Journal of Algebra 324 (2010) 598–630

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Galois orders in skew monoid rings

Vyacheslav Futorny [a,*], Serge Ovsienko [b]

[a] Instituto de Matemática e Estatística, Universidade de São Paulo, Caixa Postal 66281, São Paulo, CEP 05315-970, Brazil
[b] Faculty of Mechanics and Mathematics, Kiev Taras Shevchenko University, Vladimirskaya 64, 01601, Kiev, Ukraine

A R T I C L E I N F O

Article history:
Received 22 April 2008
Available online 21 May 2010
Communicated by Nicolás Andruskiewitsch

Keywords:
Galois ring
Galois order
Skew monoid ring
Harish–Chandra subalgebra

A B S T R A C T

We introduce a new class of noncommutative rings – Galois orders, realized as certain subrings of invariants in skew semigroup rings, and develop their structure theory. The class of Galois orders generalizes classical orders in noncommutative rings and contains many important examples, such as the Generalized Weyl algebras, the universal enveloping algebra of the general linear Lie algebra, associated Yangians and finite W-algebras.

Contents

* Corresponding author.
E-mail addresses: futorny@ime.usp.br (V. Futorny), ovsyenko@mechmat.univ.kiev.ua (S. Ovsienko).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2010.05.006

1. Introduction

Let Γ be an integral domain and $U \supset \Gamma$ an associative noncommutative algebra over a base field $\Bbbk$. A motivation for the study of pairs "algebra-subalgebra" comes from the representation theory of Lie algebras. In particular, in the theory of Harish-Chandra modules U is the universal enveloping algebra of a reductive finite dimensional Lie algebra L and Γ is the universal enveloping algebra of some reductive Lie subalgebra $L' \subset L$. For instance, the case when Γ is the universal enveloping algebra of a Cartan subalgebra leads to a class of Harish-Chandra modules with respect to this Cartan algebra – weight modules. Another important example is a pair (U, Γ), where U is the universal enveloping algebra and Γ is a certain maximal commutative subalgebra of U, called *Gelfand–Tsetlin subalgebra*. In the case $U = U(\mathfrak{gl}_n)$ the analogs of Harish-Chandra modules – Gelfand–Tsetlin modules – were studied in [DFO1]. Similarly, Okunkov and Vershik [OV] showed that representation theory of the symmetric group S_n is associated with a pair (U, Γ), where U is the group algebra of S_n and Γ is the maximal commutative subalgebra generated by the Jucys–Murphy elements.

An attempt to understand the phenomena related to the Gelfand–Tsetlin formulae [GTs] was the paper [DFO2] where the notion of Harish-Chandra subalgebra of an associative algebra and the corresponding notion of a Harish-Chandra module were introduced. In particular, in [DFO2] the categories of Harish-Chandra modules were described as categories of modules over some explicitly constructed categories. This construction is a broad generalization of the presentation of finite dimensional associative algebras by quivers and relations. This techniques was applied to the study of Gelfand–Tsetlin modules for $\mathfrak{gl}_n$.

Current paper can be viewed on one hand as a development of the ideas of [DFO2] in the "semi-commutative case", i.e. noncommutative algebra and commutative subalgebra and, on the other hand, as an attempt to understand the role of skew group algebras in the representation theory of infinite dimensional algebras (e.g. [Bl,Ba,BavO,Ex]). Recall, that the algebras A_1, $U(\mathfrak{sl}_2)$ and their quantum analogues are unified by the notion of a *generalized Weyl algebra*. Their irreducible modules are completely described modulo classification of irreducible elements in a skew polynomial ring in one variable over a skew field. The main property of a generalized Weyl algebra U is the existence of a commutative subalgebra $\Gamma \subset U$ such that the localization of U by $S = \Gamma \setminus \{0\}$ is the skew polynomial algebra. On the other hand this technique cannot be applied in case of more complicated algebras such as the universal enveloping algebras of simple Lie algebras of rank $\geqslant 2$.

We make an important observation that the Gelfand–Tsetlin formulae for $\mathfrak{gl}_n$ define an embedding of the corresponding universal enveloping algebra into a skew group algebra of a free abelian group over some field of rational functions L (see also [Kh]). A remarkable fact is that this field L is a Galois extension of the field of fractions of the corresponding Gelfand–Tsetlin subalgebra of the universal enveloping algebra. This fact leads to a concept of *Galois orders* defined as certain subrings of invariants in skew monoid rings.

We propose a notion of a "noncommutative order" as a pair (U, Γ) where U is a ring, $\Gamma \subset U$ a commutative subring such that the set $S = \Gamma \setminus \{0\}$ is left and right Ore subset in U and the corresponding ring of fractions $\mathcal{U}$ is a simple algebra (in general, Γ is not central in U). Galois orders introduced in the paper are examples of such noncommutative orders.

Let Γ be a commutative finitely generated domain, K the field of fractions of Γ, $K \subset L$ a finite Galois extension, $G = G(L/K)$ the corresponding Galois group, $\mathcal{M} \subset \operatorname{Aut} L$ a submonoid. Assume that G belongs to the normalizer of $\mathcal{M}$ in $\operatorname{Aut} L$ and for $m_1, m_2 \in \mathcal{M}$ their double G-cosets coincide if and only if $m_1 = g m_2 g^{-1}$ for some $g \in G$, i.e. $\mathcal{M}$ is *separating* (see Definition 1 and Lemma 2.2). If $\mathcal{M}$ is a group the last condition can be rewritten as $\mathcal{M} \cap G = \{e\}$. If G acts on $\mathcal{M}$ by conjugation then G acts on the skew group algebra $L * \mathcal{M}$ by authomorphisms: $g \cdot (am) = (g \cdot a)(g \cdot m)$. Let $\mathcal{K} = (L * \mathcal{M})^G$ be the subalgebra of G-invariants in $L * \mathcal{M}$.

We will say that an associative ring U is a *Γ-ring*, provided there is a fixed embedding $i : \Gamma \to U$. We introduce an important class of subrings in $\mathcal{K}$: a finitely generated Γ-subring $U \subset \mathcal{K}$ is called a *Galois Γ-ring* (or *Galois ring with respect to Γ*) if $KU = UK = \mathcal{K}$ (see Definition 3). If Γ is fixed then we simply say that U is a *Galois ring*.

We introduce a special class of Galois rings – *integral Galois rings* or *Galois orders*. These rings satisfy some local finiteness condition (see Definition 5).

A concept of a Galois Γ-order is a natural noncommutative generalization of a classical notion of Γ-order in skew group ring $\mathcal{K}$ since we do not require the centrality of Γ in U (cf. [MCR], Chapter 5, 3.5). We note the difference of our definition from the notion of order given in [MCR] (Chapter 3, 1.2), [HGK] (Section 9).

How big is the class of Galois rings and orders? We note that any commutative algebra is Galois. If $\Gamma \subset U \subset K \subset L$ and U is finitely generated Γ-ring, then U is a Galois Γ-ring. If Γ is noetherian then U is an order if and only if U lies in the integral closure of Γ in K. Some rings of invariant differential operators, e.g. symmetric and orthogonal differential operators on n-dimensional torus, are Galois rings with respect to certain subrings (cf. Section 7.3). We also show in Section 7 that the following algebras are Galois orders in corresponding skew group rings:

- Generalized Weyl algebras over integral domains with infinite order automorphisms which include many classical algebras, such as n-th Weyl algebra A_n, quantum plane, q-deformed Heisenberg algebra, quantized Weyl algebras, Witten–Woronowicz algebra among the others [Ba,BavO].
- The universal enveloping algebra $U(\mathfrak{gl}_n)$ with its Gelfand–Tsetlin subalgebra is a Galois order.
- It is shown in [FMO,FMO1] that shifted Yangians and finite W-algebras associated with $\mathfrak{gl}_n$ are Galois orders with respect to the corresponding Gelfand–Tsetlin subalgebras.

In Section 3 it is shown that the algebra $\mathcal{K}$ has the canonical decomposition into the direct sum of K-finite dimensional K-bimodules of a special kind (so-called balanced K-bimodules). The importance of this decomposition leads us to an investigation of the category of balanced K-bimodules. This category turns out to be tensor semisimple and its Grothendieck ring tensored with $\mathbb{Q}$ is isomorphic to the Hecke algebra over $\mathbb{Q}$ of $\operatorname{Aut}_{\Bbbk} L$ with respect to the subgroup G (Corollary 3.3). This fact provides extra information about the multiplication in $\mathcal{K}$. We define here some additive generators of $\mathcal{K}$, which we denote $[a\varphi]$, $a \in K$, $\varphi \in \mathcal{M}$. This notation is used extensively throughout the paper.

We prove that the isoclasses of the balanced (more precisely, L-balanced) bimodules are in a natural bijection with the orbits of the action of the group G on $\mathcal{M}$. Every $\varphi \in \mathcal{M}$ defines a simple L-balanced K-bimodule $V(\varphi)$. We show that the bimodules $V(\varphi)$ exhaust all simple objects in the category of balanced K-bimodules. In particular, the K-module $K[a\varphi]K \subset \mathcal{K}$ is isomorphic to $V(\varphi)$ (cf. Theorem 3.2).

In Sections 4 and 5 we study the structure and properties of Galois rings and Galois orders respectively. Since the main feature of the Galois rings and Galois orders is their realization as subalgebras of $\mathcal{K} = (L * \mathrm{M})^G$ we present in 4.1 some general properties of the rings of invariants in skew group algebras. We show that $U \cap K$ is a maximal commutative subring in U and the center of U coincides with $\mathcal{M}$-invariants in $U \cap K$ (Theorem 4.1). Moreover, the set $S = \Gamma \setminus \{0\}$ is an Ore multiplicative set (both from the left and from the right) and the corresponding localizations $U[S^{-1}]$ and $[S^{-1}]U$ are canonically isomorphic to $\mathcal{K}$ (Proposition 4.2).

An important tool in the study of Galois rings is their Gelfand–Kirillov dimension. It is used to construct examples of Galois rings in Section 6.

We emphasize that the theory of Galois orders unifies the representation theories of universal enveloping algebras and generalized Weyl algebras. On one hand the Gelfand–Tsetlin formulae give an embedding of $U(\mathfrak{gl}_n)$ into a certain localization of the Weyl algebra A_m for $m = n(n+1)/2$ (cf. Remark 7.1 and [Kh]). On the other hand the intrinsic reason for such unification is a similar hidden skew group ring structure of these algebras as Galois orders. We believe that the concept of a Galois order will have a strong impact on the representation theory of infinite dimensional associative algebras. We will discuss the representation theory of Galois rings in a subsequent paper (see [FO2]). Preliminary version of this paper appeared in the preprint form [FO].

2. Preliminaries

All fields in the paper contain the base field $\mathbb{k}$, which is algebraically closed of characteristic 0. All algebras in the paper are $\mathbb{k}$-algebras.

2.1. Integral extensions

Let A be an integral domain, K its field of fractions and $\tilde{A}$ the integral closure of A in K. Recall that the ring A is called *normal* if $A = \tilde{A}$. Let A be a normal noetherian ring, $K \subset L$ a finite Galois extension, $\bar{A}$ the integral closure of A in L.

Proposition 2.1.

- *If $\tilde{A}$ is noetherian then $\bar{A}$ is finite over $\tilde{A}$.*
- *If A is a finitely generated $\mathbb{k}$-algebra then $\bar{A}$ is finite over A. In particular, $\tilde{A}$ is finite over A.*

The following statement is probably well known but we include the proof for the convenience of the reader.

Proposition 2.2. *Let $i : A \hookrightarrow B$ be an embedding of integral domains with a regular A. Assume the induced morphism of varieties $i^* : \mathrm{Specm}\, B \to \mathrm{Specm}\, A$ is surjective (e.g. $A \subset B$ is an integral extension). If $b \in B$ and $ab \in A$ for some nonzero $a \in A$ then $b \in A$.*

Proof. In this case i induces an epimorphism of the $\mathrm{Spec}\, B$ onto $\mathrm{Spec}\, A$. Fix $\mathsf{m} \in \mathrm{Specm}\, A$. Assume $ab = a' \in A$. Since the localization A_{m} is a unique factorization domain, we can assume that $a_{\mathsf{m}} b = a'_{\mathsf{m}}$, where $a_{\mathsf{m}}, a'_{\mathsf{m}} \in A_{\mathsf{m}}$ are coprime. If a_{m} is invertible in A_{m} then $b \in A_{\mathsf{m}}$. If a_{m} is not invertible in A_{m} then there exists $P \in \mathrm{Spec}\, A_{\mathsf{m}}$ such that $a_{\mathsf{m}} \in P$ and $a'_{\mathsf{m}} \notin P$. It shows that P does not lift to $\mathrm{Spec}\, B_{\mathsf{m}}$. Hence $b \in A_{\mathsf{m}}$ for every $\mathsf{m} \in \mathrm{Specm}\, A$, which implies $b \in A$ (see [Mat], Theorem 4.7). $\square$

2.2. Skew monoid rings: notations and conventions

If a monoid $\mathcal{M}$ acts on a set S, $\mathcal{M} \times S \xrightarrow{\varphi} S$, then $\varphi(m, s)$ will be denoted either by $m \cdot s$, or ms, or s^m. In particular $s^{mm'} = (s^{m'})^m$, $m, m' \in \mathcal{M}$, $s \in S$. By $S^{\mathcal{M}}$ we denote the subset of all $\mathcal{M}$-invariant elements in S.

Besides in this paper we use the following notation. Let H be a group, action on a set X, X/H the set of orbits, $F(x)$ be an expression depending on $x \in X$, such that $F(x)$ is constant on the orbit. Then the notation $\sum_{x \in X/H} F(x)$ means that

$$\begin{gathered}\textit{the sum is taken over some set of representatives of the orbits,}\\ \textit{the sum does not depend on this choice due to equivariency of } F.\end{gathered} \tag{2.1}$$

Mostly we use this notation in the case where H is a subgroup in a finite group G and the sum $\sum_{x\in G/H} F(x)$ is taken over the set of left cosets (e.g., see (2.4)). The same agreement we use in the notation $\bigoplus_{x\in X/H}$.

Let R be a ring with a unit, $\mathcal{M}$ a monoid and $f : \mathcal{M} \to \operatorname{Aut}(R)$ a homomorphism. Then $\mathcal{M}$ acts naturally on R (from the left): $g \cdot r = f(g)(r)$ for $g \in \mathcal{M}$, $r \in R$. The *skew monoid ring* of R and $\mathcal{M}$, $R * \mathcal{M}$, associated with the left action of $\mathcal{M}$ on R, is a free left R-module, $\bigoplus_{m\in\mathcal{M}} Rm$, with a basis $\mathcal{M}$ and with the multiplication defined as follows

$$(r_1m_1)\cdot(r_2m_2) = \left(r_1r_2^{m_1}\right)(m_1m_2), \quad m_1, m_2 \in \mathcal{M},\ r_1, r_2 \in R.$$

Assume that a finite group G acts on R by automorphisms and on $\mathcal{M}$ by conjugation. Define a map

$$G \times (R * \mathcal{M}) \longrightarrow R * \mathcal{M}, \quad (g, rm) \longmapsto r^g m^g,\ r \in R,\ m \in \mathcal{M},\ g \in G. \tag{2.2}$$

This map defines an action of G on $R * \mathcal{M}$ by automorphisms. Denote by $(R * \mathcal{M})^G$ the subring of G-invariant elements in $R * \mathcal{M}$.

