one can give $W(A)$ the structure of a $W_p(A)$-module. Namely, if $S = \mathbb{Z}_{\geq 0} \setminus p\mathbb{Z}_{\geq 0}$, one has $W_p(A)^S$ is a $W_p(A)$-module by componentwise multiplication. Moreover, using the diagonal embedding $\iota : W_p(A) \to W_p(A)^S$, one finds that $P^{-1} \circ \iota$ is an injective ring homomorphism from $W_p(A)$ to $W(A)$, meaning that $W_p(A)$ can be viewed as a subring of $W(A)$. Observe that $\pi_p \circ (P^{-1} \circ \iota) = \mathrm{Id}_{W_p(A)}$, since $w = P^{-1}((\alpha_n)_{n \in S})$ satisfies $\pi_p(w) = \pi_p(P_1(w)) = \alpha_1$ for each $(\alpha_n)_{n \in S} \in W(A)^S$.

5 Brauer-Nesbitt

Notation 5.1 In this section, unless noted otherwise, k denotes a field, A denotes a k-algebra and M and N denote A-modules that are finite-dimensional over k.

5.1 Definitions and notations

Notation 5.2 Let a in A. We denote by a_M the k-linear map $M \to M$ given by $m \mapsto a \cdot m$. We denote by $\mathrm{Tr}_M(a)$ the trace of a_M.

We repeat Definition 4.13.

Definition 5.3 Let $a \in A$. The *characteristic polynomial* of a with respect to M is $\chi_M(a) = \det(I - Ta_M)^{-1} \in \Lambda(k)$. The n-th coefficient of $\chi_M(a)$ is denoted $\chi_{M,n}(a)$.

Note that this is not the standard definition of the characteristic polynomial. Observe however that in this way, $\chi_M(1)$ corresponds to $\dim_k(M) \cdot 1_{W(k)}$ via the identification of $\Lambda(k)$ with $W(k)$.

Notation 5.4 We denote by $\psi_M(a) \in W(k)$ the Witt vector associated to $\chi_M(a) \in \Lambda(k)$ and for each $n \in \mathbb{Z}_{>0}$, we denote by $\psi_{M,n}(a)$ the n-th component of $\psi_M(a)$.

Remark 5.5 Note that for any $a \in A$, one has $\mathrm{Tr}_M(a) = \chi_{M,1}(a) = \psi_{M,1}(a)$.

Note that if $M' \subseteq M$ is an A-submodule of M, then $M'' = M/M'$ is an A-module as well, and $\chi_M(a) = \chi_{M'}(a)\chi_{M''}(a)$ for any $a \in A$, as can be seen by choosing a k-basis of M' and extending it to a k-basis of M. Note that in particular, we have $\psi_M(a) = \psi_{M'}(a) + \psi_{M''}(a)$.

From this, we can conclude that for any $a \in A$, the maps $\chi_-(a) : \mathcal{M}_k(A) \to \Lambda(k)$ and $\psi_-(a) : \mathcal{M}_k(A) \to W(k)$ are additive in the sense of Definition 2.15.

5.2 The Brauer-Nesbitt Theorem

A known theorem is the following.

Quotation 5.6 (Brauer-Nesbitt, 1937) *Let G be a group and let k be an algebraically closed field. Let A and B be two representations of a group G which associate the matrices A_Q and B_Q with the element Q of G. If both A_Q and B_Q have the same characteristic roots for every Q in G, then A and B have the same irreducible constituents.*

Essentially, this quotation tells us that two modules A and B over a group algebra $k[G]$, with k algebraically closed and G a group, are Jordan-Hölder isomorphic if and only if for each element Q of G, the characteristic polynomials of the action of Q on A and B by left multiplication are equal.

In other words, we only need information about characteristic polynomials in order to determine the Jordan-Hölder isomorphism class of an $k[G]$-module. We aim to generalize this theorem.

We formulate a somewhat stronger version of the Brauer-Nesbitt theorem.

Theorem 5.7 *Let B be a subset of A that generates A as a k-vector space. Then one has $M \cong_{\mathrm{JHA}} N$ if and only if for each $b \in B$, one has $\chi_M(b) = \chi_N(b)$.*

This theorem immediately implies Quotation 5.6, as the elements of G form a basis of $k[G]$ as a k-vector space. A proof of Theorem 5.7 will be provided at the end of this subsection.

Lemma 5.8 *Let $a \in A$. Suppose a_M has eigenvalue $\lambda \in k$. Then $\chi_M(a)^{-1}$, viewed as an element of $k[T]$, is divisible by $(1 - \lambda T)$. If $\lambda \neq 0$, one has $\chi_M(a) \neq 1$.*

Proof If a_M has eigenvalue $\lambda \in k$, there is some k-basis $\{m_1, \ldots, m_n\}$ of M satisfying $a_M m_1 = \lambda m_1$. We easily see that for $M' = km_1$ and $M'' = M/M'$, we have $\chi_M(a)^{-1} = \chi_{M'}(a)^{-1} \cdot \chi_{M''}(a)^{-1}$. As $\chi_{M'}(a)^{-1} = (1 - \lambda T)$, one has $\chi_M(a)^{-1}$ is divisible by $(1 - \lambda T)$. If $\lambda \neq 0$, one has $(1 - \lambda T)$ is not invertible in $k[T]$, hence it follows that $\chi_M(a)^{-1} \neq 1$ and hence $\chi_M(a) \neq 1$. ∎

Lemma 5.9 *Let R be a semisimple ring and let S be a simple R-module. Then for each $s \in S \setminus \{0\}$ there is some $r \in R$ with $rs = s$ and such that for any simple R-module T that is not isomorphic to S, one has $rT = 0$.*

Proof Let $s \in S \setminus \{0\}$. Consider the R-linear map $f : R \to S$ defined by $f(r) = rs$ for each $r \in R$. As S is simple and $f(1) = s \neq 0$, one has $f(R) = S$. Consider the exact sequence $0 \to \mathrm{Ker}(f) \to R \xrightarrow{f} S \to 0$. Since R is semisimple, this sequence splits, hence there is an R-linear map $\phi : S \to R$ such that $f \circ \phi = \mathrm{Id}_S$. Define $r = \phi(s)$. Then one has $rs = f(r) = f(\phi(s)) = (f \circ \phi)(s) = s$.

Let T be a simple R-module and suppose it is not isomorphic to S. Let $t \in T$. Then there is an R-linear map $g : S \to T$ defined by $s' \mapsto \phi(s')t$ for $s' \in S$. If g is injective, it is an isomorphism since T is simple and S is not

0. This is false by assumption, hence $\mathrm{Ker}(g) \neq 0$. Since S is simple, it follows $\mathrm{Ker}(g) = S$. In particular, one has $rt = \phi(s)t = g(s) = 0$. Hence one has $rT = 0$. ∎

Theorem 5.10 *Let M, N be semisimple A-modules that are finite-dimensional over k. Then the following are equivalent.*

1 *One has M and N are isomorphic as A-modules.*

2 *For all $a \in A$, one has $\chi_M(a) = \chi_N(a)$.*

Proof The implication **1** $\Rightarrow$ **2** is trivial. Suppose **2** holds.

First, we show that we may assume that A is finite-dimensional over k and semisimple. Let $I \subset A$ be the annihilator of $M \bigoplus N$. Then both M and N are A/I-modules and A/I is semisimple and finite-dimensional over k by Lemma 2.11.

As $(a+I)_M = a_M$ and $(a+I)_N = a_N$ for any $a \in A$, we have $\chi_M(a+I) = \chi_N(a+I)$ for all $a \in A$. Note that we have a canonical bijection $\mathrm{Hom}_A(M,N) \cong \mathrm{Hom}_{A/I}(M,N)$, since any A-linear map from M to N is also A/I-linear and vice versa. Hence we have $M \cong_A N$ if and only if $M \cong_{A/I} N$. Moreover, M and N are still semisimple as A/I-modules. So if the theorem holds with A replaced by A/I, it holds for A as well.

Assume that A is semisimple and finite-dimensional over k.

Write $M = \bigoplus_{i=1}^{d} S_i$ and $N = \bigoplus_{i=1}^{e} T_i$ with $d, e \in \mathbb{Z}_{\geq 0}$, and $S_1, \ldots, S_d$, $T_1, \ldots, T_e$ simple A-modules. Assume $d \geq e$ without loss of generality. We apply induction to d.

If $d = 0$, both M and N are the 0-module, and hence one has $M = N$.

Suppose $d > 0$ and that the result is true for all $d' < d$. View a component S_1 of M as a subset of M. Let $s \in S_1 \setminus \{0\}$. Let $a \in A$ such that $as = 1$ and $aT = 0$ for each simple A-module T that is not isomorphic to S_1. Such a exists by Lemma 5.9.

Suppose S_1 is not isomorphic to T_i for any $i \in \{1, 2, \ldots, e\}$. Then one has $aT_i = 0$ for each $i \in \{1, 2, \ldots, e\}$. In particular, it follows that $aN = 0$, yielding that $\chi_N(a)$ equals 1.

On the other hand, viewing S_1 as an A-submodule of M, we see that a_M has eigenvalue 1 since we have $as = s$. Thus $\chi_M(a) \neq 1$ by Lemma 5.8, contradicting $\chi_M(a) = \chi_N(a)$. So at least one of the T_i is isomorphic to S_1.

Assume without loss of generality that T_1 and S_1 are isomorphic. Now consider the modules M/S_1 and N/T_1; these satisfy $\chi_{M/S_1}(a) = \chi_M(a)/\chi_{S_1}(a) = \chi_N(a)/\chi_{T_1}(a) = \chi_{N/T_1}(a)$ for all $a \in A$ by **2**, using $\chi_{S_1}(a) = \chi_{T_1}(a)$ since $S_1 \cong T_1$. As both M/S_1 and N/T_1 have precisely one fewer simple submodule in their decomposition, we can apply the induction hypothesis to M/S_1 and N/T_1 and conclude $M/S_1 \cong N/T_1$. As $M \cong M/S_1 \bigoplus S_1$ and $N \cong N/T_1 \bigoplus T_1$ since M and N are semisimple, it follows that M and N are isomorphic. ∎

Corollary 5.11 *Let M, N be A-modules that are finite-dimensional over k. Then the following are equivalent.*

1 *One has M and N are Jordan-Hölder isomorphic as A-modules.*

2 *For all $a \in A$, one has $\chi_M(a) = \chi_N(a)$.*

PROOF One has M and N are Jordan-Hölder isomorphic if and only if their semisimplifications M_{ss} and N_{ss} are isomorphic. Both M_{ss} and N_{ss} will also be semisimple and finite-dimensional over k. Moreover, for any $a \in A$, one has $\chi_M(a) = \chi_{M_{\text{ss}}}(a)$ and $\chi_N(a) = \chi_{N_{\text{ss}}}(a)$. Now apply the previous theorem to M_{ss} and N_{ss}. ∎

We can reformulate the above corollary as follows, using Theorem 2.18:

Corollary 5.12 *The group homomorphism $\phi : G_k(A) \to \Lambda(k)^A$ defined by $[M] \mapsto (\chi_M(a))_{a \in A}$ is injective.*

This immediately has the following consequence.