Any $x \in R * \mathcal{M}$ can be written in the form $x = \sum_{m\in\mathcal{M}} x_m m$, where only finitely many $x_m \in R$ are nonzero. We call the finite set

$$\operatorname{supp} x = \{m \in \mathcal{M} \mid x_m \neq 0\}$$

the *support* of x. For $\varphi \in \mathcal{M}$ denote its G-stabilizer and G-orbit by

$$H_\varphi = \left\{h \in G \,\middle|\, \varphi^h = \varphi\right\}, \qquad \mathcal{O}_\varphi = \left\{\varphi^g \,\middle|\, g \in G\right\}, \tag{2.3}$$

respectively.

Denote by $\mathcal{K}$ the subring of G-invariants $(R * \mathcal{M})^G \subset R * \mathcal{M}$.

Lemma 2.1. *In the assumption above holds the following.*

(1) *$x \in R * \mathcal{M}$ is G-invariant if and only if $x_{m^g} = x_m^g$ for all $m \in \mathcal{M}$, $g \in G$. In this case* $\operatorname{supp} x \subset \mathcal{M}$ *is a finite G-invariant set.*

(2) *Let $\varphi \in \mathcal{M}$, $a \in R^{H_\varphi}$. Then the element of $R * \mathcal{M}$,*

$$[a\varphi] := \sum_{g\in G/H_\varphi} a^g \varphi^g \in \mathcal{K}, \tag{2.4}$$

defined following (2.1)*, is G-invariant.*

(3) *Let $\varphi \in \mathcal{M}$. Then the set*

$$\mathcal{K}_\varphi = \left\{[a\varphi] \,\middle|\, a \in R^{H_\varphi}\right\}$$

is an R^{H_φ}-bimodule (*hence R^G-bimodule*)*, where R^{H_φ} acts on $\mathcal{K}_\varphi$ by left and right multiplication in $R * \mathcal{M}$,*

$$\gamma \cdot [a\varphi] = \left[(a\gamma)\varphi\right], \qquad [a\varphi]\cdot\gamma = \left[\left(a\gamma^\varphi\right)\varphi\right], \quad \gamma \in R^{H_\varphi}.$$

(4) *As an R^G-bimodule*

$$\mathcal{K} = \bigoplus_{\varphi\in\mathcal{M}/G} \mathcal{K}_\varphi.$$

In particular, every $x \in \mathcal{K}$ has the unique presentation

$$\sum_{\varphi\in\mathcal{M}/G} [x_\varphi \varphi], \quad x_\varphi \in R^{H_\varphi} \setminus \{0\},$$

where $\mathcal{M}/G$ denotes the set of orbits of the action G on $\mathcal{M}$ by conjugations.

Proof. The statement (1) is obvious. To prove (2), note that by definition $a^g\varphi^g$ depends only on left coset gH_φ. Then for $g' \in G$ holds $([a\varphi])^{g'} = \sum_{g\in G/H_\varphi} a^{g'g}\varphi^{g'g}$. In this sum $g'g$ runs a set of representatives cosets G/H_φ, hence $([a\varphi])^{g'} = [a\varphi]$.

In (3) is enough to prove, that $a\gamma, a\gamma^\varphi \in R^{H_\varphi}$. The first is obvious. Then for $h \in H_\varphi$ holds $h\cdot\gamma^\varphi = h\varphi\gamma = (h\varphi h^{-1})(h\gamma) = \gamma^\varphi$. The statement (4) is proved by the induction in $|\operatorname{supp} x|$. $\square$

Analogously, for $a, b \in R^{H_\varphi}$ we can denote

$$[a\varphi b] = \sum_{g\in G/H_\varphi} a^g\varphi^g b^g, \quad \text{in particular} \quad [a\varphi] = \left[\varphi a^{\varphi^{-1}}\right], \tag{2.5}$$

with the properties, analogous to Lemma 2.1.

2.3. *Separating actions*

Let in assumption of Section 2.2 $R = L$ be a field, $K \subset L$ a finite Galois extension of fields, $G = G(L/K)$ the Galois group and $\imath$ the canonical embedding $K \hookrightarrow L$. Then $K = L^G$ and

$$\dim^r_K \mathcal{K}_\varphi = \dim^l_K \mathcal{K}_\varphi = \left[L^{H_\varphi} : K\right] = |G : H_\varphi| = |\mathcal{O}_\varphi|, \tag{2.6}$$

where $\dim^r_K$, $\dim^l_K$ are right and left K-dimensions.

Definition 1.

(1) A monoid $\mathcal{M} \subset \operatorname{Aut} L$ is called *separating* (with respect to K) if for any $m_1, m_2 \in \mathcal{M}$ the equality $m_1|_K = m_2|_K$ implies $m_1 = m_2$.
(2) An automorphism $\varphi : L \to L$ is called *separating* (with respect to K) if the monoid generated by $\{\varphi^g \mid g \in G\}$ in $\operatorname{Aut} L$ is separating.

Lemma 2.2. *Let monoid $\mathcal{M}$ be separating with respect to K. Then*:

(1) $\mathcal{M} \cap G = \{e\}$.
(2) *For any $m \in \mathcal{M}$, $m \neq e$ there exists $\gamma \in K$ such that $\gamma^m \neq \gamma$.*
(3) *If $Gm_1G = Gm_2G$ for some $m_1, m_2 \in \mathcal{M}$, then there exists $g \in G$ such that $m_1 = m_2^g$.*
(4) *If $\mathcal{M}$ is a group, then the statements* (1), (2), (3) *are equivalent and each of them implies that $\mathcal{M}$ is separating.*

Proof. We prove the statement (3), other statements are trivial. $Gm_1G = Gm_2G$ if and only if for some $g, g' \in G$ holds $m_1^g = m_2g'$. Then m_1^g and m_2 acts in the same way on K, hence $m_1^g = m_2$. □

Let $\jmath : K \hookrightarrow L$ be an embedding. Denote $\mathrm{St}(\jmath) = \{g \in G \mid g\jmath = \jmath\}$.

Lemma 2.3. *Let $\varphi \in \mathcal{M}$, $\jmath = \varphi\imath$. Then:*

(1) *If φ is separating, then $H_\varphi = \mathrm{St}(\jmath)$.*
(2) *$K\varphi(K) = L^{\mathrm{St}(\jmath)}$, in particular, $K\varphi(K) = L^{H_\varphi}$ if φ is separating.*

Proof. If $g \in H_\varphi$ then applying $\imath$ to the equality $g\varphi = \varphi g$ we obtain $H_\varphi \subset \mathrm{St}(\jmath)$. Conversely, if $g\varphi\imath = \varphi\imath$, then $\varphi^{-1}g\varphi\imath = \imath$, hence $\varphi^{-1}g\varphi = g_1 \in G$ and $\varphi^{-1}(g\varphi g^{-1}) = g_1g^{-1}$. Thus φ and $g\varphi g^{-1}$ coincide on K, implying $g\varphi g^{-1} = \varphi$ and (1). Note that $g \in G(L/K\varphi(K)) \cap G$ if and only if $g|_{\varphi(K)} = \mathrm{id}$ (i.e. $g \in \mathrm{St}(\jmath)$), implying (2). □

3. Bimodules

3.1. Balanced bimodules

For commutative $\Bbbk$-algebras A and B we will denote by $(A - B)$-bimod the category of finitely generated $A - B$-bimodules. If $A = B$ we will simply write A-bimod.

Proposition 3.1. *Let $K \subset L$ be a finite field extension. The full subcategories of K-*bimod*, $(K - L)$-*bimod *or $(L - K)$-*bimod *consisting of objects, which are finite dimensional as left or as right modules are Jordan–Hoelder and Krull–Schmidt categories.*

Proof. It follows from the finiteness of the length of the objects of these categories. □

In this section all bimodules over fields are assumed to be finite dimensional from both sides and $\Bbbk$-central (*unless the contrary is stated*). A homomorphism of algebras $\varphi : A \to B$ naturally endows B with the structure of $B - A$-bimodule B_φ such that for $a \in A$, $b \in B$, $b' \in B_\varphi$ holds $b \cdot b' \cdot a = bb'\varphi(a)$.

Remark 3.1.

(1) In opposite, a $B - A$-bimodule V, which is free of rank 1 from the left, defines a homomorphism $\varphi = \varphi_V : A \to B$ by $va = \varphi(a)v$, where $v \in V$ is a right free generator of V.
(2) If $\varphi : A \to B$ and $\psi : B \to C$ are homomorphisms of algebras then there exists an isomorphism of $C - A$-bimodules

$$C_\psi \otimes_B B_\varphi \simeq C_{\psi\varphi}, \quad c \otimes b \longmapsto c\psi(b), \quad c \in C,\ b \in B.$$

Let $K \subset L$ be an extension and $\imath_K$ the canonical embedding $K \subset L$. We will write $\imath$ instead of $\imath_K$ when the field K is fixed. If $V = {}_KV_K$ is a K-bimodule then denote ${}_KV_L = V \otimes_K L$, ${}_LV_K = L \otimes_K V$ and ${}_LV_L = L \otimes_K {}_KV_L$.

Let $K \subset L$ is a Galois extension with the Galois group $G = G(L/K)$, then the group $G \times G$ acts on ${}_LV_L$ as

$$(g_1, g_2) \cdot (l_1 \otimes v \otimes l_2) \longmapsto l_1^{g_1} \otimes v \otimes l_2^{g_2^{-1}}, \quad (g_1, g_2) \in G \times G,\ v \in V,\ l_1, l_2 \in L,$$

by automorphism of K-bimodules. The K-bimodule of invariants is canonically isomorphic to V. If we restrict the action of $G \times G$ to the action of G from the left (from the right), by automorphisms of $K - L$ $(L - K)$ bimodules, then the invariants will be ${}_KV_L$ $({}_LV_K)$.

Analogously, G acts naturally from the left on the $L-K$-bimodule ${}_LV_K$ by automorphisms of K-bimodule,

$$g \cdot (l \otimes v) \longmapsto l^g \otimes v, \quad g \in G,\ v \in V,\ l \in L \quad \text{and} \quad ({}_LV_K)^G \simeq {}_KV_K.$$

Assume that the right action of K on V is L-diagonalizable from the left. It means ${}_LV_K$ splits into a sum of $L-K$-bimodules, which are one-dimensional as right L-modules. By Remark 3.1, (1) such one-dimensional $L-K$-bimodule is of the form $L_\jmath$ for some field embedding $\jmath : K \to L$.

Definition 2. A K-bimodule ${}_KV_K$ is called *L-balanced* over a finite Galois extension $K \subset L$ if ${}_LV_L$ is a direct sum of one-dimensional from the left and from the right L-bimodules, i.e. bimodules of the form L_φ for $\varphi \in \operatorname{Aut} L$. A K-bimodule ${}_KV_K$ is called *balanced* if it is *L-balanced* over some finite Galois extension $K \subset L$.

3.2. Monoidal category of balanced bimodules

Denote by $K\text{-}\operatorname{bimod}_L$ the full subcategory in $K\text{-}\operatorname{bimod}$ consisting of all L-balanced K-bimodules.

Remark 3.2. The category $L\text{-}\operatorname{bimod}_L$ is by definition semisimple and its isoclasses of simples are represented by the bimodules L_φ, were $\varphi : L \to L$ is an automorphism.

Theorem 3.1. *The category $K\text{-}\operatorname{bimod}_L$ is an abelian semisimple monoidal category.*

Proof. Note that by Remarks 3.1, (2) and by Remark 3.2 above the category $L\text{-}\operatorname{bimod}_L$ satisfies the theorem.

Let V, W be L-balanced K-bimodules, $p : V \to W$ a K-bimodule epimorphism, $p_L : {}_LV_L \to {}_LW_L$ the induced epimorphism of L-bimodules. Since G acts trivially on K the map p_L is a homomorphism of $(K \otimes_{\Bbbk} K)[G \times G]$-bimodules.

On the other hand p_L admits the right inverse $L-L$-bimodule monomorphism

$$s_L : {}_LW_L \longrightarrow {}_LV_L, \quad p_Ls_L = \mathrm{id}_{{}_LW_L}.$$

Since G acts trivially on K for every $g = (g_1, g_2) \in G \times G$ the morphisms

$$gs_Lg^{-1} : {}_LW_L \longrightarrow {}_LV_L, \quad l_1 \otimes w \otimes l_2 \longmapsto g_1 \cdot s_L\big(l_1^{g_1^{-1}} \otimes w \otimes l_2^{g_2}\big) \cdot g_2^{-1}$$

are K-bimodule homomorphisms. Then the K-bimodule homomorphism

$$\sigma_L = \frac{1}{|G|^2} \sum_{g \in G \times G} gs_Lg^{-1}$$

commutes with the action $G \times G$, hence both σ_L and p_L are $(K \otimes_{\Bbbk} K)[G \times G]$-bimodule homomorphisms. We have

$$p_L\sigma_L = \frac{1}{|G|^2} \sum_{g \in G \times G} p_Lgs_Lg^{-1} = \frac{1}{|G|^2} \sum_{g \in G \times G} gp_Ls_Lg^{-1} = \mathrm{id}_{{}_LW_L}.$$

Since σ_L maps ${}_LW_L^{G \times G}$ to ${}_LV_L{}^{G \times G}$, it induces a K-bimodule homomorphism $\sigma : W \to V$, which splits p. Hence $K\text{-}\operatorname{bimod}_L$ is semisimple.

Consider the standard K-bimodule monomorphism

$$i : V \otimes_K W \longrightarrow V \otimes_K L \otimes_K W, \quad v \otimes w \longmapsto v \otimes 1 \otimes w.$$

Then the induced L-bimodule homomorphism

$$i_L :_L (V \otimes_K W)_L \longrightarrow L \otimes_K V \otimes_K L \otimes_K W \otimes_K L \simeq {}_L V_L \otimes_L {}_L W_L$$

is a monomorphism. Since ${}_L V_L$ and ${}_L W_L$ are isomorphic to the sums of simple one-dimensional L-bimodules, the same is true for their tensor product over L and for its subbimodule $i_L({}_L(V \otimes_K W)_L)$. The unit with respect to $\otimes_K$ in $K\text{-}\mathrm{bimod}_L$ is K. $\square$

3.3. Simple balanced bimodules

In this section we describe all simple objects in $K\text{-}\mathrm{bimod}_L$.

Lemma 3.1. *Let $K \subset L$ be a Galois extension, $G = G(L/K)$.*

(1) ([DK], *Ch.* 5.1) *If for a field F holds $K \subset F \subset L$, $H = G(L/F)$ and $i_F : F \hookrightarrow L$ is the canonical embedding, then as $L - F$-bimodule*

$$L \otimes_K F \simeq \bigoplus_{g \in G/H} L_{g i_F}, \quad \textit{in particular} \quad L \otimes_K L \simeq \bigoplus_{g \in G} L_g.$$

(2) *A K-bimodule V is L-balanced if and only if the $L - K$-bimodule ${}_L V_K$ is a direct sum of modules of the form $L_{\varphi\imath}$, $\varphi \in \mathrm{Aut}\, L$.*

(3) *Let $\varphi, \varphi' \in \mathrm{Aut}\, L$, $\jmath = \varphi\imath$, $\jmath' = \varphi'\imath$. Then the $L - K$-bimodules L_φ and $L_{\varphi'}$ are isomorphic if and only if* $\mathrm{St}(\varphi)$ *and* $\mathrm{St}(\varphi')$ *are G-conjugate, equivalently $\varphi^{-1}\varphi' \in G$.*

(4) *The right and the left K-dimensions of a balanced bimodule coincide.*

Proof. To prove the statement (1) we present F as a simple extension $F = K[\alpha]$, $\alpha \in F$. Let $f(X)$ be a minimal polynomial of α over K, $\alpha = \alpha_1, \dots, \alpha_k \in L$ all roots of $f(X)$. Then $F \simeq K[X]/(f(X))$ and

$$L \otimes_K F \simeq L \otimes_K K[X]/\bigl(f(X)\bigr) \simeq L[X]/\bigl(f(X)\bigr) \simeq \prod_{i=1}^{k} L[X]/(X - \alpha_i).$$

The right F-module structure on $L[X]/(X - \alpha_i)$ is defined by multiplication on X, that proves (1).

To show (2) we prove first the implication “if”. Applying Remark 3.1, (2) we obtain the following chain of isomorphisms of L-bimodules, which implies the statement

$$L_{\varphi\imath} \otimes_K L \simeq (L_\varphi \otimes_L L_\imath) \otimes_K L \simeq L_\varphi \otimes_L (L \otimes_K L)$$
$$\simeq L_\varphi \otimes_L \left(\bigoplus_{g \in G} L_g \right) \simeq \bigoplus_{g \in G} L_{\varphi g}.$$

Now we prove the “only if” part. If ${}_L V_L \simeq \bigoplus_{\varphi \in S} L_\varphi^{d_\varphi}$, $S \subset \mathrm{Aut}\, L$, $d_\varphi > 0$ as L-bimodule, then as $L - K$-bimodule it is isomorphic to $\bigoplus_{\varphi \in S} L_{\varphi\imath}^{d_\varphi}$. In particular, ${}_L V_L$ is a semisimple $L - K$-bimodule. Note, that ${}_L V_K$ can be identified with $({}_L V_L)^{\{e\} \times G}$, which is an $L - K$-submodule in ${}_L V_L$. Hence ${}_L V_K$ as a subbimodule of the semisimple $L - K$-bimodule ${}_L V_L$ is a direct sum of some $L_{\varphi\imath}$, $\varphi \in S$.

Let $f : L_\varphi \simeq L_{\varphi'}$ be an isomorphism of $L-K$-bimodules. Since L_φ is free from the left, then as a left module homomorphism f is uniquely defined by the image of the unit: $f(1) = x \in L_{\varphi'}$. The condition of a bimodule homomorphism $f(l \cdot l' \cdot k) = l \cdot f(l') \cdot k$, $l \in L$, $l' \in L_\varphi$, $k \in K$, gives us $(l\varphi(k))l'x = l\varphi'(k)(l'x)$. It implies that the automorphisms φ and φ' coincide on K, that is $\varphi^{-1}\varphi' \in G$, proving (3).

The statement (4) follows from

$$\dim^l_{K\ L} V_L = \dim^l_{K\ L} V_K [L : K] = \dim^l_{K\ K} V_K [L : K]^2$$

and analogous equalities for $\dim^r_{K\ L} V_L$. $\square$

Lemma 3.2. *Let $\varphi \in \operatorname{Aut} L$, $\jmath = \varphi\imath$, $H = \operatorname{St}(\jmath)$.*

(1) *The canonical action of H on L defines an action by $L^H - K$-bimodule automorphisms on L-bimodule L_φ and on $L - K$-bimodule $L_\jmath$.*
(2) *Let $j : K \to L^H$ be the induced by $\jmath$ embedding, $V(\varphi) = L^H_\jmath$. Then $V(\varphi)$ is a simple $L^H - K$-subbimodule in L_φ.*

Proof. Note that the structure of $L - K$-bimodule on $L_\jmath$ is just the restriction of $L - L$-bimodule structure on L_φ to the action of L from the left and K from the right. It allows in (1) consider only the case of L_φ. Let $l \in L_\varphi$, $l_1 \in L^H$, $k \in K$ and "$\cdot$" is the bimodule action on L_φ. Then for $h \in H$ holds

$$d\ (l_1 \cdot l \cdot k)^h = \big(l_1 l \varphi(k)\big)^h = l_1^h l^h h\varphi(k) = l_1 l^h \varphi(k) = l_1 \cdot l^h \cdot k,$$

which proves the statement (1).

Further, (1) implies that $V(\varphi)$ (as the set of the fixed elements of the action of H) is an $L^H - K$-bimodule. The simplicity of $V(\varphi)$ is obvious. $\square$

Since $K \subset L^H$ (Lemma 3.2, (2)), $L^H - K$-bimodule structure induces on $V(\varphi)$ the structure of a K-bimodule. It turns out, that the set $V(\varphi)$, $\varphi \in \operatorname{Aut} L$ exhausts all simples in $K\text{-}\operatorname{bimod}_L$. Namely, we have the following result.

Theorem 3.2.

(1) *Let $\varphi \in \operatorname{Aut} L$. Then $L \otimes_K V(\varphi) \simeq \bigoplus_{g \in G/H} L_{g\varphi\imath}$ as an $L - K$-bimodule, that is $V(\varphi)$ is L-balanced.*
(2) *$V(\varphi)$ is a simple K-bimodule.*
(3) *Any simple object in $K\text{-}\operatorname{bimod}_L$ is isomorphic to $V(\varphi)$ for some $\varphi \in \operatorname{Aut} L$.*
(4) *Let $\varphi, \varphi' \in \operatorname{Aut} L$. Then $V(\varphi) \simeq V(\varphi')$ if and only if one from the following holds*:
 (a) *$G\varphi|_K = G\varphi'|_K$.*
 (b) *$G\varphi G = G\varphi' G$.*
 (c) *If φ is separating, then $\varphi' = \varphi^g$ for some $g \in G$.*
(5) *Let $\varphi \in \operatorname{Aut} L$ be separating, $a \in L^{H_\varphi}$, $v = [a\varphi] \in \mathcal{K}$, (2.4). Then $KvK \simeq V(\varphi)$ as K-bimodule.*

Proof. As above denote $\jmath = \varphi\imath$, $H = \operatorname{St}(\jmath)$. Consider $V(\varphi)$ as K-bimodule. Using Lemma 3.1, (1) and Remark 3.1, (2) we obtain the following isomorphisms of $L - K$-bimodules.

$$\begin{aligned} L \otimes_K V(\varphi) &= L \otimes_K L^H_\jmath \simeq L \otimes_K \big(L^H \otimes_{L^H} L^H_\jmath\big) \simeq \big(L \otimes_K L^H\big) \otimes_{L^H} L^H_\jmath \\ &\simeq \Big(\bigoplus_{g \in G/H} L_g\Big) \otimes_{L^H} L^H_\jmath \simeq \bigoplus_{g \in G/H} \big(L_g \otimes_{L^H} L^H_\jmath\big) \simeq \bigoplus_{g \in G/H} L_{g\jmath}, \end{aligned}$$

which, together with Lemma 3.1, (2), proves (1). To prove the simplicity of $V(\varphi)$ consider any nonzero $x \in L^H$. Then $K \cdot x \cdot K = \varphi(K)K = L^H x$, implying (2).

Now we prove (3). Let V be a simple L-balanced K-bimodule. We divide the proof into the following steps. If A is a $\Bbbk$-algebra, then in the proofs below instead of the structure of $A - K$-bimodule we will use the corresponding structure of left $A \otimes_{\Bbbk} K$-module.

Step 1. The equality $(l'g \otimes k) \cdot (l \otimes v) = l'l^g \otimes kv$, $k \in K$, $g \in G$, $l, l' \in L$, $v \in V$, endows ${}_L V_K$ with the structure of a simple left $(L * G) \otimes_{\Bbbk} K$-module.

The correctness of $(L * G) \otimes_{\Bbbk} K$-module structure is checked immediately. To prove the simplicity consider $0 \neq x \in {}_L V_K$, $x = \sum_{g \in G} l_g \otimes v_g$, where $v_g \in V$, $g \in G$ and $\{l_g \mid l \in L,\ g \in G\}$ is a normal K-basis of L. Consider $g' \in G$ such that $v_{g'} \neq 0$. By the theorem of independence of characters the maps $w_g : G \to L$, $w_g(g_1) = l_{gg_1}$, $g, g_1 \in G$, form a basis in the L-vector space of maps $G \to L$. Hence there exist $\sum_{g \in G} \lambda_g g \in L * G$, such that

$$\left(\sum_{g \in G} \lambda_g g\right) \cdot x = \sum_{g \in G} \left(\sum_{g_1 \in G} \lambda_{g_1} l_{gg_1}\right) \otimes v_g = 1 \otimes v_{g'}.$$

Since v' generates V as K-bimodule, obviously $1 \otimes v_{g'}$ generates ${}_L V_K$ as $L - K$-bimodule.

Step 2. ${}_L V_K \simeq \bigoplus_{g \in G/H} L_{g\jmath}^d$ for some $d \geqslant 1$, where $\jmath = \varphi\imath$ for some $\varphi \in \operatorname{Aut} L$, $H = \operatorname{St}(\jmath)$. Besides every $L_{g\jmath}$ is a simple $(L * H) \otimes_{\Bbbk} K$-submodule in ${}_L V_K$.

By Lemma 3.1, (2), ${}_L V_K \simeq \bigoplus_{\jmath \in S} L_{\jmath}^{d_\jmath}$ as an $L - K$-module for pairwise nonisomorphic $L_\jmath$. Let $S = \bigsqcup_{i=1}^k O_i$, where O_i's are the orbit of the action of G on S from the left and $H_i = \operatorname{St}(\jmath_i)$ for some $\jmath_i \in O_i$. Then by Lemma 3.1, (3) and since $g(L_\jmath) \simeq L_{g\jmath}$ we have

$${}_L V_K \simeq \bigoplus_{i=1}^k \left(\bigoplus_{g \in G/H_i} L_{g\jmath}^d\right) \quad \text{and} \quad {}_K V_K \simeq ({}_L V_K)^G \simeq \bigoplus_{i=1}^k \left(\bigoplus_{g \in G/H_i} L_{g\jmath}^d\right)^G$$

which is a splitting of ${}_K V_K$ in a sum of $K - K$-subbimodules. Since ${}_K V_K$ is simple as $K - K$-bimodule, we have $k = 1$ and ${}_L V_K \simeq \bigoplus_{g \in G/H} L_{g\jmath}^d$ as an $L - K$-bimodule. The $L - K$-subbimodule $L_{g\jmath}$ of ${}_L V_K$ is H-invariant, hence it is an $(L * H) \otimes_K K$-module, where $H = \operatorname{St}(g\jmath)$. Besides, $L_{g\jmath}$ is simple even as $L - K$-bimodule.

Step 3. $d = 1$.

Note that $(L * G) \otimes_{\Bbbk} K$ is a free right $(L * H) \otimes_{\Bbbk} K$-module of rank $[G : H]$. The canonical embedding of $(L * H) \otimes_{\Bbbk} K$-modules $L_\jmath \hookrightarrow {}_L V_K$ induces a homomorphism of $(L * G) \otimes_{\Bbbk} K$-modules

$$\Phi : (L * G) \otimes_{L*H} L_\jmath \longrightarrow {}_L V_K,$$

which is an epimorphism, since $\Phi \neq 0$ and ${}_L V_K$ is simple. On the other hand for the left K-dimensions $\dim_K^l$ holds

$$\dim_K^l (L * G \otimes_{L*H} L_\jmath) = [L : K][G : H], \qquad \dim_K^l {}_L V_K = d[L : K][G : H].$$

Hence, $d = 1$ and Φ is an isomorphism.

Step 4. The mapping

$$\psi : K[G] \times L_j \longrightarrow (L * G) \otimes_{L*H} L_J, \quad (kg, l) \longmapsto kg \otimes l,\ k \in K,\ g \in G,\ l \in L_j,$$

induces an isomorphism of left $K[G] \otimes_{\Bbbk} K$-modules

$$\Psi : K[G] \otimes_{K[H]} L_j \longrightarrow (L * G) \otimes_{L*H} L_J.$$

Indeed, ψ is $K[H]$-bilinear and commutes with the action of $K[G]$ from the left and with the action of K from the right. Again a comparison of K-dimensions implies the statement.

Step 5. $V \simeq V(\varphi)$.

Steps 3 and 4 shows, that the composition

$$\Phi \circ \Psi : K[G] \otimes_{K[H]} L_J \longrightarrow {}_L V_K$$

is an isomorphism of $K[G] \otimes_{\Bbbk} K$-modules. By the Frobenius reciprocity for left $K[H]$-module L_J we obtain the chain of K-bimodule isomorphisms

$$\begin{aligned} V &\simeq ({}_L V_K)^G \simeq \big(K[G] \otimes_{K[H]} L_J\big)^G \simeq \mathrm{Hom}_{K[G]}\big(K, K[G] \otimes_{K[H]} L_J\big) \\ &\simeq \mathrm{Hom}_{K[G]}\big(K, \mathrm{Hom}_{K[H]}\big(K[G], L_J\big)\big) \simeq \mathrm{Hom}_{K[H]}\big(K[G] \otimes_{K[G]} K, L_J\big) \simeq \mathrm{Hom}_{K[H]}(K, L_J) \simeq L_J^H. \end{aligned}$$

It proves the statement (3).

Assume $V(\varphi) \simeq V(\varphi')$ and $H' = \mathrm{St}(\varphi'\imath)$. Then $L \otimes_K V(\varphi) \simeq L \otimes_K V(\varphi')$ as $L-K$-bimodules. By Step 3 above and Lemma 3.1, (3), there exists $g, g' \in G$, such that $\varphi^{-1}(g'\varphi') = g$ or $g'\varphi' = \varphi g$. Thus $G\varphi\imath = G\varphi'\imath$, $G\varphi|_K = G\varphi'|_K$ and $G\varphi G = G\varphi' G$. The statement on separating φ follows from Lemma 2.2. The converse statement easily follows.

It remains to prove (5). Using (2.5) and Lemma 2.3, (2) we obtain

$$K[a\varphi]K = \big[K\varphi(K)a\varphi\big] = \big[L^H a\varphi\big],$$

which immediately implies the isomorphism $[L^H a\varphi] \simeq V(\varphi)$ and hence the last statement. □

3.4. Grotendieck ring of the category of balanced bimodules and Hecke algebra

Let $K_0(K, L)$ be the Grothendieck ring of $K\text{-}\mathrm{bimod}_L$ and for $V \in K\text{-}\mathrm{bimod}_L$ $[V]$ the class of V in $K_0(K, L)$. Theorem 3.2 shows that simple L-balanced K-bimodules in $K\text{-}\mathrm{bimod}_L$ can be enumerated by the double cosets $G\varphi G$ or by the G-orbits $G\varphi\imath$. We show that the ring structure on $K_0(K, L)$ is closely related to some Hecke algebra (Corollary 3.3).

To calculate in $K_0(K, L)$ we need some preliminaries. A *family of elements* S of a set T is a mapping $S : \mathcal{I} \to T$, where $\mathcal{I}$ in the set of indices. If the group G acts on $\mathcal{I}$ and T, then we say S is G-invariant provided that S is a map of G-sets. To simplify the notation we will write i instead of $S(i)$, $i \in \mathcal{I}$. By S/G we denote the induced map of factor sets $S/G : \mathcal{I}/G \to T/G$. In particular, S/G is a family of elements of T/G, indexed by $\mathcal{I}/G$.