Corollary 5.13 *Let l be a field extension of k. Then the group homomorphism $\iota : G_k(A) \to G_l(A_l)$ defined by $[M] \mapsto [M_l]$ is injective.*

PROOF Define $\phi : G_k(A) \to \Lambda(k)^A$ as in Corollary 5.12. Define the group homomorphism $\phi_l : G_l(A_l) \to \Lambda(l)^A$ by $[M] \mapsto (\chi_M(a))_{a \in A}$, viewing A as a subring of A_l in the canonical way. The inclusion $k \subseteq l$ induces an inclusion $i : \Lambda(k)^A \to \Lambda(l)^A$ via the induced inclusion $\Lambda(k) \subseteq \Lambda(l)$.

Clearly, the following diagram commutes.

$$\begin{array}{ccc} G_l(A_l) & \xrightarrow{\phi_l} & \Lambda(l)^A \\ \uparrow{\scriptstyle \iota} & & \uparrow{\scriptstyle i} \\ G_k(A) & \xhookrightarrow{\phi} & \Lambda(k)^A \end{array}$$

As $i \circ \phi$ is injective, ι must be injective as well. ∎

The following is Lemma 9 in [8].

Lemma 5.14 *Let $\mathbb{Z}\langle X, Y\rangle$ denote the noncommutative polynomial ring generated by X and Y. Then there exists a unique sequence $f_0(X,Y), f_1(X,Y), \ldots$ of polynomials in $\mathbb{Z}\langle X, Y\rangle$ such that in $\mathbb{Z}\langle X, Y\rangle[[T]]$ we have*

$$(1 - (X+Y)T) = (1 - XT)(1 - YT) \prod_{k=0}^{\infty} (1 - f_k(X,Y)XYT^{k+2}).$$

The polynomial $f_m(X,Y)$ is homogeneous of degree m in X and Y.

A proof can be found in [8].

Lemma 5.15 *Let $R = \mathbb{Z}\langle X, Y\rangle$ denote the noncommutative polynomial ring generated by X and Y. Let V be the set of homogeneous polynomials in R of degree at least equal to 2. Let S be the polynomial ring over $\mathbb{Z}$ in the variables*

$H_{w,i}$ where w ranges over the elements of V and i ranges over the positive integers. We make S into a graded ring by defining the weight of $H_{w,i}$ to be equal to the degree of w times i.

For each $s \in \mathbb{Z}_{>0}$ there is a polynomial $\tilde{Q}_s \in S$ such that for every field k, every k-algebra A, every A-module M that is finite-dimensional over k and for all $a, b \in A$, one has the following.

Define a ring homomorphism $S \to k$ by mapping $H_{w,i}$ to the i-th coefficient $\chi_{M,i}(w(a,b))$ of the characteristic polynomial $\chi_M(w(a,b))$ of $w(a,b)$ for each pair $(w,i) \in V \times \mathbb{Z}_{>0}$.

Then one has

$$\chi_{M,s}(a+b) = \chi_{M,s}(a) + \chi_{M,s}(b) + \tilde{Q}_s((\chi_{M,i}(w(a,b)))_{(w,i)\in V\times\mathbb{Z}_{>0}}).$$

Moreover, $\tilde{Q}_s$ is homogeneous of degree s.

PROOF For $m \in \mathbb{Z}_{\geq 0}$, let $f_m(X,Y)$ be the polynomial from Lemma 5.14. Let k be a field, A a k-algebra, M an A-module that is finite-dimensional over k and let $a, b \in A$.

Then one has $(1-(a+b)T) = (1-aT)(1-bT)\prod_{i=0}^{\infty}(1-(f_i(a,b)ab)T^{i+2}) \in \Lambda(A)$. Taking determinants and inverting on both sides, one finds $\chi_M(a+b) = \chi_M(a)\chi_M(b)\prod_{i=0}^{\infty}(1+\sum_{j=1}^{\infty}\chi_{M,j}(f_i(a,b)ab)T^{(i+2)j})$.

Comparing the coefficients of T^s on both sides, one finds a formal relation $\tilde{Q}_s$ of the form we seek that does not depend on a, b, M, A and k for each $s \in \mathbb{Z}_{>0}$. ∎

Remark 5.16 Observe that in terms of Witt vectors, the equality

$$\chi_M(a+b) = \chi_M(a)\chi_M(b)\prod_{i=0}^{\infty}(1+\sum_{j=1}^{\infty}\chi_{M,j}(f_i(a,b)ab)T^{(i+2)j})$$

can be written as

$$\psi_M(a+b) = \psi_M(a) + \psi_M(b) + \sum_{i=0}^{\infty} V_{i+2}(\psi_M(f_i(a,b)ab)).$$

Theorem 5.17 *Let $R = \mathbb{Z}\langle X, Y\rangle$ denote the noncommutative polynomial ring generated by X and Y. Let W be the set of monomials in R of degree at least equal to 2 that are not equal to x^n or y^n for any $n \in \mathbb{Z}_{>1}$. Let S be the polynomial ring over $\mathbb{Z}$ in the variables $H_{w,i}$ where w ranges over the elements of W and i ranges over the positive integers. We make S into a graded ring by defining the weight of $H_{w,i}$ to be equal to the degree of w times i.*

For each $s \in \mathbb{Z}_{>0}$ there is a polynomial $Q_s \in S$ such that for every field k, every k-algebra A, every A-module M that is finite-dimensional over k and for all $a, b \in A$, one has the following.

Define a ring homomorphism $S \to k$ by mapping $H_{w,i}$ to the i-th coefficient $\chi_{M,i}(w(a,b))$ of the characteristic polynomial $\chi_M(w(a,b))$ of $w(a,b)$ for each pair $(w,i) \in W \times \mathbb{Z}_{>0}$.

Then one has

$$\chi_{M,s}(a+b) = \chi_{M,s}(a) + \chi_{M,s}(b) + Q_s((\chi_{M,i}(w(a,b)))_{(w,i)\in W\times\mathbb{Z}_{>0}}).$$

Moreover, Q_s is homogeneous of degree s.

Remark 5.18 One can prove this theorem by induction to s. We will not do this here. The main conclusion of Theorem 5.17 is that if k is a field, A a k-algebra, M an A-module, $a, b \in A$ and $s \in \mathbb{Z}_{>0}$, one has $\chi_{M,s}(a+b) = \chi_{M,s}(a) + \chi_{M,s}(b) + Q_s((\chi_{M,i}(w(a,b)))_{(w,i)\in W\times\mathbb{Z}_{>0}})$, where Q_s does not depend on the $\chi_{M,i}(w(a,b))$ for which the product of i and the degree of $w(X,Y)$ exceeds s. Moreover, Q_s does not depend on the $\chi_{M,i}(w(a,b))$ for which $w(x,y)$ has the form x^n or y^n for some $n \in \mathbb{Z}_{\geq 0}$.

Observe that similar polynomials W_s exist such that one has $\psi_{M,s}(a+b) = \psi_{M,s}(a) + \psi_{M,s}(b) + W_s(\psi_{M,i}(w(a,b))_{(w,i)\in W\times\mathbb{Z}_{>0}})$, where W_s does not depend on the $\psi_{M,i}(w(a,b))$ for which the product of i and the degree of $w(X,Y)$ exceeds s.

Corollary 5.19 *Let B be a subset of A that generates A as a k-vector space. Then the following are equivalent.*

1 *For all $a \in A$, one has $\chi_M(a) = \chi_N(a)$.*

2 *For all $b \in B$, one has $\chi_M(b) = \chi_N(b)$.*

PROOF The implication **1** $\Rightarrow$ **2** is trivial. Suppose **2** holds. For any $a \in A$, one has $\chi_{M,1}(a) = \chi_{N,1}(a)$ by the linearity of the trace.

Let $S \in \mathbb{Z}_{>1}$ and assume inductively that one has $\chi_{M,s}(a) = \chi_{N,s}(a)$ for any $s \in \{1, 2, \ldots, S-1\}$ and any $a \in A$. Let $a \in A$. Then one has $a = \sum_{i=1}^{m} \lambda_i b_i$ for certain $m \in \mathbb{Z}_{\geq 0}$, $\lambda_i \in k$ and $b_i \in B$. One has $\chi_{M,S}(\lambda_i b_i) = \lambda_i^S \chi_{M,S}(b_i) = \chi_{N,S}(\lambda_i b_i)$ for each i by assumption. Thus if $m = 0$ or $m = 1$, one has $\chi_{M,S}(a) = \chi_{N,S}(a)$.

Suppose $m > 1$. Inductively, assume one has the equality $\chi_{M,S}(\sum_{i=1}^{m-1} \lambda_i b_i) = \chi_{N,S}(\sum_{i=1}^{m-1} \lambda_i b_i)$. Write $a' = \sum_{i=1}^{m-1} \lambda_i b_i$. Then one has $\chi_{M,S}(a) = \chi_{M,S}(a') + \chi_{M,S}(\lambda_m b_m) + Q_S((\chi_{M,s}(w(a', \lambda_m b_m)))_{(w,s)\in W\times\mathbb{Z}_{>0}})$ by Theorem 5.17. One has $\chi_{M,S}(a') = \chi_{N,S}(a')$ by assumption and we already showed that $\chi_{M,S}(\lambda_m b_m)$ equals $\chi_{N,S}(\lambda_m b_m)$. Note that $Q_S((\chi_{M,s}(w(a', \lambda_m b_m)))_{(w,s)\in W\times\mathbb{Z}_{>0}})$ is polynomial in the $\chi_{M,s}(w(a', \lambda_m b_m))$ with $s < S$. By the induction hypothesis for S, we have $\chi_{M,s}(w(a', \lambda_m b_m)) = \chi_{N,s}(w(a', \lambda_m b_m))$ if $s < S$ and hence it follows that $Q_S((\chi_{M,s}(w(a', \lambda_m b_m)))_{(w,s)\in W\times\mathbb{Z}_{>0}}) = Q_S((\chi_{N,s}(w(a', \lambda_m b_m)))_{(w,s)\in W\times\mathbb{Z}_{>0}})$. Hence one finds $\chi_{M,S}(a) = \chi_{N,S}(a)$.