For $\varphi \in \mathrm{Aut}\, L$ set $S_\varphi = \mathrm{St}(\varphi\imath)$, where $\imath : K \hookrightarrow L$ is the canonical embedding.

Denote $\mathrm{Hom}_{\Bbbk-f}(K, L)$ the set of all field $\Bbbk$-embeddings $K \to L$, and

$$\mathcal{B}(K, L) = \big\{S \bigm| S\colon \mathcal{I} \to \mathrm{Hom}_{\Bbbk-f}(K, L),\ \ |\mathcal{I}| < \infty,\ gS = S\big\}.$$

Then by Lemma 3.1, (2) we can correspond to a finitely generated balanced K-bimodule V a G-invariant family $S_V : \mathcal{I}_V \to \mathrm{Hom}_{\Bbbk}(K, L)$, such that ${}_L V_K \simeq \bigoplus_{\tau \in \mathcal{I}_V} L_{S_V(\tau)}$. The factorization by G induces the family

$$s_V = S_V/G : \mathcal{I}_V/G \longrightarrow \mathcal{B}(K, L) = \mathrm{Hom}_{\Bbbk - f}(K, L)/G.$$

Obviously, the image of s_V defines the K-bimodule V uniquely up to an isomorphism and we can write ${}_L V_K \simeq \bigoplus_{\tau \in \mathcal{I}_V/G} L_{s_V(\tau)}$.

In particular, by Theorem 3.2 (1), we can choose $\mathcal{I}_{V(\varphi)}$ to be the set G/S_φ, $S_V(gS_\varphi) = g\varphi$. Then $\mathcal{I}_{V(\varphi)}/G$ is a one-element set and the image of s_V is the subset $\{g\varphi \mid g \in G/S_\varphi\}$. On the other hand, any double coset $C = G\varphi G \in G\backslash \mathrm{Aut}\, L/G$ defines an element

$$b_C = b_\varphi = \sum_{\psi \in C} \psi = \sum_{g \in G/S_\varphi} \sum_{\tau \in g\varphi G} \tau \in \mathbb{Q}[\mathrm{Aut}\, L].$$

If $x = \sum_{\varphi \in G\backslash \mathrm{Aut}\, L/G} n_\varphi b_\varphi \in \mathbb{Q}[\mathrm{Aut}\, L]$, $n_\varphi \in \mathbb{N}$, then one defines

$$V(x) = \bigoplus_{\varphi \in G\backslash \mathrm{Aut}\, L/G} V(\varphi)^{n_\varphi}.$$

In particular, $V(b_\varphi) \simeq V(\varphi)$.

Corollary 3.1. *Let V be an object of K-bimod_L, $V \simeq \bigoplus_{\tau \in \mathcal{I}_V/G} V(S_V(\tau))$.*

(1) *For $\varphi \in \mathrm{Aut}\, L$ the multiplicity n_φ of $V(\varphi)$ in V is given by the formula*

$$n_\varphi = \sum_{\tau \in \mathcal{I}_V,\, S_V(\tau) = \varphi\imath} \frac{|S_\varphi|}{|G|}.$$

(2) $[V] = \sum_{\tau \in \mathcal{I}_V} \frac{|\mathrm{St}(S_V(\tau))|}{|G|} [V(S_V(\tau))]$.

Proof. The statement (2) follows from (1). The statement (1) follows from Theorem 3.2, (1). □

Recall, if G_1 is a group, $G \subset G_1$ is a finite subgroup and A is a commutative ring, then the Hecke algebra $\mathcal{H}_A(G_1; G) \subset A[G_1]$ is a free module over A with a basis $h_{G\varphi G}$ labeled by double cosets in $G\backslash G_1/G$. For details on Hecke algebras we refer to [Kr]. We will need the following result from [Kr] (Theorem 1.6.6) slightly adapted to our conditions.

Theorem 3.3. *Let $\Omega = \mathrm{Aut}\, L$. Then*:

(1) $e_G = \frac{1}{|G|} \sum_{g \in G} g$ *is an idempotent in the group algebra* $\mathbb{Q}[\Omega]$.
(2) *One has* $e_G \varphi e_G = \frac{|S_\varphi|}{|G|^2} b_\varphi$ *for all* $\varphi \in \Omega$ *and* $e_G \mathbb{Q}[\Omega] e_G$ *becomes a subalgebra of* $\mathbb{Q}[\Omega]$ *with* e_G *as its identity element.*
(3) *The mapping* $\Phi : \mathcal{H}_{\mathbb{Q}}(\Omega; G) \to e_G \mathbb{Q}[\Omega] e_G \subset \mathbb{Q}[\Omega]$, *where*

$$\sum_{\varphi \in G\backslash \Omega/G} n_\varphi h_{G\varphi G} \longmapsto \frac{1}{|G|} \sum_{\varphi \in G\backslash \Omega/G} n_\varphi b_\varphi$$

is an isomorphism of $\mathbb{Q}$*-algebras.*

We will identify the Hecke algebra $\mathcal{H}_{\mathbb{Q}}(\Omega; G)$ with $\operatorname{Im}(\Phi) \subset \mathbb{Q}[\Omega]$. Given $\varphi, \psi \in \operatorname{Aut} L$, introduce an equivalence relation $\sim$ ($= \sim(\varphi, \psi)$) on G as follows:

$$g \sim g' \quad \text{if and only if} \quad G\varphi g\psi G = G\varphi g'\psi G.$$

Theorem 3.4. *Let $\varphi, \psi \in \operatorname{Aut} L$. Then*

$$V(\varphi) \otimes_K V(\psi) \simeq \bigoplus_{c_g \in G/\sim} V(\varphi g\psi)^{s^g_{\varphi\psi}|c_g|},$$

where c_g is the equivalence class of g, $|c_g|$ its size and $s^g_{\varphi\psi} = \frac{|S_{\varphi g\psi}|}{|S_\varphi||S_\psi|}$.

Proof. Let $\varphi, \psi \in \operatorname{Aut} L$. Then by Theorem 3.2, (1) and Remark 3.1, (2)

$$\begin{aligned} L \otimes_K V(\varphi) \otimes_K V(\psi) &\simeq \bigoplus_{g \in G/S_\varphi} L_{g\varphi\iota} \otimes_K V(\psi) \\ &\simeq \bigoplus_{g \in G/S_\varphi} (L_{g\varphi} \otimes_L L) \otimes_K V(\psi) \simeq \bigoplus_{g \in G/S_\varphi} L_{g\varphi} \otimes_L \big(L \otimes_K V(\psi)\big) \\ &\simeq \bigoplus_{g \in G/S_\varphi} \bigoplus_{g' \in G/S_\psi} L_{g\varphi} \otimes_L L_{g'\psi\iota} \simeq \bigoplus_{g \in G/S_\varphi} \bigoplus_{g' \in G/S_\psi} L_{g\varphi g'\psi\iota}. \end{aligned}$$

Then by Corollary 3.1

$$\big[V(\varphi) \otimes_K V(\psi)\big] = \sum_{\substack{g \in G/S_\varphi \\ g' \in G/S_\psi}} \frac{|S_{g\varphi g'\psi}|}{|G|}\big[V\big(g\varphi g'\psi\big)\big] = \sum_{c_g \in G/\sim} s^g_{\varphi\psi}|c_g|\big[V(\varphi g\psi)\big], \tag{3.7}$$

which completes the proof. □

Corollary 3.2. *Let $\varphi, \psi \in \operatorname{Aut} L$. Then $\frac{1}{|G|} b_\varphi b_\psi \in \mathbb{Z}[\operatorname{Aut} L]$ and*

$$V(b_\varphi) \otimes_K V(b_\psi) \simeq V\left(\frac{1}{|G|} b_\varphi \cdot b_\psi\right).$$

Proof. Clearly,

$$\frac{1}{|G|} b_\varphi b_\psi = \sum_{g_1, g_2, g \in G} g_1 \varphi g \psi g_2,$$

which proves the first statement. On the other hand we have the following equalities in $\mathbb{Q}[\operatorname{Aut} L]$:

$$b_\varphi \cdot b_\psi = \Bigg(\sum_{\substack{g \in G/S_\varphi \\ g' \in G}} g\varphi g'\Bigg)\Bigg(\sum_{\substack{g \in G/S_\psi \\ g' \in G}} g\psi g'\Bigg) = \frac{|G|}{|S_\varphi||S_\psi|} \sum_{g \in G} |S_{\varphi g\psi}| b_{\varphi g\psi}.$$

Comparison with (3.7) we complete the proof. □

Corollary 3.3. *The map*

$$\Psi : \mathbb{Q} \otimes_{\mathbb{Z}} K_0(K, L) \longrightarrow \mathcal{H}_{\mathbb{Q}}(\operatorname{Aut} L; G), \quad \Psi\big(\big[V(\varphi)\big]\big) = \frac{1}{|G|} b_\varphi,$$

is an isomorphism of $\mathbb{Q}$-algebras.

Proof. Since the classes $[V(\varphi)]$ and the elements $\frac{1}{|G|} b_\varphi$, $\varphi \in G \backslash \operatorname{Aut} L/G$, form the $\mathbb{Q}$-bases in $\mathbb{Q} \otimes_{\mathbb{Z}} K_0(K, L)$ and in $\mathcal{H}_{\mathbb{Q}}(\operatorname{Aut} L; G)$ respectively, then Ψ is an isomorphism of $\mathbb{Q}$-vector spaces. The fact that Ψ is an algebra homomorphism follows immediately from Corollary 3.2. □

4. Galois rings

4.1. Notation and some examples

For the rest of the paper we will assume that Γ is an integral domain, K the field of fractions of Γ, $K \subset L$ is a finite Galois extension with the Galois group G, $\imath : K \to L$ is a natural embedding, $\mathcal{M} \subset \operatorname{Aut} L$ is a separating monoid on which G acts by conjugations, $\bar{\Gamma}$ is the integral closure of Γ in L, $\mathcal{K} = (L * \mathcal{M})^G$.

Now we introduce the main objects of our study.

Definition 3. A finitely generated Γ-subring $U \subset \mathcal{K}$ is called a *Galois Γ-ring* (or *Galois ring with respect to Γ*) if $KU = UK = \mathcal{K}$.

We will always assume that a Galois Γ-ring U has a structure of a $\Bbbk$-algebra. Hence there exists finitely many $u_1, \dots, u_k \in U$, which together with Γ generate U as $\Bbbk$-algebra. Note that following Lemma 4.1 below both equalities $KU = \mathcal{K}$ and $UK = \mathcal{K}$ are equivalent.

Example 4.1.

- Let $U = \Gamma[x; \sigma]$ be the *skew polynomial ring* over Γ, where $\sigma \in \operatorname{Aut} \Gamma$, $x\gamma = \sigma(\gamma)x$, for all $\gamma \in \Gamma$. Denote

$$\mathcal{M} = \big\{\sigma^n \;\big|\; n = 0, 1, \dots\big\} \subset \operatorname{Aut} K, \mathcal{M} \simeq \mathbb{Z}_+.$$

  Then for $L = K$, $G = \{e\}$ the algebra U is a Galois Γ-ring in $K * \mathcal{M}$, when x is identified with $1 * \sigma \in K * \mathcal{M}$.
- Analogously the *skew Laurent polynomial ring* $U = \Gamma[x; \sigma^{\pm 1}]$ is a Galois ring with $\mathcal{M} = \{\sigma^n \mid n \in \mathbb{Z}\}$ and trivial G.
- Let $\Gamma = \Bbbk[x_1, \dots, x_n]$ and $\sigma_1, \dots, \sigma_n \in \operatorname{Aut} \Gamma$, such that $\sigma_i \sigma_j = \sigma_j \sigma_i$, $i, j = 1, \dots, n$, $\mathcal{M} \subset \operatorname{Aut} \Gamma$ subgroup generated by $\sigma_1, \dots, \sigma_n$. Then the skew group ring $\Gamma * \mathcal{M}$ is a Galois Γ-ring with trivial G.

More examples, in particular with a nontrivial group G, will be given in Section 7.

4.2. Characterization of a Galois ring

A Γ-subbimodule of $\mathcal{K}$ which for every $m \in \mathcal{M}$ contains $[b_1 m], \dots, [b_k m]$ where $b_1, \dots, b_k$ is a K-basis in L^{H_m} will be called a *Γ-form* of $\mathcal{K}$. We will show that any Galois ring in $\mathcal{K}$ is its Γ-form.

Lemma 4.1. *Let U be a Galois Γ-ring, $u \in U$ a nonzero element, $T = \operatorname{supp} u$, $u = \sum_{m \in T/G} [a_m m]$ for some $a_m \in L^{H_m}$. Then*

$$K(\Gamma u \Gamma) = (\Gamma u \Gamma)K = KuK \simeq \bigoplus_{m \in T/G} V(m).$$

In particular U is a Γ-form of $\mathcal{K}$ and the statements $KU = \mathcal{K}$ and $UK = \mathcal{K}$ are equivalent. Besides, in $L * \mathcal{M}$ holds

$$L(\Gamma u \Gamma) = (\Gamma u \Gamma)L = LuL = \sum_{m\in T} Lm.$$

Proof. We prove the statement about the multiplications from the left, their right analogues can be proved analogously. Note that by Theorem 3.2, (5) and Lemma 2.2, (3) the modules $V(m)$, $m \in T/G$, are pairwise nonisomorphic simple K-bimodules. Since by Lemma 2.3, (2)

$$K[m]K = KK^m[m] \simeq V(m), \quad m \in T/G,$$

we have

$$KuK \subset \sum_{m\in T/G} K[a_m m]K = \bigoplus_{m\in T/G} K[a_m m]K \simeq \bigoplus_{m\in T/G} V(m).$$

Since all $V(m)$ are pairwise nonisomorphic simples, the image of KuK is not contained in any proper subbimodule of $W = \bigoplus_{m\in T/G} V(m)$. Hence $KuK \simeq W$ and therefore $K[a_m m]K \subset KuK$ for any $m \in T/G$.

For $m \in \operatorname{supp} u$ we prove, that $[am] \in KuK$ for some a. Then for some $\gamma_1, \gamma_2 \in \Gamma$ holds $\gamma_1[a\varphi]\gamma_2 = [\gamma_1 a \gamma_2^m m]$ belongs to $\Gamma u \Gamma$. So, for the rest of the proof it is enough to consider $u = [am]$. For every $\gamma \in \Gamma$ the element γ^m is algebraic over K, hence holds $(\gamma^m)^{-1} \in K[\gamma^m]$, henceforth $Km(\Gamma) = m(K)$. Then

$$\Gamma[am]\Gamma = \big[\Gamma \cdot m(\Gamma)am\big] \quad \text{and} \quad K\Gamma m(\Gamma) = Km(K).$$

The statement $K(\Gamma u \Gamma) = (\Gamma u \Gamma)K = KuK$ now follows from Lemma 2.3, (2).