By induction one has $\chi_M(a) = \chi_N(a)$ for all $a \in A$. ∎

The combination of Corollary 5.11 and Corollary 5.19 proves Theorem 5.7.

Example 5.20 Let k be a field and G a group. Let $A = k[G]$ and let M, N be A-modules. We have that G is a k-vector space basis of A, hence one has $M \cong_{\mathrm{JH}} N$ if and only if for each $g \in G$, one has $\chi_M(g) = \chi_N(g)$.

Equivalently to Theorem 5.7, we have the following.

Theorem 5.21 *Let B be a subset of A that generates A as a k-vector space. Then the group homomorphism $\phi : G_k(A) \to \Lambda(k)^B$ defined by $[M] \mapsto (\chi_M(a))_{b\in B}$ is injective.*

5.3 Generalizations

In this subsection, we give a few generalizations of Theorem 5.21. We still use Notation 5.1.

5.3.1 Replacing $\Lambda(k)^B$ by $W_p(k)^B$

In this subsubsection, we prove the following generalization of Theorem 5.21. Recall that π_p denotes the projection $W(k) \to W_p(k)$.

Theorem 5.22 *Let $p = \mathrm{char}(k)$. Let B be a subset of A that generates A as a k-vector space. Then the group homomorphism $G_k(A) \to W_p(k)^B$ defined by $[M] \mapsto (\pi_p(\psi_M(b)))_{b\in B}$ is injective.*

A proof will be provided at the end of this subsubsection.

Proposition 5.23 *Let k be a field of positive characteristic p. Let A be a k-algebra and let $a \in A$. Let $j \in \mathbb{Z}_{\geq 0}$; suppose that $\pi_{\{1,p,\dots,p^{j-1}\}}(\psi_M(a^n)) = 0$ for each $n \in \mathbb{Z}_{>0}$. Then one has $\psi_M(a) \in V_{p^j}(W(A))$.*

Proof Let P denote the isomorphism $W(A) \to W_p(A)^{\mathbb{Z}_{>0}\setminus p\mathbb{Z}_{>0}}$ from Theorem 4.23, noting that k is a $\mathbb{Z}_{(p)}$-algebra. For any $n \in \mathbb{Z}_{>0} \setminus p\mathbb{Z}_{>0}$, one has $\pi_p(P_n(\psi_M(a))) = \pi_p(\psi_M(a^n)) \in V_{p^j}(W_p(A))$ by assumption, using Proposition 4.15. By Proposition 4.20, one has $\psi_M(a) \in V_{p^j}(W(A))$. ∎

Proposition 5.24 *Let k be a field of positive characteristic p. Let A be a k-algebra and let $a, b \in A$. Let $\mathbb{Z}\langle X, Y\rangle$ be the noncommutative polynomial ring generated by X and Y. Let $j \in \mathbb{Z}_{\geq 0}$; suppose that $\pi_{\{1,p,\dots,p^{j-1}\}}(\psi_M(w(a,b))) = 0$ for each monomial $w \in \mathbb{Z}\langle X, Y\rangle$ that is not of the form Y^n for some $n \in \mathbb{Z}_{\geq 0}$. Then one has $\pi_{\{1,2,\dots,p^j\}}(\psi_M(a+b)) = \pi_{\{1,2,\dots,p^j\}}(\psi_M(a)) + \pi_{\{1,2,\dots,p^j\}}(\psi_M(b))$.*

Proof By assumption, for any $w \in \mathbb{Z}\langle X, Y\rangle$ not of the form Y^n for any $n \in \mathbb{Z}_{\geq 0}$, one has $\psi_{M,i}(w(a,b)) = 0$ if $i < p^j$ using Proposition 5.23. Using Remark 5.18, we find that this means that one has $\psi_{M,n}(a+b) = \psi_{M,n}(a) + \psi_{M,n}(b)$ for each $n \in \{1, 2, \dots, p^j\}$. Hence one has $\pi_{\{1,2,\dots,p^j\}}(\psi_M(a+b)) = \pi_{\{1,2,\dots,p^j\}}(\psi_M(a)) + \pi_{\{1,2,\dots,p^j\}}(\psi_M(b))$, using Corollary 3.14. ∎

Remark 5.25 The proposition above can be made more general. One can replace the set $\{1, 2, \dots, p^j\}$ by the set $S = (\mathbb{Z}_{>0} \setminus p^j\mathbb{Z}_{>0}) \bigcup \{p^j\}$. This is simply because for any $s \in S$ with $s \neq p^j$, the s-th coefficient of $\psi_M(w(a,b))$ equals 0 for any monomial $w \in \mathbb{Z}\langle X, Y\rangle$ not of the form Y^n for some $n \in \mathbb{Z}_{\geq 0}$. It seems this S is the largest possible, since if $n \in \mathbb{Z}_{>1}$, the $p^j n$-th coefficient of $\psi_M(a+b)$ may have extra terms arising from the $V_{i+2}(\psi_M(f_i(a,b)ab))$ for which $i+2$ divides n from Remark 5.16.

Theorem 5.26 *Suppose k is a field of characteristic $p > 0$. Let I be a subset of A that is closed under left and right multiplication by elements of A, meaning that if $a \in A$ and $i \in I$, one has $ai \in I$ and $ia \in I$. Let $j \in \mathbb{Z}_{\geq 0}$ and suppose that $\pi_{\{1,p,\ldots,p^{j-1}\}}(\psi_M(b)) = 0$ for each $b \in I$. Then one has the following.*

1 *For all $b \in I$, one has $\psi_M(b) \in V_{p^j}(W(A))$.*

2 *For all $a \in A$, $b \in I$, one has $\pi_{\{1,2,\ldots,p^j\}}(\psi_M(a+b)) = \pi_{\{1,2,\ldots,p^j\}}(\psi_M(a)) + \pi_{\{1,2,\ldots,p^j\}}(\psi_M(b))$.*

This theorem follows directly from Proposition 5.23 and Proposition 5.24.

Remark 5.27 If I, j and k are as in the theorem, then for all $a, b \in I$ and $i \in \{0, 1, \ldots, j-1\}$, one has $\psi_{M,p^i}(a+b) = 0$. The subgroup I' spanned by I is a two-sided ideal satisfying $\pi_{\{1,p,\ldots,p^{j-1}\}}(\psi_M(b)) = 0$ for all $b \in I'$.

Corollary 5.28 *Suppose k has positive characteristic p. Let B be a subset of A that generates A as a k-vector space.*

1 *Let $j \in \mathbb{Z}_{\geq 0}$ and suppose $\psi_{M,p^i}(b) = 0$ for all $b \in B$ and $i \in \{0, 1, \ldots, j-1\}$. Then for all $a \in A$, one has $\psi_M(a) \in V_{p^j}(W(A))$.*

2 *Suppose $\dim_k(M)$ is bounded above by $n \in \mathbb{Z}_{>0}$ and assume that $\psi_{M,p^i}(b) = 0$ for any $b \in B$ and $i \in \{0, 1, \ldots, \lfloor \log_p(n) \rfloor\}$. Then M is the 0-module.*

Proof The first part follows from Remark 5.27 and Theorem 5.26.

For the second part, let $j = \lfloor \log_p(n) \rfloor$. Note that from Theorem 5.26, it follows $\psi_M(1) \in V_{p^{j+1}}(W(A))$. On the other hand, if M is not the 0-module, there are $u \in \{1, 2, \ldots, p-1\}$ and $i \in \{0, 1, \ldots, j\}$ such that $n = p^i u$. Then one has $\psi_M(1) = p^i u$, which has p^i-th component equal to $u \neq 0$, a contradiction. ∎

In essence, there is no real difference between knowing the coefficients of $\chi_M(a) \in \Lambda(k)$ and the components of the associated Witt vector $\psi_M(a) \in W(k)$ of an element of A. The following propositions and theorems will make this a bit more explicit. In particular, they give analogues to Theorem 5.26, Remark 5.27 and Corollary 5.28.

Proposition 5.29 *Let k be a field of positive characteristic p, let I be a subset of A that is closed under left and right multiplication by elements of A and let $j \in \mathbb{Z}_{>0}$. The following are equivalent.*

1 *For all $a \in I$ and $i \in \{0, 1, \ldots, j-1\}$, one has $\psi_{M,p^i}(a) = 0$.*

2 *For all $a \in I$ and $s \in \mathbb{Z}_{>0}$ with $p^j \nmid s$, one has $\psi_{M,s}(a) = 0$.*

3 *For all $a \in I$ and $i \in \{0, 1, \ldots, j-1\}$, one has $\chi_{M,p^i}(a) = 0$.*

4 *For all $a \in I$ and $s \in \mathbb{Z}_{>0}$ with $p^j \nmid s$, one has $\chi_{M,s}(a) = 0$.*

5 *For $S = \{1, p, p^2, \ldots, p^{j-1}\}$, the map $I \to W_S(k)$ defined by $a \mapsto \pi_S(\psi_M(a))$ is the zero map.*

6 *For $S = \mathbb{Z}_{>0} \setminus p^j\mathbb{Z}_{>0}$, the map $I \to W_S(k)$ defined by $a \mapsto \pi_S(\psi_M(a))$ is the zero map.*

PROOF The implications **2** $\Rightarrow$ **1** and **4** $\Rightarrow$ **3** are trivial; the implication **1** $\Rightarrow$ **2** is part **1** of Theorem 5.26. The equivalence of **2**, **4** and **6** is trivial, and so is the equivalence of **1** and **5**.