Obviously $L[am]$ is an L-subbimodule in $\sum_{m\in T} Lm$, which is a direct sum of nonisomorphic simple L-bimodules. Any its subbimodule has the form $\sum_{m\in T'} Lm$, $T' \subset T$. On the other hand $\operatorname{supp}[am] = T$, and thus $L[am] = \sum_{m\in T} Lm$. $\square$

Corollary 4.1. *Let $[a\varphi], [b\psi] \in \mathcal{K}$. Then*

$$\operatorname{supp}[a\varphi]\Gamma[b\psi] = \operatorname{supp}[a\varphi]\operatorname{supp}[b\psi] = \mathcal{O}_\varphi \mathcal{O}_\psi.$$

Proof. Multiplication on L does not change the support. Then applying Lemma 4.1

$$\begin{aligned}\operatorname{supp}[a\varphi]\Gamma[b\psi] &= \operatorname{supp} L\big([a\varphi]\Gamma[b\psi]\big) = \operatorname{supp} L\big(K[a\varphi]\Gamma\big)[b\psi] \\ &= \operatorname{supp}\big(L[a\varphi]L\big)[b\psi] = \operatorname{supp}\Bigg(\sum_{m\in\mathcal{O}_\varphi} Lm\Bigg)[b\psi] = \mathcal{O}_\varphi \mathcal{O}_\psi. \qquad \square\end{aligned}$$

Proposition 4.1. *Assume a Γ-ring $U \subset \mathcal{K}$ is generated by $u_1, \dots, u_k \in U$.*

(1) *If $\bigcup_{i=1}^k \operatorname{supp} u_i$ generate $\mathcal{M}$ as a monoid, then U is a Galois ring.*
(2) *If $LU = L * \mathcal{M}$, then U is a Galois ring.*

Proof. The statement (2) follows from (1). Consider a K-subbimodule $Ku_1K + \cdots + Ku_kK$ in $\mathcal{K}$. By Lemma 4.1, this bimodule contains the elements $[a_1\varphi_1], \ldots, [a_N\varphi_N]$, where $\varphi_1^g, \ldots, \varphi_N^g$, $g \in G$, generate $\mathcal{M}$. By Corollary 4.1 $\operatorname{supp}([a_1m_1]\Gamma[a_2m_2]) = \operatorname{supp}[a_1m_1] \cdot \operatorname{supp}[a_2m_2]$ for $[a_1m_1], [a_2m_2] \in U$. It means, that even in the subalgebra U' of U, generated by $[a_1\varphi_1], \ldots, [a_N\varphi_N]$ and Γ for every $m \in \mathcal{M}$ there exists a nonzero $a_m \in L^{H_m}$ such that $[a_m m] \in U'$. Applying Lemma 4.1 and Lemma 2.1, (4) we obtain, that $KU = \mathcal{K}$. $\square$

Theorem 4.1. *Let U be a Galois ring, $e \in \mathcal{M}$ the unit element and $U_e = U \cap Le$. Then*

(1) *For every $x \in U$ holds $x_e \in K$ and $U_e \subset Ke$.*
(2) *The $\Bbbk$-subalgebra in $L * \mathcal{M}$ generated by U and L coincides with $L * \mathcal{M}$.*
(3) *$U \cap K$ is a maximal commutative $\Bbbk$-subalgebra in U.*
(4) *The center $Z(U)$ of algebra U equals $U \cap K^{\mathcal{M}}$.*

Proof. Let $x \in U$ and $x_e = \lambda$, $\lambda \in L$. Then for any $g \in G$ holds $\lambda = x_e = (x^g)_e = \lambda^g$. Hence $\lambda \in L^G = K$. The statement (2) follows from Lemma 4.1.

Consider any $x \in L * \mathcal{M}$ such that $x\gamma = \gamma x$ for all $\gamma \in \Gamma$. Assume $x_\varphi \neq 0$ for some $\varphi \in \mathcal{M}$, $\varphi \neq e$. Since the action of $\mathcal{M}$ is separating, there exists $\gamma \in \Gamma$ such that $\gamma^\varphi \neq \gamma$. Then $(\gamma x)_\varphi = \gamma x_\varphi \neq \gamma^\varphi x_\varphi = (x\gamma)_\varphi$ which is a contradiction. Hence $x \in U \cap Le = U_e \subset K$ which completes the proof of (3).

To prove (4) consider a nonzero $z \in Z(U)$. It follows from the proof of (3) that $z \in U \cap K$. Besides, $z \in \Gamma \cap Z(U)$ if and only if for every $[a\varphi] \in U$ holds $z[a\varphi] = [a\varphi]z$, i.e. $z = z^\varphi$. $\square$

Theorem 4.1, (3) in particular shows that a noncommutative associative algebra is never a Galois ring with respect to its center. For the same reason the universal enveloping algebra of a simple finite dimensional Lie algebra is not a Galois ring with respect to the enveloping algebra of its Cartan subalgebra.

Definition 4. A multiplicative closed subset H of $\mathcal{M}$ is called an *ideal* of $\mathcal{M}$ if $\mathcal{M}H \subset H$ and $H\mathcal{M} \subset H$.

Corollary 4.2. *There is one-to-one correspondence between the two-sided ideals in $\mathcal{K}$ and the G-invariant ideals in the monoid $\mathcal{M}$. This correspondence is given by the following bijection*

$$I \longmapsto \mathcal{I} = \mathcal{I}(I) = \bigcup_{u \in I} \operatorname{supp} u, \qquad \mathcal{I} \longmapsto I = I(\mathcal{I}) = \sum_{\varphi \in \mathcal{I}} K[\varphi]K, \tag{4.8}$$

where $I \subset \mathcal{K}$, $\mathcal{I} \subset \mathcal{M}$ are ideals, $\mathcal{I}$ is G-invariant. In particular, if $\mathcal{M}$ is a group then $\mathcal{K}$ is a simple ring.

Proof. Let I be a nonzero ideal in $\mathcal{K}$. If $0 \neq u \in I$ then

$$KuK \simeq \sum_{\varphi \in \operatorname{supp} u/G} K[\varphi]K$$

by Lemma 4.1 and for every $m \in \mathcal{M}$ holds $(K[m]K)(KuK) \subset I$, $(KuK)(K[m]K) \subset I$. By Corollary 4.1 for every $m \in \mathcal{M}$ and $\varphi \in \operatorname{supp} u$ there exist $u', u'' \in I$ such that $m\varphi \in \operatorname{supp} u'$ and $\varphi m \in \operatorname{supp} u''$, i.e. $\mathcal{I}$ is an ideal in $\mathcal{M}$. This gives the map $I \mapsto \mathcal{I}(I)$. Analogously, $I(\mathcal{I})$ is a two-sided ideal in $\mathcal{K}$ and both maps are mutually inverse. $\square$

Proposition 4.2. *Let U be a Galois ring with respect to Γ, $S = \Gamma \setminus \{0\}$.*

(1) *The multiplicative set S satisfies both left and right Ore conditions.*
(2) *The canonical embedding $U \hookrightarrow \mathcal{K}$ induces the isomorphisms of rings of fractions $[S^{-1}]U \simeq \mathcal{K}$, $U[S^{-1}] \simeq \mathcal{K}$.*

Proof. Assume $s \in S, u \in U$. Following Lemma 4.1, U contains a right K-basis $u_1, \ldots, u_k$ of KuK, hence in $\mathcal{K}$ holds

$$s^{-1}u = \sum_{i=1}^{k} u_i \gamma_i s_i^{-1} \quad \text{for some } s_i \in S,\ \gamma_i \in \Gamma,\ i = 1, \ldots, k.$$

Then in U holds

$$u \cdot (s_1 \ldots s_k) = s \cdot \left(\sum_{i=1}^{k} u_i \gamma_i s_1 \ldots s_{i-1} s_{i+1} \ldots s_k \right),$$

which shows (1). Besides S acts on U torsion free both from the left and from the right. Then there exist the right and left rings of fractions $U[S^{-1}]$, $[S^{-1}]U$. Following Lemma 4.1, the canonical embedding $U \hookrightarrow \mathcal{K}$ satisfies the conditions for the ring of fractions ((i)–(iii), [MCR], 2.1.3). Hence (2) follows. $\square$

Theorem 4.2. *The tensor product of two Galois rings is a Galois ring.*

Proof. Let U_i be a Galois Γ_i-subring in the skew-group algebra $L_i * \mathcal{M}_i$ with fraction fields K_i, $G_i = G(L_i/K_i)$, $i = 1, 2$. Then $\mathcal{M} = \mathcal{M}_1 \times \mathcal{M}_2$ acts on $L_1 \otimes_{\Bbbk} L_2$, $(m_1, m_2) \cdot (l_1 \otimes l_2) = m_1 l_1 \otimes m_2 l_2$. Since $\Bbbk$ is algebraically closed, $L_1 \otimes_{\Bbbk} L_2$ is a domain, hence $\mathcal{M}$ acts on its field of fractions L. Let $K \subset L$ be the field of fractions of $K_1 \otimes_{\Bbbk} K_2$. The extension $K \subset L$ is a finite Galois extension with the Galois group $G = G_1 \times G_2$. Consider the composition

$$\imath : U_1 \otimes_{\Bbbk} U_2 \longrightarrow (L_1 * \mathcal{M}_1) \otimes_{\Bbbk} (L_2 * \mathcal{M}_2) \overset{\Phi}{\simeq} (L_1 \otimes_{\Bbbk} L_2) * (\mathcal{M}_1 \times \mathcal{M}_2) \hookrightarrow L * \mathcal{M}.$$

We identify $U_1 \otimes_{\Bbbk} U_2$ with its image. To endow $U_1 \otimes_{\Bbbk} U_2$ with the structure of a Galois ring we shall prove that $L(U_1 \otimes_{\Bbbk} U_2) = L * \mathcal{M}$ (Proposition 4.1). But $L(U_1 \otimes_{\Bbbk} U_2) \supset L_1 U_1 \otimes_{\Bbbk} L_2 U_2 = (L_1 * \mathcal{M}_1) \otimes_{\Bbbk} (L_2 * \mathcal{M}_2)$, which contains $\Phi^{-1}(\mathcal{M}_1 \times \mathcal{M}_2)$. $\square$

5. Galois orders

5.1. Characterization of Galois orders

In this section we introduce a special class of Galois rings – Galois orders.

Definition 5. A Galois Γ-ring U is called *right* (*respectively left*) *integral Galois Γ-ring, or Galois order*, if for any finite dimensional right (respectively left) K-subspace $W \subset U[S^{-1}]$ (respectively $W \subset [S^{-1}]U$), $W \cap U$ is a finitely generated right (respectively left) Γ-module. A Galois ring is *Galois order* if it is both right and left Galois order.

Let M be a right Γ-submodule in a torsion free right Γ-module N. Consider the right subbimodule in N,

$$\mathbb{D}_{r,N}(M) = \{x \in N \mid \text{there exists } \gamma \in \Gamma,\ \gamma \neq 0 \text{ such that } x \cdot \gamma \in M\},$$

which is clearly a right Γ-module. For the left modules $M \subset N$ analogously is defined $\mathbb{D}_{l,N}(M)$. If N is a Galois Γ-ring U, the we skip N and write $\mathbb{D}_r(M)$ and $\mathbb{D}_l(M)$.

Lemma 5.1. *For right Γ-submodules of U holds the following*:

(1) $M \subset \mathbb{D}_r(M)$, $\mathbb{D}_r(\mathbb{D}_r(M)) = \mathbb{D}_r(M)$.
(2) $\mathbb{D}_r(M) = MK \cap U$.
(3) *If* $N \subset M$ *then* $\mathbb{D}_r(N) \subset \mathbb{D}_r(M)$.
(4) $\mathbb{D}_r(\Gamma) = U_e$.

Proof. Statements (1) and (3) are obvious. Statement (2) follows from the fact that U is torsion free left and right Γ-module. Theorem 4.1, (1) claims that $U_e \subset K$, implying (4). □

Lemma 5.1, (2) gives the following characterization of Galois orders.

Corollary 5.1. *A Galois ring U with respect to a noetherian Γ is* right Galois order *if and only if for every finitely generated right Γ-module $M \subset U$, the right Γ-module $\mathbb{D}_r(M)$ is finitely generated.*

Corollary 5.2. *If a Galois ring U with respect to a noetherian domain Γ is projective as a right* (*left*) *Γ-module then U is a right* (*left*) *Galois order.*

Proof. If U is right projective, then there exists some projective right Γ-module U', such that $U \oplus U' \simeq \bigoplus_{\mathfrak{I}} \Gamma$ for some set $\mathfrak{I}$. If M is a finitely generated right submodule in U, then there exists a finite subset $\mathfrak{J} \subset \mathfrak{I}$, such that $M \subset \bigoplus_{\mathfrak{J}} \Gamma \subset \bigoplus_{\mathfrak{I}} \Gamma$. Then $D_{r,U}(M) = D_{r,U\oplus U'}(M) = D_{r,\bigoplus_{\mathfrak{J}} \Gamma}(M) \subset \bigoplus_{\mathfrak{J}} \Gamma$. Then $D_r(M)$ is finitely generated since $|\mathfrak{J}| < \infty$ and Γ is noetherian. □

Corollary 5.3. *If U is right* (*left*) *Galois order then $\Gamma \subset U_e$ is an integral extension. In particular U_e is a normal ring.*

Proof. Lemma 5.1, (4) shows that $U_e = D_r(\Gamma) \subset K$ is finitely generated right (left) Γ-module. Moreover, it is finitely generated as left and right Γ-module simultaneously. The statement follows from Proposition 2.1. □

We will show in Theorem 5.2, (2) that the converse statement holds when $\mathcal{M}$ is a group.

5.2. Harish-Chandra subalgebras

Following [DFO2] a commutative subalgebra $\Gamma \subset U$ is called a *Harish-Chandra subalgebra* in U if for any $u \in U$, the Γ-bimodule $\Gamma u \Gamma$ is finitely generated both as a left and as a right Γ-module. Assume Γ and some family $\{u_i \in U\}_{i \in I}$ generate U as $\Bbbk$-algebra and every $\Gamma u_i \Gamma$, $i \in I$, is left and right finitely generated. Then it is easy to see, that Γ is a Harish-Chandra subalgebra in U.