Let $S = \{1, 2, \ldots, p^j - 1\}$, let $a \in I$. We apply induction to $i \in \{0, 1, \ldots, j - 1\}$. For $i = 0$, one has $\psi_{M,p^0}(a) = \chi_{M,p^0}(a) = 0$ for all $a \in I$. Let $i \in \{1, 2, \ldots, j - 1\}$ and assume one has $\psi_{M,p^l}(a) = 0$ for all $l \in \{0, 1, \ldots, i - 1\}$ and $a \in I$. Then by Theorem 5.26, one has $\psi_{M,s}(a) = 0$ for all $s < p^i$, and consequently $\chi_{M,s}(a) = 0$ for all $s < p^i$ and $a \in I$ since one has $\chi_{M,s}(a) = \psi_{M,s}(a)$ provided one has $\psi_{M,s'}(a) = 0$ for all $s' < s$. It immediately follows $\psi_{M,p^i}(a) = \chi_{M,p^i}(a) = 0$ for all $a \in I$. By induction, we find $\psi_{M,p^i}(a) = 0$ for all $a \in I$ and $i \in \{0, 1, \ldots, j - 1\}$. This shows the implication **3** $\Rightarrow$ **1**. ∎

Theorem 5.30 *Suppose k is a field of characteristic $p > 0$. Let I be a subset of A that is closed under left and right multiplication by elements of A. Let $j \in \mathbb{Z}_{\geq 0}$ and suppose that $\chi_{M,p^i}(a) = 0$ for all $a \in I$ and all $i \in \{0, 1, \ldots, j - 1\}$. Then for all $a \in I$, one has $\chi_{M,p^j}(a) = \psi_{M,p^j}(a)$ and for all $a \in I$, $b \in A$ and $s \in \{1, 2, \ldots, p^j\}$, one has $\chi_{M,s}(a+b) = \chi_{M,s}(a)+\chi_{M,s}(b)$. For $s \in \{1, 2, \ldots, p^j - 1\}$ and $a \in I$, $b \in A$, one has $\chi_{M,s}(a + b) = \chi_{M,s}(b)$.*

PROOF Let $S = \{1, 2, \ldots, p^j\}$, let $a \in I$ and $b \in A$. By Proposition 5.29, one has $\chi_s(a) = 0$ for all $a \in I$ and $s \in S \setminus \{p^j\}$. In particular, $\chi_M(a) \equiv 1 + \chi_{M,p^j}(a)T^{p^j} \bmod T^{p^j+1}$, showing immediately that $\chi_{M,p^j}(a) = \psi_{M,p^j}(a)$.

Moreover, if $S = \{1, 2, \ldots, p^j\}$, the equivalence $\pi_S(\psi_M(a+b)) = \pi_S(\psi_M(a))+\pi_S(\chi_M(b))$ from Theorem 5.26 tells us that $\chi_M(a + b) = \chi_M(a) \cdot \chi_M(b) \bmod T^{p^j+1}$. We immediately conclude that $\chi_{M,s}(a + b) = \chi_{M,s}(a) + \chi_{M,s}(b)$ for all $s \in S$; moreover, one has $\chi_{M,s}(a + b) = \chi_{M,s}(b)$ if $s \in S$, $s \neq p^j$. ∎

Remark 5.31 If I, j and k are as in Theorem 5.30, then for all $a, b \in I$, and $i \in \{0, 1, \ldots, j-1\}$, one has $\chi_{M,p^i}(a+b) = 0$. The subgroup I' spanned by I is a two-sided ideal satisfying $\chi_{M,p^i}(a) = 0$ for all $a \in I'$ and all $i \in \{0, 1, \ldots, j-1\}$.

Corollary 5.32 *Suppose k has characteristic $p > 0$. Let B be a subset of A that generates A as a k-vector space.*

1 *Let $j \in \mathbb{Z}_{\geq 0}$ and suppose $\chi_{M,p^i}(b) = 0$ for all $b \in B$ and $i \in \{0, 1, \ldots, j\}$. Then one has $\chi_{M,s}(a) = 0$ for all $a \in A$ and $s \in \mathbb{Z}_{>0} \setminus p^{j+1}\mathbb{Z}_{>0}$.*

2 *Suppose $\dim_k(M)$ is bounded above by $n \in \mathbb{Z}_{>0}$ and assume that $\chi_{M,p^j}(b) = 0$ for any $b \in B$ and $j \in \{0, 1, \ldots, \lfloor \log_p(n) \rfloor\}$. Then M is the 0-module.*

PROOF This follows directly from Corollary 5.28 and Proposition 5.29. ∎

Lemma 5.33 *Suppose k has characteristic $p > 0$ and let B be a subset of A that generates A as a k-vector space. Let M' be an A-submodule of M and let $M'' = M/M'$. Let $j \in \mathbb{Z}_{\geq 0}$ and suppose either $\psi_{M',p^i}(b) = 0$ for any $i \in \{0, 1, \ldots, j-1\}$, $b \in B$, or $\psi_{M'',p^i}(b) = 0$ for any $i \in \{0, 1, \ldots, j-1\}$, $b \in B$.*

Then one has $\psi_{M,p^j}(a) = \psi_{M',p^j}(a) + \psi_{M'',p^j}(a)$ for any $a \in A$.

PROOF Let $S = \{1, p, p^2, \ldots, p^j\}$, let $a \in A$. By Corollary 5.28, one has $\psi_{M'}(a)_S = (0, 0, \ldots, 0, \psi_{M',p^j}(a))$ or $\psi_{M''}(a)_S = (0, 0, \ldots, 0, \psi_{M'',p^j}(a))$, hence by Corollary 3.14, we have $\psi_{M,p^j}(a) = \psi_M(a)_{p^j} = (\psi_{M'}(a) + \psi_{M''}(a))_{p^j} = \psi_{M'}(a)_{p^j} + \psi_{M''}(a)_{p^j}$. ∎

Proposition 5.34 *Assume k has positive characteristic p and let B be a subset of A that generates A as a k-vector space. Let M and N be A-modules, finite-dimensional over k with dimensions bounded above by $n \in \mathbb{Z}_{>0}$. Then the following are equivalent.*

1 *For all $a \in A$, one has $\psi_M(a) = \psi_N(a)$*

2 *For all $a \in A$, $s \in \mathbb{Z}_{>0}$, one has $\psi_{M,s}(a) = \psi_{N,s}(a)$.*

3 *For all $a \in A$, $j \in \mathbb{Z}_{\geq 0}$, one has $\psi_{M,p^j}(a) = \psi_{N,p^j}(a)$.*

4 *For all $b \in B$, $j \in \{0, 1, \ldots, \lfloor \log_p(n) \rfloor\}$, one has $\psi_{M,p^j}(b) = \psi_{N,p^j}(b)$.*

PROOF The equivalence of **1** and **2** is trivial, and the implications **2** $\Rightarrow$ **3** and **3** $\Rightarrow$ **4** are trivial as well.

Assume that **4** holds. Let $J = \lfloor \log_p(n) \rfloor + 1$ and consider the module $P = M^{p^J - 1} \bigoplus N$. Let $S = \{1, 2, \ldots, p^J - 1\}$. Observe that one has $\psi_P(a)_S = (p^J - 1) \cdot \psi_M(a)_S + \psi_N(a)_S = -\psi_M(a)_S + \psi_N(a)_S$ for all $a \in A$ since p^J annihilates $W_S(A)$.

Note that for any $b \in B$, one has $\pi_{\{1,p,\ldots,p^{J-1}\}}(\psi_M(b)) = \pi_{\{1,p,\ldots,p^{J-1}\}}(\psi_N(b))$ by assumption. This means $\psi_{P,p^j}(b) = 0$ for all $b \in B$ and $j \in \{0, 1, \ldots, J-1\}$. Then by Corollary 5.28, one has $\psi_P(a) \in V_{p^J}(W(k))$ for all $a \in A$ and hence one has $\psi_P(a)_S = 0$ for all $a \in A$.

By these observations, we find that for all $a \in A$, one has $-\psi_M(a)_S + \psi_N(a)_S = \psi_P(a)_S = 0$. Therefore, for any $a \in A$, one has $\psi_M(a)_S = \psi_N(a)_S$. Since one has $p^J > n \geq \max\{\dim_k M, \dim_k N\}$, it follows that $\psi_M(a)$ and $\psi_N(a)$ are equal for all $a \in A$ (using that they are both inverses of polynomials of degree at most n via the isomorphism $W(k) \to \Lambda(k)$). This shows the implication **4** $\Rightarrow$ **1**. ∎

Proposition 5.35 *Suppose k has characteristic $p > 0$ and let B be a subset of A that generates A as a k-vector space. Let M and N be semisimple A-modules that are finite-dimensional over k, with dimensions bounded above by $n \in \mathbb{Z}_{>0}$. Then the following are equivalent.*

1 *One has M and N are isomorphic as A-modules.*

2 *For all $a \in A$, one has $\psi_M(a) = \psi_N(a)$.*

3 *For all $b \in B$, $j \in \{0, 1, \ldots, \max\{\lfloor \log_p(n) \rfloor\}\}$, one has $\psi_{M,p^j}(b) = \psi_{N,p^j}(b)$.*

PROOF The equivalence of **2** and **3** is Proposition 5.34. The equivalence of **1** and **2** follows immediately from Theorem 5.10. ∎

Theorem 5.36 *Suppose k has characteristic $p > 0$ and let B be a subset of A that generates A as a k-vector space. Let M and N be A-modules that are finite-dimensional over k, with dimensions bounded above by $n \in \mathbb{Z}_{>0}$. Then the following are equivalent.*

1 *One has M and N are Jordan-Hölder isomorphic as A-modules.*

2 *For all $a \in A$, one has $\psi_M(a) = \psi_N(a)$.*

3 *One has $\psi_{M,p^i}(b) = \psi_{N,p^i}(b)$ for all $b \in B$, $i \in \{0, 1, \ldots, \lfloor \log_p(n) \rfloor\}$.*

4 *For $j = \lfloor \log_p(n) \rfloor$ and $S = \{1, p, p^2, \ldots, p^j\}$, the map $B \to W_S(k)$ given by $b \mapsto \pi_S(\psi_M(b)) - \pi_S(\psi_N(b))$ is identically zero.*

PROOF The equivalence of **1** and **2** follows immediately from Corollary 5.11. The equivalence of **3** and **4** is trivial, and the equivalence of **2** and **3** is Proposition 5.35. ∎

Corollary 5.37 *Suppose k has characteristic $p > 0$. Let B be a subset of A that generates A as a k-vector space. Recall that π_p denotes the projection $W(k) \to W_p(k)$. Then the group homomorphism $G_k(A) \to W_p(k)^B$ defined by $[M] \mapsto (\pi_p(\psi_M(b)))_{b \in B}$ is injective.*

Note that the above corollary is Theorem 5.22 for positive characteristic.