Proposition 5.1. *Assume Γ is finitely generated algebra over $\Bbbk$, U is a Galois ring. Then Γ is a Harish-Chandra subalgebra in U if and only if $m \cdot \bar{\Gamma} = \bar{\Gamma}$ for every $m \in \mathcal{M}$.*

Proof. Note that $\bar{\Gamma}$ is finitely generated as Γ-module (Proposition 2.1). Suppose first $m \cdot \bar{\Gamma} = \bar{\Gamma}$ for every $m \in \mathcal{M}$. It is enough to prove that $\Gamma[am]\Gamma$ is finitely generated as a left (right) Γ-module for any $m \in \mathcal{M}, a \in L$. But following (2.5)

$$\Gamma[am]\Gamma = \big[\Gamma \cdot m(\Gamma)am\big] = \big[am\Gamma \cdot m^{-1}(\Gamma)\big] \tag{5.9}$$

is finitely generated over Γ from the left, since $\Gamma m(\Gamma) \subset \bar{\Gamma}$, and it is finitely generated from the right, since $\Gamma m^{-1}(\Gamma) \subset \bar{\Gamma}$. Conversely, assume $\Gamma[am]\Gamma$ is finitely generated right Γ-module for any $[am] \in U$. It means that $\Gamma \cdot m^{-1}(\Gamma)$ is finite over Γ, i.e. $m^{-1}(\Gamma) \subset \bar{\Gamma}$. Analogously, $m(\Gamma) \subset \bar{\Gamma}$. □

Proposition 5.2. *If U is a right (left) Galois order with respect to a noetherian Γ then for any $m \in \mathcal{M}$ holds $m^{-1}(\Gamma) \subset \bar{\Gamma}$ ($m(\Gamma) \subset \bar{\Gamma}$).*

Proof. Let U be right Galois order, $[am] \in U$, $\gamma \in \Gamma$. Assume $x = m^{-1}(\gamma) \notin \bar{\Gamma}$. Then the right Γ-submodule of U,

$$M = \sum_{i=0}^{\infty} \gamma^i [am]\Gamma = \sum_{i=0}^{\infty} \left[amx^i \Gamma\right] \simeq \sum_{i=0}^{\infty} x^i \Gamma$$

is not finitely generated. On the other hand, x is an algebraic element over K. Let

$$\gamma_0 x^n + \gamma_1 x^{n-1} + \cdots + \gamma_n = 0, \quad \gamma_i \in \Gamma,\ \gamma_0 \neq 0. \tag{5.10}$$

Consider the following finitely generated right Γ-module $N = \sum_{i=0}^{n-1} \gamma^i [am]\Gamma \simeq \sum_{i=0}^{n-1} x^i \Gamma$. But following (5.10) $M \subset \mathbb{D}_r(N)$ which is a contradiction. The case of left order treated analogously. $\square$

From Propositions 5.2 and 5.1 we immediately obtain:

Corollary 5.4. *Let Γ be a finitely generated domain over $\Bbbk$ and U a Galois order with respect to Γ. Then Γ is a Harish-Chandra subalgebra in U.*

Remark 5.1. Let Γ be integrally closed in K and $\varphi : K \to K$ an automorphism of infinite order, such that $\varphi(\Gamma) \overset{\neq}{\subset} \Gamma$. Set $L = K$, $\mathcal{M} = \{\varphi^n \mid n \geqslant 0\}$. Then $L * \mathcal{M}$ is isomorphic to the skew polynomial algebra $K[x;\varphi]$ [MCR]. Its subalgebra U generated by Γ and x is a Galois ring. Clearly, U is left Galois order (but not right Galois order).

5.3. *Properties of Galois orders*

In this section we establish basic properties of Galois orders, in particular we provide several criteria for a Galois ring to be Galois order.

Let U be a Galois ring with respect to Γ, $S \subset \mathcal{M}$ a finite G-invariant subset. Denote

$$U(S) = \{u \in U \mid \operatorname{supp} u \subset S\}. \tag{5.11}$$

Obviously, it is a Γ-subbimodule in U and $\mathbb{D}_r(U(S)) = \mathbb{D}_l(U(S)) = U(S)$. This notion will give us one more characterization of Galois orders (Theorem 5.1).

It will be convenient to consider the Γ-bimodule structure of U as a $\Gamma \otimes_{\Bbbk} \Gamma$-module structure. For every $f \in \Gamma$ define $f_S^r \in \Gamma \otimes_{\Bbbk} L$ (respectively $f_S^l \in L \otimes_{\Bbbk} \Gamma$) as follows

$$f_S^r = \prod_{s \in S} \left(f \otimes 1 - 1 \otimes f^{s^{-1}}\right) = \sum_{i=0}^{|S|} f^{|S|-i} \otimes h_i, \quad h_0 = 1, \tag{5.12}$$

$$\left(\text{respectively} \quad f_S^l = \prod_{s \in S} \left(f^s \otimes 1 - 1 \otimes f\right) = \sum_{i=0}^{|S|} h_i' \otimes f^{|S|-i}, \quad h_0' = 1\right). \tag{5.13}$$

Since S is G-invariant, then all h_i and h_i' are G-invariant expressions in f^m, $m \in \mathcal{M}$, they belongs to K. If U is right (left) integral, then $h_S^r \in \Gamma \otimes U_e$ ($h_S^l \in U_e \otimes \Gamma$). Note, that if Γ is normal (i.e. integrally closed in K), then both expressions belong to $\Gamma \otimes_{\Bbbk} \Gamma$ We will consider the properties of $f_S = f_S^r$, the case of f_S^l can be treated analogously. Note that the coefficients of $f_S = f_S^r$ a priori belong to K:

Lemma 5.2. *Let Γ be a normal domain, $m \in \mathcal{M}$, $m^{-1}(\Gamma) \subset \bar{\Gamma}$. $S \subset \mathcal{M}$ a G-invariant subset, $u \in U$, $f \in \Gamma$.*

(1) *$u \in U(S)$ if and only if $f_S \cdot u = 0$ for every $f \in \Gamma$.*
(2) *If $u \in U$ and $T = \operatorname{supp} u \setminus S$ then $f_T \cdot u \in U(S)$ for every $f \in \Gamma$.*
(3) *If $f_S = \sum_{i=1}^n f_i \otimes g_i$, $[am] \in \mathcal{K}$ then $f_S \cdot [am] = [(\sum_{i=1}^n f_i g_i^m a)m] = [\prod_{s \in S}(f - f^{ms^{-1}})am]$.*
(4) *Let S a G-orbit and T a G-invariant subset in $\mathcal{M}$. The Γ-bimodule homomorphism P_S^T $(= P_S^T(f))$: $U(T) \to U(S)\gamma^{-1} \subset \mathcal{K}$, for some $\gamma \in \Gamma$, $u \mapsto f_{T \setminus S} \cdot u$, $f \in \Gamma$ is either zero or $\operatorname{Ker} P_S^T = U(T \setminus S)$ (both cases are possible, cf. (1)). $s \in \Gamma$ can be taken as 1, provided that Γ be a normal domain.*
(5) *In the assumption of (4) let $S = S_1 \sqcup \cdots \sqcup S_n$ be the decomposition of S in G-orbits and $P_{S_i}^S : U(S) \to U(S_i)\gamma_i^{-1}$ for some $f_i \in \Gamma$, $\gamma_i \in \Gamma$, $i = 1, \dots, n$, are defined in (4) nonzero homomorphisms. Then the homomorphism*

$$P^S : U(S) \longrightarrow \bigoplus_{i=1}^n U(S_i)\gamma_i^{-1}, \quad P^S = \left(P_{S_1}^S, \dots, P_{S_n}^S\right), \tag{5.14}$$

is a monomorphism of Γ-bimodules.
(6) *The statements above hold true, provided that the normal domain Γ is a Harish-Chandra subalgebra in U. In this case we can set $\gamma = \gamma_i = 1$, $i = 1, \dots, n$.*

Note, that $U(S_i)\gamma^{-1}$ as a K-bimodule is canonically isomorphic to $U(S_i)$, $i = 1, \dots, n$.

Proof. Consider any $[am] \in \mathcal{K}$, $s \in \operatorname{Aut} L$. Then

$$\left(f \otimes 1 - 1 \otimes f^s\right) \cdot [am] = [fam] - \left[amf^s\right] = \left[\left(f - f^{ms}\right)am\right],$$

hence

$$f_S \cdot [am] = \prod_{s \in S}\left(f \otimes 1 - 1 \otimes f^{s^{-1}}\right) \cdot [am] = \left[\prod_{s \in S}\left(f - f^{ms^{-1}}\right)am\right].$$

First of all it proves (3). On the other hand, if $m \in S$, then one of $f - f^{ms^{-1}}$ equals zero, hence, $f_S \cdot [am] = 0$. To prove the converse we show that for any $m \notin S$ there exists $f \in \Gamma$ such that $f \neq f^{ms^{-1}}$ for all $s \in S$. Following Lemma 2.2, (2) for every $m \in \mathcal{M}, m \neq e$, the space of m-invariants $\Gamma^m \neq \Gamma$. But the $\Bbbk$-vector space Γ cannot be covered by finitely many proper subspaces $\Gamma^{ms^{-1}}$, $s \in S$, that completes the proof of (1).

The calculation above shows, that $f_{\operatorname{supp} u} \cdot u = 0$ for any $f \in \Gamma$. Then statement (2) follows from (1) and from the fact, that $f_{\operatorname{supp} u}$ divides $f_S f_T$. By (3), $f_{T \setminus S} \neq 0$ if and only if $\sum_{i=1}^n f_i g_i^m \neq 0$, and in this case $f_{T \setminus S}$ acts on $U(S)$ injectively, that proves (4).

Finally, (5) follows from (4), since $\bigcap_{i=1}^n \operatorname{Ker} P_{S_i}^S = 0$. The statement (6) follows from the definition. $\square$

Theorem 5.1. *Let U be a Galois ring with respect to a finitely generated over $\Bbbk$ Harish-Chandra subalgebra Γ. Then the following statements are equivalent:*

(1) *U is right (respectively left) Galois order.*
(2) *$U(S)$ is finitely generated right (respectively left) Γ-module for any finite G-invariant $S \subset \mathcal{M}$.*
(3) *$U(\mathcal{O}_m)$ is finitely generated right (respectively left) Γ-module for any $m \in \mathcal{M}$.*

Proof. Assume U is right Galois order. Let S be a finite G-invariant subset of $\mathcal{M}$, and $u_1, \dots, u_k \in U(S)$ a basis of $U(S)K$ as a right K-space. Then using Lemma 4.1 and Corollary 5.1

$$\mathbb{D}_r\left(\sum_{i=1}^{k} u_i \Gamma\right) = \left(\sum_{i=1}^{k} u_i \Gamma\right) K \cap U = U(S)K \cap U = \mathbb{D}_r\big(U(S)\big) = U(S).$$

Therefore, $U(S) = \mathbb{D}_r(\sum_{i=1}^{k} u_i \Gamma)$ is finitely generated, which proves (2). Obviously, (2) implies (3). Assume (3) holds. Let $M \subset U$ be a finitely generated right Γ-submodule, $S = \operatorname{supp} M$. Then $M \subset U(S)$ and $\mathbb{D}_r(M) \subset \mathbb{D}_r(U(S)) = U(S)$. By Corollary 5.1, it remains to prove that $U(S)$ is finitely generated. Let $S = S_1 \sqcup \dots \sqcup S_n$ be the decomposition of S into G-orbits. The constructed in Lemma 5.2, (5) P^S embeds $U(S)$ into $\bigoplus_{i=1}^{n} U(S_i)\gamma_i^{-1}$. Since Γ is noetherian, $D_r(M) \subset D_r(S)$ is finitely generated, that together with Corollary 5.1 completes the proof. □

Theorem 5.2. *Assume that U is a Galois ring, Γ is finitely generated and $\mathcal{M}$ is a group.*

(1) *Assume $m^{-1}(\Gamma) \subset \bar{\Gamma}$ (respectively $m(\Gamma) \subset \bar{\Gamma}$). Then U is right (respectively left) Galois order if and only if U_e is an integral extension of Γ.*
(2) *Assume Γ is a Harish-Chandra subalgebra in U. Then U is a Galois order if and only if U_e is an integral extension of Γ.*

Proof. Obviously (2) is proved in (1) and Proposition 5.1. The statement "only if" in (1) follows from Corollary 5.3. Assume U_e is an integral extension of Γ, $m^{-1}(\Gamma) \subset \bar{\Gamma}$, but U is not right order. Following Theorem 5.1, (3) there exists $m \in \mathcal{M}$, such that $U(\mathcal{O}_m)$ is not finitely generated.

Since $\mathcal{M}$ is a group by Lemma 4.1 there exists $[bm^{-1}] \in U$. Since $H_m = H_{m^{-1}}$ for any nonzero $\gamma \in \Gamma$ holds

$$\big([bm^{-1}]\gamma[ma]\big)_e = \sum_{g \in G/H_m} b^g \gamma^{(m^{-1})^g} a^g. \tag{5.15}$$

Denote this expression by $v_\gamma(a)$, $\gamma \in \Gamma$, $a \in L^{H_m}$. Then $v_\gamma : L^{H_m} \to K$ is a right K-linear map and $v_{\gamma_1} + v_{\gamma_2} = v_{\gamma_1+\gamma_2}$, $\gamma_1, \gamma_2 \in \Gamma$.

Denote $|G/H_m|$ by n. Let $\{a_i \in L^{H_m} \mid i = 1, \dots, n\}$ be a basis of L^{H_m} over K. In particular, $[ma_i]$, $i = 1, \dots, n$, form a right K-basis of KmK. It will be convenient to enumerate entries of matrices by the classes from G/H_m and the numbers $1, \dots, n$.

Lemma 5.3.

(1) *For any nonzero $b \in L^{H_m}$, the $n \times n$ matrix over L,*

$$X = \big(b^g a_i^g \bigm| g \in G/H_m;\ i = 1, \dots, n\big)$$

is invertible.

(2) *There exist $\gamma_1, \dots, \gamma_n \in \Gamma$, such that $n \times n$ matrix*

$$Y = \big(\gamma_i^{gm^{-1}g^{-1}} \bigm| i = 1, \dots, n;\ g \in G/H_m\big)$$

is non-degenerated. Besides for $n \times n$ matrices holds

$$YX = \big(v_{\gamma_i}(a_j) \bigm| i, j = 1, \dots, n\big).$$

(3) *Let* $Z = (\mu_{ij} \mid i = 1, \dots, n;\ j = 1, \dots, n)$ *be a non-degenerated matrix over* K, $b_i = \sum_{j=1}^n a_j \mu_{ij}$, $i = 1, \dots, n$, *the new right* K*-basis of* L^{H_m}. *Then*

$$(YX)Z = \big(v_{\gamma_j}(b_i) \bigm| i, j = 1, \dots, n\big).$$

(4) *In particular, if* $Z = (YX)^{-1}$ *holds*

$$v_{\gamma_i}(b_j) = \delta_{ij}, \quad i, j = 1, \dots, n.$$

Proof. To prove the first statement there is enough to prove the invertibility of the matrix $(a_i^g \mid g \in G/H_m;\ i = 1, \dots, n)$. Assume, opposite, i.e. $(\sum_{g \in G/H_m} \lambda_g g)(a_i) = 0$, $\lambda_g \in L$ for some vector $(\lambda_g \mid g \in G/H_m) \neq 0$ and for any $i = 1, \dots, n$. Then $(\sum_{g \in G/H_m} \lambda_g g)|_{L^{H_m}} = 0$, which contradicts to the independence of different characters $g|_{L^{H_m}} : L^{H_m} \to L$, $g \in G/H_m$.

Analogously all $\{gm^{-1}g^{-1} \mid g \in G/H_m\}$ act differently in restriction on Γ, hence the row rank of $G/H_m \times \Gamma$ matrix over L,

$$\big(\gamma^g \bigm| g \in G/H_m;\ \gamma \in \Gamma\big),$$

equals n. Then its column rank of this matrix equals n as well, that finishes the proof of the second statement.

The third and fours statement is proved by direct calculation

$$(YX)_{ij} = \sum_{g \in G/H_m} b^g \gamma_i^{gm^{-1}g^{-1}} a_j^g = v_{\gamma_i}(a_j),$$

$$\big((YX)Z\big)_{ij} = \sum_{l=1}^n v_{\gamma_i}(a_l)\mu_{lj} = v_{\gamma_i}\left(\sum_{l=1}^n a_l \mu_{lj}\right) = v_{\gamma_i}(b_j).$$

The last statement is obvious. □

Fix $\gamma_1, \dots, \gamma_n$ from Lemma 5.3, (2) and the basis $b_1, \dots, b_n$ from Lemma 5.3, (4). Possibly changing all b_i's to γb_i for some fixed $\gamma \in \Gamma$, we can assume, that $[b_i m] \in U$ and $v_{\gamma_i}(b_j) = \gamma \delta_{ij}$, $i, j = 1, \dots, n$.

Assume $U(\mathcal{O}_m)$ contains a strictly ascending chain of right Γ-submodules

$$N_k = \sum_{i=1}^k [mt_i]\Gamma, \quad i = 1, 2, \dots, \ N = \bigcup_{k=1}^\infty N_k. \tag{5.16}$$

Consider the decomposition $t_i = \sum_{j=1}^n \gamma_{ij} b_j$, $\gamma_{ij} \in K$. Then there exists $1 \leqslant l \leqslant n$, such that the Γ-module $T_l = \sum_{i=1}^\infty \gamma_{il}\Gamma \subset K$ is not finitely generated. In opposite case from notherianity of Γ and $N \subset \bigoplus_{i=1}^n [mT_i]$ follows, that N is finitely generated. Then by Lemma 5.3, (4) and (5.15) we obtain that $v_{\gamma_l}(t_i) = \gamma \gamma_{il} \delta_{il}$.

$$\big([b_l m]\gamma_l\big[m^{-1}N\big]\big)_e = v_{\gamma_l}(N) = \gamma T_l.$$

Let $S = \mathcal{O}_{m^{-1}}\mathcal{O}_m$. Since $m^{-1}(\Gamma) \subset \bar{\Gamma}$ by Lemma 5.2, (5) there exists $F = \sum_{i=1}^n f_i \otimes g_i \in \Gamma \otimes_{\Bbbk} U_e$, which defines a nonzero morphism $P_e^S : U(S) \to U(\{e\})\gamma_e^{-1} = U_e\gamma_e^{-1}$. Moreover, the value of $P_e^S(x)$,

$x \in U(S)$, depends only on x_e, namely, by Lemma 5.2, (3) $P_e^S(x) = \gamma' x_e$, where $\gamma' = \sum_{i=1}^n f_i g_i$, in particular $P_e^S(x) = 0$ if and only if $x_e = 0$. Then

$$P_e^S\big([bm]\gamma_l\big[m^{-1}N\big]\big) = P_e^S(\gamma T_l) = \gamma'\gamma T_l \subset U_e\gamma_e^{-1} \simeq U_e.$$

It means that U_e contains right Γ-submodule, isomorphic T_l, hence U_e is not finitely generated. □

Corollary 5.5. *Let $\mathcal{M}$ be a group, Γ normal and noetherian, $\mathcal{M} \cdot \bar{\Gamma} = \bar{\Gamma}$, $u_1, \dots, u_n$ are such, that $\bigcup_{i=1}^n \operatorname{supp} u_i$ generate $\mathcal{M}$ as a monoid. If for every $[am] \in \mathcal{K}$ entering in u_i, $i = 1, \dots, n$, the coefficient $a \in L^{H_\varphi}$ is algebraic over Γ, then the subring in $\mathcal{K}$, generated by $\Gamma, u_1, \dots, u_n$ is a Galois order with respect to Γ.*

Proof. Since $\mathcal{M} \cdot \bar{\Gamma} = \bar{\Gamma}$ any $u \in U$ has a form $u = \sum_{m\in\mathcal{M}}[a_m m]$, where all a_m are in $\bar{\Gamma}$. In particular, if $u \in U_e$ then $u = [a_e e]$ where $a_e \in K \cap \bar{\Gamma}$. Since Γ is normal $U_e = \Gamma$. Applying Theorem 5.2, (2) we obtain the statement. □

The next corollary is a noncommutative analog of Proposition 2.2.

Corollary 5.6. *Let $U \subset L * \mathcal{M}$ be a Galois ring with respect to noetherian Γ, $\mathcal{M}$ a group and Γ a normal $\Bbbk$-algebra. Then the following statements are equivalent*:

(1) *U is a Galois order.*
(2) *Γ is a Harish-Chandra subalgebra and, if for $u \in U$ there exists a nonzero $\gamma \in \Gamma$ such that $\gamma u \in \Gamma$ or $u\gamma \in \Gamma$, then $u \in \Gamma$.*

Proof. Assume (1). Then Γ is a Harish-Chandra subalgebra by Corollary 5.4. If $u\gamma \in \Gamma$ for $u \in U$ and $\gamma \in \Gamma$, then $\operatorname{supp} u = \{e\}$, hence $u \in U_e$. Applying Corollary 5.3 we obtain (2). To prove the converse implication consider $u \in U_e$. Since $U_e \subset K$ (Theorem 4.1, (1)), there exists $\gamma \in \Gamma$, such that $\gamma u \in \Gamma$. Thus, $u \in \Gamma$. Theorem 5.2, (2) completes the proof. □

5.4. Filtered Galois orders

Let U be a Galois ring with respect to a noetherian normal $\Bbbk$-algebra Γ. Suppose in addition that U is an algebra over $\Bbbk$, endowed with an increasing exhausting filtration $\{U_i\}_{i\in\mathbb{Z}}$, $U_{-1} = \{0\}$, $U_0 = \Bbbk$, $U_i U_j \subset U_{i+j}$ and $\operatorname{gr} U = \bigoplus_{i=0}^\infty U_i/U_{i-1}$ the associated graded algebra.

The filtration on Γ induces a degree "deg" both on U and $\operatorname{gr} U$. For $u \in U$ denote by $\bar{u} \in \operatorname{gr} U$ the corresponding homogeneous element and denote by $\operatorname{gr}\Gamma$ the image of Γ in $\operatorname{gr} U$.

Proposition 5.3. *Assume $\operatorname{gr} U$ is a domain. If the canonical embedding $\imath : \operatorname{gr}\Gamma \hookrightarrow \operatorname{gr} U$ induces an epimorphism*

$$\imath^* : \operatorname{Specm} \operatorname{gr} U \longrightarrow \operatorname{Specm} \operatorname{gr}\Gamma$$

then U is a Galois order with respect to Γ.

Proof. We apply Corollary 5.6. Suppose $y = xu \neq 0$, $y, x \in \Gamma$, $u \in U \setminus \Gamma$ with minimal possible $\deg y$. Then $\bar{y} = \bar{x}\bar{u} \neq 0$ in $\operatorname{gr} U$. By Proposition 2.2 $\bar{u} \in \operatorname{gr}\Gamma$. Hence $\bar{u} = \bar{z}$ for some in $z \in \Gamma$. Since $z \neq u$, we have $y_1 = xu_1$ where $u_1 = u - z$, $y_1 = y - xz$. Then $x, y_1 \in \Gamma$, $u_1 \notin \Gamma$ and $\deg y_1 < \deg y$. Obtained contradiction shows that $u \in \Gamma$. □

6. Gelfand–Kirillov dimension of Galois orders

In this section we assume that $\mathcal{M}$ is a group of finite growth and Γ is a finitely generated $\Bbbk$-algebra. In particular, Γ is of finite Gelfand–Kirillov dimension, which equals to the transcendence degree of K over $\Bbbk$.

6.1. Growth of group algebras

Let $S_* = \{S_1 \subset S_2 \subset \cdots \subset S_N \subset \cdots\}$ be an increasing chain of finite sets. Then the growth of S_* is defined as

$$\operatorname{growth}(S_*) = \varlimsup_{N\to\infty} \log_N |S_N|. \tag{6.17}$$

For $s \in S = \bigcup_{i=0}^{\infty} S_i$ set $\deg s = i$ if $s \in S_i \setminus S_{i-1}$. Let $\{\gamma_1, \dots, \gamma_k\}$ be a set of generators of Γ. For $N \in \mathbb{N}$ denote by $\Gamma_N \subset \Gamma$ the subspace of Γ generated by the products $\gamma_{i_1} \dots \gamma_{i_t}$, for all $t \leqslant N$, $i_1, \dots, i_t \in \{1, \dots, k\}$. Let $d_\Gamma(N) = \dim_\Bbbk \Gamma_N$ and let $B_N(\Gamma)$ be a basis in Γ_N ($B_1(\Gamma) = \{\gamma_1, \dots, \gamma_k\}$). Fix a set of generators of $\mathcal{M}$ of the form $\mathcal{M}_1 = \mathcal{O}_{\varphi_1} \cup \cdots \cup \mathcal{O}_{\varphi_n}$. For $N \geqslant 1$, let $\mathcal{M}_N$ be the set of words $w \in \mathcal{M}$ such that $l(w) \leqslant N$, where l is the length of w, i.e.

$$\mathcal{M}_{N+1} = \mathcal{M}_N \cup \left(\bigcup_{\varphi \in \mathcal{M}_1} \varphi \cdot \mathcal{M}_N \right). \tag{6.18}$$

Note that all sets $\mathcal{M}_N$ are G-invariant. Denote the cardinality of $\mathcal{M}_N$ by $d_{\mathcal{M}}(N)$. Let $\mathcal{M}_* = \{\mathcal{M}_1 \subset \mathcal{M}_2 \subset \cdots \subset \mathcal{M}_N \subset \cdots\}$. Then $\operatorname{growth}(\mathcal{M})$ is by definition $\operatorname{growth}(\mathcal{M}_*)$.

Let $\Gamma[\mathcal{M}]$ be the group algebra of $\mathcal{M}$. Assume, G acts on $\Gamma[\mathcal{M}]$, acting by $\mathcal{M}$ by conjugations and trivially on Γ. Then the space $\Gamma[\mathcal{M}]_N$ has a G-invariant basis

$$B_N\big(\Gamma[\mathcal{M}]\big) = \bigsqcup_{i=0}^{N} \bigsqcup_{\substack{w \in \mathcal{M}_{N-i} \\ l(w) = N-i}} B_i(\Gamma) w \tag{6.19}$$

and $\operatorname{GKdim} \Gamma[\mathcal{M}] = \operatorname{growth} B_*(\Gamma[\mathcal{M}])$. In particular (e.g. [MCR], Lemma 8.2.4)

$$\operatorname{GKdim} \Gamma[\mathcal{M}] = \operatorname{GKdim} \Gamma + \operatorname{growth}(\mathcal{M}). \tag{6.20}$$

The growth of the chain $B_*(\Gamma[\mathcal{M}])/G$ is equal to $\operatorname{growth} B_*(\Gamma[\mathcal{M}])$, since

$$\big|B_N\big(\Gamma[\mathcal{M}]\big)\big| > \big|B_N\big(\Gamma[\mathcal{M}]\big)/G\big| \geqslant \frac{1}{|G|} \big|B_N\big(\Gamma[\mathcal{M}]\big)\big|.$$

6.2. Gelfand–Kirillov dimension

The goal of this section is to prove (under a certain condition) an analogue of the formula (6.20) for Galois orders.

Theorem 6.1. *Let U be a Galois Γ-ring such that Γ is a normal Harish-Chandra subalgebra in U and such that for every finite dimensional $\Bbbk$-vector space $V \subset \bar{\Gamma}$ the set $\mathcal{M} \cdot V$ is contained in a finite dimensional subspace of $\bar{\Gamma}$. If $\mathcal{M}$ is a group of finite growth* $\operatorname{growth}(\mathcal{M})$, *then*

$$\operatorname{GKdim} U \geqslant \operatorname{GKdim} \Gamma + \operatorname{growth}(\mathcal{M}). \tag{6.21}$$

Proof. Since the Gelfand–Kirillov dimension is monotone with respect to the operation of taking a subalgebra, without loss of generality we can assume, that U is a Galois order. Indeed, since algebra U is a Γ-form of $\mathcal{K}$ (Lemma 4.1), then we can assume that the Galois ring U is generated by Γ and a set of generators $\mathcal{G} = \{[a_1\varphi_1], \dots, [a_n\varphi_n]\}$. Then there exists $\gamma \in \Gamma$, such that all γa_i are integral over Γ. Hence by Corollary 5.5, there is enough to prove Theorem 6.1 for a Galois order, generated by Γ and $\mathcal{G}$ with $a_i \in \bar{\Gamma}$.

Set $B_1(U) = B_1(\Gamma) \sqcup \mathcal{G}$. As above, define the subspaces U_N and dimensions $d_U(N)$. For every $N \geqslant 1$ fix a basis $B_N(U)$ of U_N.

The proof of Theorem 6.1 is based on the following lemmas. We will assume that the conditions of Theorem 6.1 are satisfied.

Lemma 6.1. *If for some $p, q \in \mathbb{Z}$ and $C > 0$ for any $N \in \mathbb{N}$ holds*

$$d_U(pN + q) \geqslant C d_{\Gamma[\mathcal{M}]}(N), \tag{6.22}$$

then $\operatorname{GKdim} U \geqslant \operatorname{GKdim} \Gamma[\mathcal{M}]$.

Proof.

$$\begin{aligned}\operatorname{GKdim} \Gamma[\mathcal{M}] &= \overline{\lim_{N\to\infty}} \log_N d_{\Gamma[\mathcal{M}]}(N) \leqslant \overline{\lim_{N\to\infty}} \log_N d_U(pN+q) \\ &= \overline{\lim_{N\to\infty}} \log_{pN+q} d_U(pN+q) \leqslant \overline{\lim_{N\to\infty}} \log_N d_U(N) = \operatorname{GKdim} U. \qquad \square\end{aligned}$$

Lemma 6.2. *Denote by $N(i)$, $i = 1, 2, \dots$, the minimal number such that for any $m \in \mathcal{M}_i$ the set $U_{N(i)}$ contains an element of the form $[bm]$, $b \neq 0$. Then holds the following*:

(1) *For every $i = 1, \dots, n$ there exists a finite dimensional over $\Bbbk$ space $V_i \subset \Gamma$, such that for any $x \in U$ and $m \in \operatorname{supp} x$ there exists $y \in [a_i\varphi_i]V_i x$ such that $\varphi_i m \in \operatorname{supp} y$. Besides $|\operatorname{supp} y| \leqslant |G||\operatorname{supp} x|$ and $\deg y - \deg x \leqslant d$ for some fixed $d > 0$.*
(2) *For every $k \geqslant 1$ there exists $t(k) \geqslant 0$ with the following property: for every $j \geqslant 1$ and $u \in U_j$, such that $|\operatorname{supp} u| \leqslant k$ and for any $m \in \operatorname{supp} u$ there exists a nonzero element $[bm] \in U_{j+t(k)}$.*
(3) *The sequence $N(i+1) - N(i)$, $i = 1, 2, \dots$, is bounded.*

Proof. Let $L(G/H_{\varphi_i})$ be the vector space over L with the basis, enumerated by cosets G/H_φ, $\varphi \in \mathcal{M}$. We endow this space with the standard scalar product. Fix i, $1 \leqslant i \leqslant n$, and consider the nonzero vector

$$v(x) = \left(a_i^g x^{\varphi_i^g}_{(\varphi_i^g)^{-1}\varphi_i m}\right)_{g \in G/H_{\varphi_i}} \in L(G/H_{\varphi_i}).$$

Then for any $\gamma \in \Gamma$ immediate calculation shows, that

$$\left([a\varphi_i]\gamma x\right)_{\varphi_i m} = v(x) \cdot \left(\gamma^{\varphi_i^g}\right)_{g \in G/H_{\varphi_i}} \in L^{H_{\varphi_i m}}. \tag{6.23}$$

Since φ_i^g, where g runs G/H_φ are different in the restriction to K, there exist $\gamma_1, \dots, \gamma_k \in \Gamma$, $k = |G/H_{\varphi_i}|$, such that the $k \times k$ matrix $(\gamma_j^{\varphi_i^g})_{j=1,\dots,k;\, g \in G/H_{\varphi_i}}$ is non-degenerated. Then we set $V_i = (\gamma_1, \dots, \gamma_k)$. Since the vector $v(x)$ is nonzero, there exists $\gamma \in V_1$, such that the element from (6.23) is nonzero, that prove existence V_i. Note, that the multiplication on $\gamma \in \Gamma$, $\gamma \neq 0$ does not change the support of x. Hence we obtain

$$|\operatorname{supp} y| \leqslant k|\operatorname{supp} x| \leqslant |G||\operatorname{supp} x|.$$

As d we can choose the maximum of $d_i = 1 + \max\{\deg v \mid v \in V_i\}$, $i = 1, \dots, n$. It proves (1).