Many of the techniques used in the section above will fail for fields of characteristic 0. We will use alternate methods to show that we may still replace $\Lambda(k)$ by $W_p(k)$ if $p = \mathrm{char}(k) = 0$.

Lemma 5.38 *Suppose A is semisimple and $\mathrm{char}(k) = 0$. Let $n \in \mathbb{Z}_{>0}$. Suppose $S_1, \ldots, S_n$ are pairwise non-isomorphic simple A-modules that are finite-dimensional over k. Then there are $a_1, \ldots, a_n \in A$ such that for all $i \in \{1, 2, \ldots, n\}$, one has $\mathrm{Tr}_{S_i}(a_i) \neq 0$ and such that for any $i, j \in \{1, 2, \ldots, n\}$ with $i \neq j$, one has $\mathrm{Tr}_{S_j}(a_i) = 0$.*

PROOF For each $i \in \{1, 2, \ldots, n\}$ let $s_i \in S_i \setminus \{0\}$. By Lemma 5.9, for each $i \in \{1, 2, \ldots, n\}$, there is $b_i \in A$ such that $b_i s_i = s_i$ and $b_i S_j = 0$ if $j \in \{1, 2, \ldots, n\}$ with $i \neq j$.

Clearly, for each $i \in \{1, 2, \ldots, n\}$, the action of b_i on S_i has eigenvalue 1. By Lemma 5.8, one has $\psi_{S_i}(b_i) \neq 0$. Since A is a $\mathbb{Q}$-algebra, this means that there is $n_i \in \mathbb{Z}_{>0}$ such that the n_i-th ghost component of $\psi_{S_i}(b_i)$ is non-zero using Corollary 4.18. By Corollary 4.16, this means $\mathrm{Tr}_{S_i}(b_i^{n_i}) \neq 0$.

Define $a_i = b_i^{n_i}$. As $b_i S_j = 0$ if $j \neq i$, one has $a_i S_j = 0$ if $j \neq i$ and hence $\mathrm{Tr}_{S_j}(a_i) = 0$ if $j \neq i$. ∎

Proposition 5.39 *Suppose $\mathrm{char}(k) = 0$. Let $n \in \mathbb{Z}_{>0}$. Suppose $S_1, \ldots, S_n$ are pairwise non-isomorphic simple A-modules that are finite-dimensional over k. Then there are $a_1, \ldots, a_n \in A$ such that for all $i \in \{1, 2, \ldots, n\}$, one has $\mathrm{Tr}_{S_i}(a_i) \neq 0$ and such that for any $i, j \in \{1, 2, \ldots, n\}$ with $i \neq j$, one has $\mathrm{Tr}_{S_j}(a_i) = 0$.*

PROOF Let $I = \mathrm{Ann}_A(\bigoplus_{i=1}^n S_i)$. By Lemma 2.11, A/I is semisimple. Moreover, one easily sees that $S_1, \ldots, S_n$ are pairwise non-isomorphic simple A/I-modules. By Lemma 5.38, there are $a_1 + I, \ldots, a_n + I \in A/I$ such that for all $i \in \{1, 2, \ldots, n\}$, one has $\mathrm{Tr}_{S_i}(a_i + I) \neq 0$ and such that for all $i, j \in \{1, 2, \ldots, n\}$ with $j \neq i$, one has $\mathrm{Tr}_{S_i}(a_j + I) = 0$. It easily follows that $\mathrm{Tr}_{S_i}(a_i) \neq 0$ for all $i \in \{1, 2, \ldots, n\}$ and $\mathrm{Tr}_{S_i}(a_j) = 0$ for all $i, j \in \{1, 2, \ldots, n\}$ with $j \neq i$. ∎

With this, we can prove Theorem 5.22 in characteristic 0.

Theorem 5.40 *Suppose k has characteristic 0 and let B be a subset of A that generates A as a k-vector space. Let M, N be A-modules that are finite-dimensional over k. Then the following are equivalent.*

1 *One has M and N are Jordan-Hölder isomorphic as A-modules.*

2 *For all $a \in A$, one has $\psi_{M,1}(a) = \psi_{N,1}(a)$.*

3 *For all $b \in B$, one has $\psi_{M,1}(b) = \psi_{N,1}(b)$.*

4 *For all $b \in B$, one has $\mathrm{Tr}_M(b) = \mathrm{Tr}_N(b)$.*

PROOF The equivalence of **3** and **4** is trivial since $\psi_{M,1}(a) = \mathrm{Tr}_M(a)$ for any $a \in A$. The equivalence of **2** and **3** follows from the linearity of the trace. The implication **1** $\Rightarrow$ **2** is trivial. Suppose **2** holds. As we may replace M and N by their semisimplifications, we may assume M and N are semisimple without loss of generality. This means there are pairwise non-isomorphic simple k-modules $S_1, \ldots, S_n$ and non-negative integers $d_1, \ldots, d_n, e_1, \ldots, e_n$ such that $M = \bigoplus_{i=1}^n S_i^{d_i}$ and $N = \bigoplus_{i=1}^n S_i^{e_i}$.

By Lemma 5.38, there are $a_1, \ldots, a_n \in A$ satisfying $\mathrm{Tr}_{S_i}(a_j) = 0$ if $i \neq j$ and $\mathrm{Tr}_{S_i}(a_i) \neq 0$. Then for $i \in \{1, 2, \ldots, n\}$, one has $d_i \mathrm{Tr}_{S_i}(a_i) = \mathrm{Tr}_M(a_i) = \psi_{M,1}(a_i) = \psi_{N,1}(a_i) = \mathrm{Tr}_N(a_i) = e_i \mathrm{Tr}_{S_i}(a_i)$. Since $\mathrm{Tr}_{S_i}(a_i) \neq 0$, it follows that $d_i = e_i$ for each $i \in \{1, 2, \ldots, n\}$ and hence one has $M \cong N$. ∎

Remark 5.41 The equivalence of **1** and **4** in the above theorem is already known. For example, Corollary 3.8 in chapter XVII of [5], together with the linearity of the trace, directly implies this result. An early version of this result for group algebras can be found in [9].

Corollary 5.42 *Suppose k has characteristic 0. Let B be a subset of A that generates A as a k-vector space. Then the group homomorphism $G_k(A) \to W_0(k)^B$ defined by $[M] \mapsto (\psi_{M,1}(b))_{b \in B}$ is injective.*

Theorem 5.22 follows immediately from Corollary 5.37 and Corollary 5.42.

5.3.2 Replacing $G_k(A)$ by $G_k(A) \bigotimes_{\mathbb{Z}} W_p(k)$.

In this subsubsection, we will prove the following theorem.

Theorem 5.43 *Let $p = \mathrm{char}(k)$. Let B be a subset of A that generates A as a k-vector space. Let $\phi : G_k(A) \to W_p(k)^B$ be the group homomorphism defined by $[M] \mapsto (\pi_p(\psi_M(b)))_{b\in B}$. Then the $W_p(k)$-linear map $\theta : G_k(A) \bigotimes_{\mathbb{Z}} W_p(k) \to W_p(k)^B$ defined by $x \otimes w \mapsto w\phi(x)$ is injective.*

Again, we have distinct proofs in characteristic 0 and $p > 0$.

Lemma 5.44 *Suppose $\mathrm{char}(k) = 0$. Let $n \in \mathbb{Z}_{>0}$. Suppose $S_1, \ldots, S_n$ are pairwise non-isomorphic simple A-modules that are finite-dimensional over k. Let B be a subset of A that generates A as a k-vector space.*

Then there are $b_1, \ldots, b_n \in B$ such that the n-tuples $(\mathrm{Tr}_{S_i}(b_1), \ldots, \mathrm{Tr}_{S_i}(b_n))$ for $i \in \{1, 2, \ldots, n\}$ are k-linearly independent.

PROOF By Proposition 5.39, there are $a_1, \ldots, a_n \in A$ such that for any $i, j \in \{1, 2, \ldots, n\}$ with $i \neq j$, one has $\mathrm{Tr}_{S_i}(a_j) = 0$ and $\mathrm{Tr}_{S_i}(a_i) \neq 0$. In particular, the n-tuples $(\mathrm{Tr}_{S_1}(a_i), \ldots, \mathrm{Tr}_{S_n}(a_i))$ for $i \in \{1, 2, \ldots, n\}$ are k-linearly independent. As these n-tuples lie in the k-span of the n-tuples $(\mathrm{Tr}_{S_1}(b), \ldots, \mathrm{Tr}_{S_n}(b))$ for $b \in B$, there are $b_1, \ldots, b_n \in B$ such that the n-tuples $(\mathrm{Tr}_{S_1}(b_i), \ldots, \mathrm{Tr}_{S_n}(b_i))$ are k-linearly independent. Then the n-tuples $(\mathrm{Tr}_{S_i}(b_1), \ldots, \mathrm{Tr}_{S_i}(b_n))$ for $i \in \{1, 2, \ldots, n\}$ must be k-linearly independent as well. ∎

Theorem 5.45 *Suppose k has characteristic 0. Let B be a subset of A that generates A as a k-vector space. Let $\phi : G_k(A) \to W_0(k)^B$ be the group homomorphism defined by $[M] \mapsto (\mathrm{Tr}_M(b))_{b\in B}$. Then the $W_0(k)$-linear map $\theta : G_k(A) \bigotimes_{\mathbb{Z}} W_0(k) \to W_0(k)^B$ defined by $x \otimes \lambda \mapsto \lambda\phi(x)$ is injective.*

PROOF Note that θ is well-defined. Let $x \in G_k(A) \bigotimes_{\mathbb{Z}} W_0(k)$ and suppose $\theta(x) = 0$. Then x has the form $\sum_{i=1}^m [M_i] \otimes \lambda_i$ for certain $M_i \in \mathcal{M}_k(A)$ and $\lambda_i \in k$. Then there are simple pairwise non-isomorphic A-modules $S_1, \ldots, S_n$, finite-dimensional over k, and non-negative integers $d_{i,j}$ for $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$ such that $[M_i] = \sum_{j=1}^n d_{i,j}[S_j]$. It follows easily that there are $\mu_1, \ldots, \mu_n \in k$ such that $x = \sum_{i=1}^n [S_i] \otimes \mu_i$.

By Lemma 5.44, there are elements $b_1, \ldots, b_n \in B$ such that the n-tuples $(\mathrm{Tr}_{S_i}(b_1), \ldots, \mathrm{Tr}_{S_i}(b_n))$ are k-linearly independent. This means that one has $\sum_{i=1}^n \mu_i(\mathrm{Tr}_{S_i}(b_1), \ldots, \mathrm{Tr}_{S_i}(b_n)) \neq 0$ unless $\mu_1 = \mu_2 = \ldots = \mu_n = 0$. Since $\theta(x) = 0$, one has $\sum_{i=1}^n \mu_i \mathrm{Tr}_{S_i}(b_j) = 0$ for each j, hence it follows that $\mu_1 = \mu_2 = \ldots = \mu_n = 0$ and therefore $x = 0$. ∎

In positive characteristic, we have to work a bit harder for a similar result.

Lemma 5.46 *Suppose k is perfect of positive characteristic p. Then $W_p(k)$ is a domain.*

PROOF Let $w, v \in W_p(k)$, both not equal to 0. Suppose $n, m \in \mathbb{Z}_{\geq 0}$ are minimal such that $w_{p^n} \neq 0$ and $v_{p^m} \neq 0$. Then there are $w', v' \in W_p(k)$ such that $w = p^n w'$, $v = p^m v'$. Namely, define $w'_{p^i} = w_{p^{n+i}}^{1/p^n}$ and $v'_{p^i} = v_{p^{m+i}}^{1/p^m}$. By Lemma 3.20, one has $p^n w' = w$ and $p^m v' = v$. Note that $(w')_1 \neq 0$ and $(v')_1 \neq 0$. Then $(w' \cdot v')_1 \neq 0$, hence $w' \cdot v' \neq 0$. Now $w \cdot v \neq 0$ as $w \cdot v = p^{n+m} w' \cdot v'$ and hence $(w \cdot v)_{p^{n+m}} = ((w' \cdot v')_1)^{p^{n+m}} \neq 0$. ∎

Proposition 5.47 *Suppose k has positive characteristic p. Then $W_p(k)$ is a domain.*

PROOF We can embed $W_p(k)$ in $W_p(\bar{k})$. Since the algebraic closure $\bar{k}$ of k is perfect, it follows by Lemma 5.46 that $W_p(k)$ can be embedded in a domain. Hence $W_p(k)$ is a domain. ∎

Lemma 5.48 *Suppose k has positive characteristic p and suppose k is algebraically closed. Suppose $S_1, \ldots, S_t$ are pairwise non-isomorphic simple A-modules. Then there are $a_1, \ldots, a_t \in A$ such that for all $i \in \{1, 2, \ldots, t\}$, one has $\mathrm{Tr}_{S_i}(a_i) \neq 0$ and such that for all $i, j \in \{1, 2, \ldots, t\}$, one has $\mathrm{Tr}_{S_i}(a_j) = 0$ if $i \neq j$.*

PROOF Let $I = \mathrm{Ann}_A(\bigoplus_{i=1}^t S_i)$. Then A/I is finite-dimensional over k and semisimple by Lemma 2.11. Moreover, $S_1, \ldots, S_t$ are pairwise non-isomorphic simple A/I-modules. By Lemma 2.22, one has $A/I \cong \prod_{i=1}^u M(n_i, k)$ for certain $u \in \mathbb{Z}_{\geq 0}$ and $n_1, \ldots, n_u \in \mathbb{Z}_{>0}$. Moreover, each S_i is isomorphic to some unique k^{n_j} with trivial action by $M(n_l, k)$ if $l \neq j$ and with standard matrix multiplication by $M(n_j, k)$. By permuting the coordinates if necessary, we may assume without loss of generality that $S_i \cong k^{n_i}$ with trivial action by $M(n_j, k)$ if $j \neq i$ and with standard matrix multiplication by $M(n_i, k)$. The element $a_i + I \in M(n_i, k) \subseteq A/I$ satisfying $(a_i + I)_{1,1} = 1$ and $(a_i + I)_{j,k} = 0$ if $(j, k) \neq (1, 1)$ satisfies $(a_i + I)S_j = 0$ if $i \neq j$ and $\mathrm{Tr}_{S_j}(a_i + I) = 1 \neq 0$. It immediately follows that $a_1, \ldots, a_t \in A$ satisfy the required properties. ∎

Corollary 5.49 *Suppose k has positive characteristic p and suppose k is algebraically closed. Let B be a subset of A that generates A as a k-vector space. Suppose $S_1, \ldots, S_n$ are pairwise non-isomorphic simple A-modules.*

Then there are $b_1, \ldots, b_n \in B$ such that the n-tuples $(\mathrm{Tr}_{S_i}(b_1), \ldots, \mathrm{Tr}_{S_i}(b_n))$ for $i \in \{1, 2, \ldots, n\}$ are k-linearly independent.

PROOF The proof is analogous to the proof of Lemma 5.44, using Lemma 5.48 instead of Proposition 5.39 where necessary. ∎

Proposition 5.50 *Suppose k has positive characteristic p and suppose k is algebraically closed. Let B be a subset of A that generates A as a k-vector space. Recall that π_p is the projection $W(k) \to W_p(k)$. Let $\phi : G_k(A) \to W_p(k)^B$ be the group homomorphism defined by $[M] \mapsto (\pi_p(\psi_M(b)))_{b \in B}$. Then the $W_p(k)$-linear map $\theta : G_k(A) \bigotimes_{\mathbb{Z}} W_p(k) \to W_p(k)^B$ defined by $x \otimes w \mapsto w\phi(x)$ is injective.*

PROOF Note that θ is well-defined. Let $x \in G_k(A) \bigotimes_{\mathbb{Z}} W_p(k)$ and assume $\theta(x) = 0$. We may write $x = \sum_{i=1}^n [S_i] \otimes w_i$ for certain pairwise non-isomorphic A-modules $S_1, \ldots, S_n$ and elements $w_1, \ldots, w_n \in W_p(k)$.

By Corollary 5.49, there are elements $b_1, \ldots, b_n \in B$ such that the n-tuples $(\mathrm{Tr}_{S_i}(b_1), \ldots, \mathrm{Tr}_{S_i}(b_n))$ for $i \in \{1, 2, \ldots, n\}$ are k-linearly independent.

Consider the following commutative diagram.

$$\begin{array}{ccc} G_k(A)\bigotimes_{\mathbb{Z}} W_p(k) & \xrightarrow{\theta} & W_p(k)^B \\ & \searrow^{\tau} & \downarrow{\scriptstyle \Pi_0} \\ & & k^B \end{array}$$

Here Π_0 is the projection $W_p(k)^B \to k^B$ defined by the componentwise projection $\pi_0 : W_p(k) \to W_0(k) = k$. Note that the map τ sends a simple tensor $[M] \otimes w$ to $(\mathrm{Tr}_M(b)\pi_0(w))_{b\in B}$ since $\mathrm{Tr}_M(b)$ is the first coefficient of $\psi_M(b)$ for each $b \in B$.

Suppose $w_1, \ldots, w_n$ are not all 0. Then there is some minimal $l \in \mathbb{Z}_{\geq 0}$ such that there is $i \in \{1, 2, \ldots, n\}$ for which the p^l-th coefficient of w_i is non-zero, say $i = 1$ without loss of generality. As k is algebraically closed and hence perfect, it follows that there are $w_1', \ldots, w_n' \in W_p(k)$ such that $w_i = p^l w_i'$ for each $i \in \{1, 2, \ldots, n\}$. In particular, one has $\pi_0(w_1') = ((w_1)_{p^l})^{1/p^l} \neq 0$. Let $x' = \sum_{i=1}^n [S_i] \otimes w_i'$.

We now find $x = p^l x'$. As $\theta(x) = 0$, it follows that $p^l\theta(x') = 0$ and hence $\theta(x') = 0$ since $W_p(k)$ is torsion-free as an abelian group. As the n-tuples $(\mathrm{Tr}_{S_i}(b_1), \ldots, \mathrm{Tr}_{S_i}(b_n))$ are k-linearly independent, this can only be the case if $\pi_0(w_i') = 0$ for each $i \in \{1, 2, \ldots, n\}$, contradicting $\pi_0(w_1') \neq 0$. Hence one has $w_i = 0$ for each $i \in \{1, 2, \ldots, n\}$ and hence x is equal to 0. ∎

Theorem 5.51 *Suppose k has positive characteristic p. Let B be a subset of A that generates A as a k-vector space. Let $\phi : G_k(A) \to W_p(k)^B$ be the group homomorphism defined by $[M] \mapsto (\pi_p(\psi_M(b)))_{b\in B}$. Then the $W_p(k)$-linear map $\theta : G_k(A)\bigotimes_{\mathbb{Z}} W_p(k) \to W_p(k)^B$ defined by $x \otimes w \mapsto w\phi(x)$ is injective.*

Proof Let i denote the natural inclusion $W_p(k) \to W_p(\bar{k})$ and let ι denote the map $G_k(A) \to G_{\bar{k}}(A_{\bar{k}})$ defined by $[M] \mapsto [M_{\bar{k}}]$. Note that the latter is well-defined and injective by Corollary 5.13.

As both $W_p(\bar{k})$ and $G_k(A)$ are torsion-free, they are both flat by Lemma 2.26. Hence the maps $\mathrm{Id} \otimes i : G_k(A)\bigotimes_{\mathbb{Z}} W_p(k) \to G_k(A)\bigotimes_{\mathbb{Z}} W_p(\bar{k})$ and $\iota \otimes \mathrm{Id} : G_k(A)\bigotimes_{\mathbb{Z}} W_p(\bar{k}) \to G_{\bar{k}}(A_{\bar{k}})\bigotimes_{\mathbb{Z}} W_p(\bar{k})$ are injective and thus the map $\iota \otimes i = (\iota \otimes \mathrm{Id}) \circ (\mathrm{Id} \otimes i)$ is injective.

The following diagram is commutative.

$$\begin{array}{ccc} G_k(A)\bigotimes_{\mathbb{Z}} W_p(k) & \xrightarrow{\theta} & W_p(k)^B \\ \downarrow{\scriptstyle \iota \otimes i} & & \downarrow{\scriptstyle i_B} \\ G_{\bar{k}}(A_{\bar{k}})\bigotimes_{\mathbb{Z}} W_p(\bar{k}) & \xrightarrow{\bar{\theta}} & W_p(\bar{k})^B \end{array}$$

Here i_B is the componentwise inclusion and $\bar{\theta}$ is the injective group homomorphism from Proposition 5.50. It follows that θ is injective as well. ∎

Together, Theorem 5.45 and Theorem 5.51 prove Theorem 5.43. The following example will show that it is possible that surjectivity of the map θ in Theorem 5.43 may occur.

Example 5.52 Let k be any field and assume $A = k$. Clearly, the set $B = \{1\}$ generates A as a k-vector space. Then one has $G_k(A) \bigotimes_{\mathbb{Z}} W_p(k) \cong W_p(k)$, as $G_k(A) \cong \mathbb{Z}$. Hence the map $\theta : G_k(A) \bigotimes_{\mathbb{Z}} W_p(k) \to W_p(k)^B$, defined as in the previous theorem, is an isomorphism.

Example 5.53 Surjectivity is not guaranteed. For example, let k be any field and take $A = k[X]/(X^2)$. It only has one simple module, namely $k[X]/(X)$, so $G_k(A) \bigotimes_{\mathbb{Z}} W_p(k) \cong W_p(k)$ which cannot map surjectively to $W_p(k)^B$ for any subset B of A that generates A as a k-vector space since $\dim_k(A) = 2$.

Note that the proof of Theorem 5.51 and Theorem 5.45 suggests that the cardinality of a set $B \subseteq A$ such that the conclusion of Theorem 5.43 is satisfied can be bounded above by the cardinality of the set of isomorphism classes of simple A-modules that are finite-dimensional over k. If there are only finitely many pairwise non-isomorphic simple A-modules $S_1, \ldots, S_n$ that are finite-dimensional over k, one has $G_k(A) \bigotimes_{\mathbb{Z}} W_p(k) \cong \bigoplus_{i=1}^n W_p(k)[S_i]$. Moreover, the number n is bounded above by $\dim_k(A)$. If k is algebraically closed or if k has characteristic 0, one may take $B = \{a_1, \ldots, a_n\}$ where $a_1, \ldots, a_n$ satisfy the conditions of Lemma 5.48 or Proposition 5.39 depending on whether k is algebraically closed or has characteristic 0. In this case, the set $B = \{a_1, \ldots, a_n\}$ does not necessarily generate A as a k-vector space. I do not know whether a similar result holds if k is neither algebraically closed nor has characteristic 0. Likewise, I do not know whether a similar result holds if A has infinitely many pairwise non-isomorphic simple modules.

In general, if $\mathcal{S}$ is the set of isomorphism classes of simple A-modules, one has $G_k(A) \bigotimes_{\mathbb{Z}} W_p(k) \cong \bigoplus_{S \in \mathcal{S}} W_p(k)[S]$, which embeds into $W_p(k)^B$ by Theorem 5.43. Since $W_p(k)^B$ is a product of copies of $W_p(k)$ and not a direct sum, the cardinality of B may be strictly smaller than the cardinality of $\mathcal{S}$. For example, take $A = k[X]$ with A an uncountable field. Then the set $B = \{1, X, X^2, \ldots\}$ is countable, while there are uncountably many pairwise non-isomorphic simple A-modules (for example, for each $\lambda, \mu \in k$, the modules $k[X]/(X - \lambda)$ and $k[X]/(X - \mu)$ are simple and non-isomorphic).

Conversely, the cardinality of a set B such that the conclusion of Theorem 5.43 is satisfied should be at least equal to the minimum of the cardinality of $\mathbb{N}$ and the cardinality of the set of isomorphism classes of simple A-modules that are finite-dimensional over k.

5.3.3 The injection $G_k(A) \bigotimes_{\mathbb{Z}} W(k) \hookrightarrow W(k)^B$

As might be expected from the title of this subsubsection, we are going to prove the following theorem.

Theorem 5.54 *Let k be a field, let A be a k-algebra and let B be a subset of A that generates A as a k-vector space. Let $\phi : G_k(A) \to W(k)^B$ be the group homomorphism defined by $[M] \mapsto (\psi_M(b))_{b \in B}$.*

Then the $W(k)$-linear map $\vartheta : G_k(A) \bigotimes_{\mathbb{Z}} W(k) \to W(k)^B$ defined by $x \otimes w \mapsto w\phi(x)$ is injective.

Lemma 5.55 *Let k be a field of characteristic $p > 0$. Let $w = (w_1, w_p, w_{p^2}, \ldots)$ be an element of $W_p(k)$ and assume $w_1 \neq 0$. Then w is invertible.*

PROOF Let $n, m \in \mathbb{Z}_{>0}$; assume $n \geq m$ without loss of generality. Let $\alpha, \beta \in k$. Then one has $V_{p^n}(\{\alpha\})V_{p^m}(\{\beta\}) = p^m V_{p^n}(\{\alpha\beta^{p^{n-m}}\}) = V_{p^{n+m}}(\{\alpha^{p^m}\beta^{p^n}\})$. Hence for any $v, u \in W_p(k)$, one has $V_{p^n}(v) \cdot V_{p^m}(u) \in V_{p^{n+m}}(W_p(k))$.

Write $v = 1 - w\{w_1^{-1}\}$. Then the first component of v is equal to 0, hence $v \in V_p(W_p(k))$ (noting that V_p is well-defined on $W_p(k)$). Then one has $v^l \in V_{p^l}(W_p(k))$ for each $l \in \mathbb{Z}_{>0}$ and hence $\sum_{i=0}^{\infty} v^i$ exists in $W_p(k)$.

One has $w\{w_1^{-1}\} \cdot \sum_{i=0}^{l} v^i = (1-v)\sum_{i=0}^{l} v^i = 1 - v^{l+1}$ and hence one finds $w\{w_1^{-1}\}\sum_{i=0}^{\infty} v^i = 1$ by continuity of multiplication. Hence w is invertible. ∎

Proposition 5.56 *Let k be a perfect field. Let $p = \mathrm{char}(k)$. Then $W_p(k)$ is a principal ideal domain, and each non-zero ideal of $W_p(k)$ has the form $p^n W_p(k)$ for some $n \in \mathbb{Z}_{\geq 0}$.*

PROOF If $p = 0$, this is trivial; the only ideals are 0 and $W_0(k) = k$. Assume $p > 0$. Let $I \subseteq W_p(k)$ be a non-zero ideal. Then there is some minimal $n \in \mathbb{Z}_{>0}$ such that there is $w = (w_1, w_p, \ldots) \in I$ that satisfies $w_{p^n} \neq 0$. As k is perfect, one has $w = p^n v$ for some $v = (v_1, v_p, \ldots) \in W_p(k)$ with $v_1 \neq 0$. By Lemma 5.55, v is invertible and hence $p^n \in I$. Hence $p^n W_p(k) \subseteq I$. Let $u = (u_1, u_p, \ldots) \in I$. Then by the minimality condition on n, one has $u_1 = u_p = \ldots = u_{p^{n-1}} = 0$. Hence one has $u \in p^n W_p(k)$ since k is perfect. Hence one has $I = p^n W_p(k)$. ∎

Proposition 5.57 *Let k be a perfect field, let A be a k-algebra and let B be a subset of A that generates A as a k-vector space. Let $p = \mathrm{char}(k)$. Let $\theta : G_k(A) \bigotimes_{\mathbb{Z}} W_p(k) \to W_p(k)^B$ be the injective $W_p(k)$-linear map from Theorem 5.43. Then the map $\theta \otimes \mathrm{Id} : (G_k(A) \bigotimes_{\mathbb{Z}} W_p(k)) \bigotimes_{W_p(k)} W(k) \to W_p(k)^B \bigotimes_{W_p(k)} W(k)$ is well-defined and injective.*

PROOF Note that $W(k)$ is a $W_p(k)$-module by Remark 4.24, so $\theta \otimes \mathrm{Id}$ is well-defined. Since $W(k) \cong W_p(k)^{\mathbb{Z}_{>0} \setminus p\mathbb{Z}_{>0}}$ as a $W_p(k)$-module, it is torsion-free as a $W_p(k)$-module as well.

By Proposition 5.56, $W_p(k)$ is a principal ideal domain. By Lemma 2.26, it follows $W(k)$ is flat and therefore, $\theta \otimes \mathrm{Id}$ is injective. ∎

Lemma 5.58 *Let k be a field of characteristic p and let A be a k-algebra. The map $\gamma : G_k(A) \bigotimes_{\mathbb{Z}} W(k) \to (G_k(A) \bigotimes_{\mathbb{Z}} W_p(k)) \bigotimes_{W_p(k)} W(k)$, given by $[M] \otimes w \mapsto ([M] \otimes 1) \otimes w$, is an isomorphism.*

PROOF One has $G_k(A) \bigotimes_{\mathbb{Z}} W(k) \cong G_k(A) \bigotimes_{\mathbb{Z}} (W_p(k) \bigotimes_{W_p(k)} W(k)) \cong (G_k(A) \bigotimes_{\mathbb{Z}} W_p(k)) \bigotimes_{W_p(k)} W(k)$. One easily verifies that this canonical isomorphism is given by $[M] \otimes w \mapsto ([M] \otimes 1) \otimes w$. ∎

Lemma 5.59 *Let k be a perfect field and let A be a k-algebra. Let B be a subset of A that generates A as a k-vector space and let $p = \mathrm{char}(k)$. Then the $W_p(k)$-linear map $\iota : W_p(k)^B \bigotimes_{W_p(k)} W(k) \to W(k)^B$ defined by $(v_b)_{b \in B} \otimes w \mapsto (v_b w)_{b \in B}$ is injective.*

PROOF Since $W_p(k)$ is a principal ideal domain and since $W(k)$ is torsion-free as a $W_p(k)$-module, this follows directly from Proposition 2.27. ∎

Proposition 5.60 *Let k be a perfect field and let A be a k-algebra. Let B be a subset of A that generates A as a k-vector space. Let $\phi : G_k(A) \to W(k)^B$ be the group homomorphism defined by $[M] \mapsto (\psi_M(b))_{b\in B}$. Then the $W(k)$-linear map $\vartheta : G_k(A) \bigotimes_{\mathbb{Z}} W(k) \to W(k)^B$ defined by $x \otimes w \mapsto w\phi(x)$ is injective.*

PROOF Let $p = \mathrm{char}(k)$ and consider the following diagram.

$$\begin{array}{ccc} (G_k(A) \bigotimes_{\mathbb{Z}} W_p(k)) \bigotimes_{W_p(k)} W(k) & \xrightarrow{\theta \otimes \mathrm{Id}} & W_p(k)^B \bigotimes_{W_p(k)} W(k) \\ \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \iota} \\ G_k(A) \bigotimes_{\mathbb{Z}} W(k) & \xrightarrow{\qquad\qquad\vartheta\qquad\qquad} & W(k)^B \end{array}$$

The maps in the diagram are those from Proposition 5.57, Lemma 5.58 and Lemma 5.59. One easily verifies that this diagram is commutative. Injectivity of ϑ follows immediately. ∎

Theorem 5.61 *Let k be a field and let A be a k-algebra. Let B be a subset of A that generates A as a k-vector space. Let $\phi : G_k(A) \to W(k)^B$ be the group homomorphism defined by $[M] \mapsto (\psi_M(b))_{b\in B}$. Then the $W(k)$-linear map $\vartheta : G_k(A) \bigotimes_{\mathbb{Z}} W(k) \to W(k)^B$ defined by $x \otimes w \mapsto w\phi(x)$ is injective.*

PROOF Let $\bar{k}$ be some algebraic closure of k. Let i denote the natural inclusion $W(k) \to W(\bar{k})$ and let ι denote the map $G_k(A) \to G_{\bar{k}}(A_{\bar{k}})$ defined by $[M] \mapsto [M_{\bar{k}}]$. Note that the latter is well-defined and injective by Corollary 5.13.

As both $W(\bar{k})$ and $G_k(A)$ are torsion-free as $\mathbb{Z}$-modules, they are both flat by Lemma 2.26. Hence the maps $\mathrm{Id} \otimes i : G_k(A) \bigotimes_{\mathbb{Z}} W(k) \to G_k(A) \bigotimes_{\mathbb{Z}} W(\bar{k})$ and $\iota \otimes \mathrm{Id} : G_k(A) \bigotimes_{\mathbb{Z}} W(\bar{k}) \to G_{\bar{k}}(A_{\bar{k}}) \bigotimes_{\mathbb{Z}} W(\bar{k})$ are injective and thus the map $\iota \otimes i = (\iota \otimes \mathrm{Id}) \circ (\mathrm{Id} \otimes i)$ is injective.

The following diagram is commutative.

$$\begin{array}{ccc} G_k(A) \bigotimes_{\mathbb{Z}} W(k) & \xrightarrow{\vartheta} & W(k)^B \\ \downarrow{\scriptstyle \iota \otimes i} & & \downarrow{\scriptstyle i_B} \\ G_{\bar{k}}(A_{\bar{k}}) \bigotimes_{\mathbb{Z}} W(\bar{k}) & \xrightarrow{\bar{\vartheta}} & W(\bar{k})^B \end{array}$$

Here i_B is the componentwise inclusion and $\bar{\vartheta}$ is the injective group homomorphism from Proposition 5.60. It follows that ϑ is injective as well. ∎

This proves Theorem 5.54.

Finally, note that one has an even stronger version of Theorem 5.61 since the image of ϑ is contained in $\varinjlim S^B$, where S ranges over the finitely generated $W_p(k)$-submodules of $W(k)$. If B is infinite, $\varinjlim S^B$ is not equal to $W(k)^B$.

5.3.4 A different way of generalization

In the previous subsection, we found a generalization of Theorem 5.21 by replacing $G_k(A)$ by the larger ring $G_k(A) \bigotimes_{\mathbb{Z}} W(k)$. In this section, we find a generalization of Theorem 5.21 by replacing a subset B of A that generates A as a k-vector space by a subset C of A such that one has $A = \sum_{c \in C} k[c] \cdot c$.

Theorem 5.62 *Let k be a field and A a k-algebra. Let C be a subset of A such that one has $A = \sum_{c \in C} k[c] \cdot c$. Then the group homomorphism $\phi : G_k(A) \to W(k)^C$ defined by $[M] \mapsto (\psi_M(c))_{c \in C}$ is injective.*

PROOF Let $B = \{c^n : c \in C, n \in \mathbb{Z}_{>0}\}$. Then B generates A as a k-vector space. Define $\theta : \mathrm{Im}(\phi) \to W(k)^B$ by mapping $(\psi_M(c))_{c \in C}$ to $(P_n(\psi_M(c)))_{c^n \in B}$ (recall that P_n denotes the n-th Witt power sum). Note that θ is well-defined; if one has $c^n = \tilde{c}^{\tilde{n}}$, one has $P_n(\psi_M(c)) = \psi_M(c^n) = \psi_M(\tilde{c}^{\tilde{n}}) = P_{\tilde{n}}(\psi_M(\tilde{c}))$ using Proposition 4.15. It is easily seen that θ is an injective group homomorphism. Since the group homomorphism $G_k(A) \to W(k)^B$ defined by $[M] \mapsto (\psi_M(b))_{b \in B}$ is injective by Theorem 5.21, and since this homomorphism is equal to $\theta \circ \phi$ by Proposition 4.15, one must have that ϕ is injective as well. ∎

Unfortunately, if C is as above, the group homomorphism $G_k(A) \bigotimes_{\mathbb{Z}} W(k) \to W(k)^C$ defined by $[M] \otimes w \mapsto (\psi_M(c)w)_{c \in C}$ is not in general injective and likewise, if $p = \mathrm{char}(k)$, the group homomorphism $G_k(A) \to W_p(k)^C$ defined by $[M] \mapsto (\pi_p(\psi_M(c)))_{c \in C}$ is not in general injective.

Example 5.63 The following are counterexamples to the statements of Theorem 5.22 and Theorem 5.54 with B replaced by a set C as above.

1 Let k be a field of characteristic p not equal to 2. Let $A = k[X]$ be the polynomial ring in X and let $C = \{1, X\}$. Clearly one has $A = \sum_{c \in C} k[c]c$. Let $M = k[X]/(X) \bigoplus k[X]/(X)$ and let $N = k[X]/(X^2 - 1)$. Then M and N are semisimple, not Jordan-Hölder isomorphic (as $\chi_M(X^2) \neq \chi_N(X^2)$) and satisfy $(\pi_p(\psi_M(1)), \pi_p(\psi_M(X))) = (2, 0) = (\pi_p(\psi_N(1)), \pi_p(\psi_N(X)))$. Hence the homomorphism $G_k(A) \to W_p(k)^C$ given by $[M] \mapsto (\psi_M(c))_{c \in C}$ is not injective.

2 Let k be a field of characteristic p not equal to 2. Let $A = k[X]/(X^2 - 1)$. Let $C = \{X\}$. Since one has $X^2 = 1$, the set $\{X, X^2\}$ generates A as a k-module and hence one has $\sum_{c \in C} k[c]c = A$. Let $M = k[X]/(X - 1)$ and let $N = k[X]/(X + 1)$. Then M and N are simple non-isomorphic A-modules. Let w be the Witt vector associated to $(1+T)^{-1} \in \Lambda(k)$. The elements $[M] \otimes 1$ and $[N] \otimes w$ in $G_k(A) \bigotimes_{\mathbb{Z}} W(k)$ are distinct, and one has $\psi_M(X) \cdot 1 = 1 = \psi_N(X) \cdot w$. Hence the homomorphism $G_k(A) \bigotimes_{\mathbb{Z}} W(k) \to W(k)^C$ given by $[M] \otimes v \mapsto v \cdot (\psi_M(c))_{c \in C}$ is not injective.

3 Let k be any field and let $A = k[X]$. The set $C = \{1, X\}$ satisfies $A = \sum_{c \in C} k[c]c$. In this case, there is no subset C' of A of cardinality at most 1 such that the group homomorphism $\phi : G_k(A) \to W(k)^{C'}$ defined as in

Theorem 5.62 is injective. Suppose namely that such C' exists. Clearly one has $C' \neq \emptyset$, so C' contains one element, say $f \in k[X]$. If f is constant, one has $\psi_M(f) = \dim_k(M) \cdot \{f\}$ for each A-module M that is finite-dimensional over k. The modules $M = k[X]/(X)$ and $N = k[X]/(X + 1)$ are both one-dimensional and are not Jordan-Hölder isomorphic, and one has $\psi_M(f) = \psi_N(f)$, contradicting injectivity. If f is not constant, consider the modules $M = k[X]/(f)$ and $N = 0$. Clearly, the modules M and N are not Jordan-Hölder isomorphic. On the other hand, one has $\psi_M(f) = 0 = \psi_N(f)$, contradicting the assumption of injectivity again. So the minimal cardinality of a set C' such that group homomorphism $\phi : G_k(A) \to W(k)^{C'}$ defined as in Theorem 5.62 is injective is 2. So C is minimal in a way.

References

[1] A. Cohen, G. Ivanyos, D. Wales, *Finding the radical of an algebra of linear transformations*, 1997, Journal of Pure and Applied Algebra 117 & 118, 177-193

[2] L. Rónyai, *Computing the Structure of Finite Algebras*, 1990, Journal of Symbolic Computation 9, 355-373

[3] G. Dalla Torre, *Representation Theory*, 2010 http://www.win.tue.nl/mm-representation-theory/representation_theory.pdf

[4] H.W. Lenstra, *Construction of the ring of Witt vectors*, March 4, 2002 math.berkeley.edu/ hwl/papers/witt.pdf

[5] S. Lang, *Algebra*, 2002

[6] R. Brauer and C. Nesbitt, *On the modular representations of groups of finite order I*, 1980, Richard Brauer: Collected papers, Vol I, 336-354

[7] http://crazyproject.wordpress.com/2011/05/30/over-a-pid-flat-and-torsion-free-are-equivalent/

[8] M. Bhargava and M. Satriano, *On a notion of "Galois closure" for extensions of rings*, 2010

[9] G. Frobenius and I. Schur, *Über die Äquivalenz der Gruppen linearer Substitutionen*, Sitzungsberichte d Preuss. Akad. d. Wiss. 1906, 209-217