Now we prove (2). If $\operatorname{supp} u = G \cdot m$ then $u = [bm]$ for some $b \in L^{H_m}$ and then put $t(1) = 0$. Fix some $k \geqslant 2$. Assume $u = [cm] + v, m \notin \operatorname{supp} v, |\operatorname{supp} v| \leqslant k - 1$. For $f \in \Gamma_1$ consider the polynomial f_S (Section 5.3, (5.12)) with $S = \operatorname{supp} u \setminus G \cdot m$. Applying Lemma 5.2 we obtain the element

$$f_S \cdot u = f_S \cdot [cm] = \left[a \prod_{s \in S} \left(f - f^{ms^{-1}}\right) m\right].$$

Since nonunit elements $ms^{-1}, s \in S$ act nontrivially on Γ, there exists $f \in \Gamma^1$ such that $f_S \cdot u$ is nonzero. Then

$$[bm] := f_S \cdot u = \sum_{i=0}^{|S|} T_i u f^{|S|-i}, \quad \text{where } T_i = \sum_{\substack{T \subset S \\ T = \{t_1, \dots, t_i\}}} f^{t_1} \dots f^{t_i} \in \Gamma.$$

Note that all f^t, $t \in S$, belong to a finite dimensional space V generated by $\{\psi \Gamma_1 \mid \psi \in \mathcal{M}\} \subset \bar{\Gamma}$. Hence all T_i-th belong to the finite dimensional space $V(k) = \Gamma \cap \sum_{i=0}^{k} \underbrace{V \cdot \dots \cdot V}_{i}$. Denote C_k the maximal degree of elements from $V(k)$. Then

$$\deg[bm] \leqslant \max\left\{\deg T_i u f^{|S|-i} \;\middle|\; i = 0, \dots, |S|\right\} \leqslant C_k + \deg u + |S|.$$

Hence we can set $t(k) = k + C_k$.

To prove (3) consider $x = [cm] \in U_{N(i)}$, $m \in \mathcal{M}_i$. By (1) for given $\varphi_i \in \mathcal{M}_1$ there exists $y \in U_{N(i)+d}$ such that $\varphi m \in \operatorname{supp} y$ and $\operatorname{supp} y \leqslant |G|$. Then by (2) $U_{N(i)+d+t(|G|)}$ contains an element of the form $[b\varphi_i m]$, hence $N(i+1) - N(i) \leqslant d + t(|G|)$. $\square$

Now we are in the position to prove Theorem 6.1. Let $D = d + t(|G|)$. The space U_1 contains elements $[a_i\varphi_i]$, where φ_i runs over $\mathcal{M}_1/G$. Then, by Lemma 6.2, (3), $U_{D(N-1)+1}$ contains a set of the form $\tilde{\mathcal{M}}_N = \{[c_m m] \mid m \in \mathcal{M}_N,\ c_m \neq 0\}$, hence $U_{D(N-1)+N+1}$ contains $\Gamma_N \tilde{\mathcal{M}}_N$. All elements from $\Gamma_N \tilde{\mathcal{M}}_N$ are linearly independent over $\Bbbk$. But the set $B_N(\Gamma[\mathcal{M}]/G)$ is embedded into $\Gamma_N \tilde{\mathcal{M}}_N$ by setting $\gamma[w] \mapsto \gamma[c_w w]$, $\gamma \in \Gamma_N$, $w \in \mathcal{M}_{N+1}$. Therefore,

$$d_U\big(D(N-1) + N + 1\big) = d_U\big(N(D+1) - D + 1\big) \geqslant \big|B_N\big(\Gamma[\mathcal{M}]/G\big)\big| \geqslant \frac{1}{|G|}\big|B_N\big(\Gamma[\mathcal{M}]\big)\big|.$$

It remains to set $p = D + 1$, $q = 1 - D$, $C = \frac{1}{|G|}$ and apply Lemma 6.1. $\square$

7. Examples of Galois rings and orders

7.1. Generalized Weyl algebras

Let σ be an automorphism of Γ of infinite order, X and Y generators of the bimodules $\Gamma_{\sigma^{-1}}$ and Γ_σ respectively, $V = \Gamma_{\sigma^{-1}} \oplus \Gamma_\sigma$, $G = \{e\}$ and $\mathcal{M}$ is the cyclic group generated by σ. Consider a Galois order U in $K * \mathcal{M}$ which is the image of some homomorphism $\tau : \Gamma[V] \to K * \mathcal{M}$ of the form

$\tau(X) = a_X b_X^{-1}\sigma$, $\tau(Y) = a_Y b_Y^{-1}\sigma^{-1}$ for some $a_X, b_X, a_Y, b_Y \in \Gamma \setminus \{0\}$. We can assume $a_X = b_X = 1$. The element $a = a_Y b_Y^{-1}$ defines a 2-cocycle $\xi : \mathbb{Z} \times \mathbb{Z} \to K^*$, such that $\xi(-1, 1) = a$. The following statement is obvious.

Proposition 7.1. *U is a Galois order with respect to Γ if and only if $a \in \Gamma$. In this case U is isomorphic to a generalized Weyl algebra of rank* 1 [Ba], *i.e. the algebra generated with respect to Γ by X, Y subject to the relations*

$$X\lambda = \lambda^\sigma X, \quad \lambda Y = Y\lambda^\sigma, \quad \lambda \in \Lambda; \qquad YX = a, \quad XY = a^\sigma.$$

7.2. Filtered algebras

Let U be an associative filtered algebra over $\Bbbk$.

Theorem 7.1. *Let Γ is a finitely generated $\Bbbk$-algebra, $K \subset L$ is a finite Galois extension, $\mathcal{M} \subset \operatorname{Aut} L$ a group of finite growths, such that $\mathcal{M} \cdot \bar{\Gamma} \subset \bar{\Gamma}$. Assume U is a PBW algebra, such that $\Gamma \subset U$ and U is generated by $\Gamma, u_1, \ldots, u_k \in U$. If U is a PBW algebra, $f : U \to \mathcal{K}$ a homomorphism such that* $\operatorname{supp} f(u_1), \ldots, \operatorname{supp} f(u_n)$ *generate $\mathcal{M}$ as a monoid and if*

$$\operatorname{GKdim} \Gamma + \operatorname{growth} \mathcal{M} = \operatorname{GKdim} \operatorname{gr} U,$$

then f is an embedding and U is a Galois ring with respect to the Harish-Chandra subalgebra Γ.

Proof. Since $\bigcup_i \operatorname{supp} f(u_i)$ generates $\mathcal{M}$ as a monoid, by Proposition 4.1 $f(U)$ is a Galois Γ-ring. Also by Theorem 6.1

$$\operatorname{GKdim} f(U) \geqslant \operatorname{GKdim} \Gamma + \operatorname{growth} \mathcal{M} = \operatorname{GKdim} \operatorname{gr} U.$$

Prove that $I = \operatorname{Ker} f$ equals zero. Assume $I \neq 0$. Then

$$\operatorname{GKdim} \operatorname{gr} U > \operatorname{GKdim} \operatorname{gr} U / \operatorname{gr} I = \operatorname{GKdim} U/I = \operatorname{GKdim} f(U) \geqslant \operatorname{GKdim} \operatorname{gr} U,$$

which is a contradiction. Γ is a Harish-Chandra subalgebra in U by 5.1. □

Below in 7.2.1, Theorem 7.1 will be applied to construct examples of Galois rings.

7.2.1. General linear Lie algebras

Let $\mathfrak{gl}_n$ be the general linear Lie algebra over $\Bbbk$, e_{ij}, $i, j = 1, \ldots, n$, its standard basis, $U_n = U(\mathfrak{gl}_n)$ its universal enveloping algebra and Z_n the center of U_n. Then we have natural embeddings on the left upper corner

$$\mathfrak{gl}_1 \subset \mathfrak{gl}_2 \subset \cdots \subset \mathfrak{gl}_n \quad \text{and induced embeddings} \quad U_1 \subset U_2 \subset \cdots \subset U_n.$$

The *Gelfand–Tsetlin* subalgebra Γ in U_n is generated by $\{Z_m \mid m = 1, \ldots, n\}$, which is a polynomial algebra in $\frac{n(n+1)}{2}$ variables. Denote by K be the field of fractions of Γ. In the paper [Zh] was constructed a system of generators $\{\lambda_{ij} \mid 1 \leqslant j \leqslant i \leqslant n\}$ of Γ and the integral Galois extension $\Lambda \supset \Gamma$ with the following properties.

(1) Λ is the algebra of polynomial functions on $\mathfrak{L}$ algebra in variables $\{\lambda_{ij} \mid \ell_{ij} \in \mathbb{k},\ 1 \leqslant j \leqslant i \leqslant n\}$, $\mathfrak{L} = \operatorname{Specm} \Lambda$. An element $\ell = (\lambda_{ij} - \ell_{ij} \mid \ell_{ij} \in \mathbb{k},\ 1 \leqslant j \leqslant i \leqslant n)$ of $\mathfrak{L}$ is usually written in the form of tableaux consisting of n rows

$$\begin{array}{ccccccc} \ell_{n1} & & \ell_{n2} & & \cdots & & \ell_{nn} \\ & \ell_{n-1,1} & & \cdots & & \ell_{n-1,n-1} & \\ & & \cdots & \cdots & \cdots & & \\ & & \ell_{21} & & \ell_{22} & & \\ & & & \ell_{11} & & & \end{array} \tag{7.24}$$

(2) The product of the symmetric groups $G = \prod_{i=1}^n S_i$ acts naturally on $\mathfrak{L}$, where every S_i permutes elements of i-th row. This action induces the action of G on Λ.

(3) Γ is identified with the invariants Λ^G, such that $\gamma_{ij} = \sigma_{ij}(\gamma_{i1}, \ldots, \gamma_{ii})$ where σ_{ij} is the j-th symmetrical polynomial in i variables. Denote by L the fraction field of Λ. Then $L^G = K$ and $G = G(L/K)$ is the Galois group of the field extension $K \subset L$.

(4) Denote by $\delta_{ij} \in \mathfrak{L}$ a tableau whose ij-th element equals 1 and all other elements are 0. Let $\mathcal{M} \simeq \mathbb{Z}^{\frac{n(n-1)}{2}}$ be additive free abelian group with free generators δ^{ij}, $1 \leqslant j \leqslant i \leqslant n-1$. Analogously to (7.24) the elements of $\mathcal{M}$ are written as tableaux with zero upper row. Then $\mathcal{M}$ acts on $\mathfrak{L}$ by shifts: $\delta^{ij} \cdot \ell = \ell + \delta^{ij}$, $\delta^{ij} \in \mathcal{M}$. This action of $\mathcal{M}$ on $\mathfrak{L}$ induces the action on Λ and L, hence we can consider $\mathcal{M}$ as a subgroup in $\operatorname{Aut} L$. Note that G acts on $\mathcal{M}$ by conjugations. As in Section 4 denote $\mathcal{K} = (L * \mathcal{M})^G$.

In [Zh], Ch. X.70, Theorem 7, the Gelfand–Tsetlin formulae (in Zhelobenko form) are given for the action of generators of $\mathfrak{gl}_n$ on a Gelfand–Tsetlin basis of a finite dimensional irreducible representation. We show that these formulae in fact endow U_n with a structure of a Galois order (Proposition 7.2). We need the following corollary from the Gelfand–Tsetlin formulae (see [BL] or [DFO2]).

Theorem 7.2. *Let $\Omega \subset \mathfrak{L}$ be a set of tableaux $\ell = (\ell_{ij})$ such that $\ell_{ij} - \ell_{i'j'} \notin \mathbb{Z}$ for all possible pairs i, i', j, j', $(i, j) \neq (i', j')$. Consider a $\mathbb{k}$-vector space T_ℓ with the basis $\mathcal{M}$ and with the action of $E_k^+ = e_{k,k+1}$, $E_k^- = e_{k+1,k}$, $k = 1, \ldots, n-1$, given by the formulae*

$$E_k^{\pm} \cdot m = \sum_{i=1}^{k} a_{ki}^{\pm}(\ell)\big(m \pm \delta^{ki}\big),$$

where $m \in \mathcal{M}$ and

$$a_{ki}^{\pm}(\ell) = \mp \frac{\prod_j (\ell_{k\pm 1,j} - \ell_{ki})}{\prod_{j \neq i} (\ell_{kj} - \ell_{ki})}. \tag{7.25}$$

The action of an element $\gamma \in \Gamma$ on the basis vector $[\ell]$ is just the multiplication on $\gamma(\ell) \in \mathbb{k}$. Then the formulae above define on T_ℓ the structure of U_n-module.

Analogously to [O] we will show that the formulae above define a homomorphism of U_n to $\mathcal{K}$.

Proposition 7.2. *U_n is a Galois ring with respect to Γ. This structure is defined by the embedding $\imath : U_n \to \mathcal{K}$ where*

$$\imath(e_{k\,k+1}) = \sum_{i=1}^{k} \delta^{ki} a_{ki}^{+} = \left[\delta^{k1} a_{k1}^{+}\right], \qquad \imath(e_{k+1\,k}) = \sum_{i=1}^{k} \left(-\delta^{ki}\right) a_{ki}^{-} = \left[\left(-\delta^{k1}\right) a_{k1}^{-}\right],$$

$$a_{ki}^{\pm} = \mp \frac{\prod_j (\lambda_{k\pm 1, j} - \lambda_{ki})}{\prod_{j \neq i} (\lambda_{kj} - \lambda_{ki})}, \quad \textit{for } k = 1, \ldots, n. \tag{7.26}$$

Proof. Let S be the multiplicative $\mathcal{M}$-invariant subset in Γ, generated by $\lambda_{ij} - \lambda_{ij'} - k$ for all possible i, i', j, j' with $(i, j) \neq (i', j')$, where k running $\mathbb{Z}$, and Λ_S the corresponding localization. Then $\Lambda_S * \mathcal{M}$ has a structure of a $\Lambda_S * \mathcal{M}$-bimodule and every $\ell \in \Omega = \operatorname{Specm} \Lambda_S$ defines a left $\Lambda_S * \mathcal{M}$-module

$$V_\ell = (\Lambda_S * \mathcal{M}) \otimes_{\Lambda_S} (\Lambda_S / \ell).$$

Analogously the action from the left by elements $\sum_{i=1}^{k} (\pm \delta^{ki}) a_{ki}^{\pm}(\lambda)$, $k = 1, \ldots, n-1$, defines on $V(\ell)$ the structure of the left U_n-module, isomorphic to the module T_ℓ from Theorem 7.2. These module structures define homomorphisms of $\mathbb{k}$-algebras

$$\tau_\ell : U_n \longrightarrow \operatorname{End}_{\mathbb{k}}(V_\ell) \quad \text{and} \quad \rho_\ell : \Lambda_S * \mathcal{M} \longrightarrow \operatorname{End}_{\mathbb{k}}(V_\ell),$$

besides $\operatorname{Im} \tau_\ell \subset \operatorname{Im} \rho_\ell$. It gives us the diagonal homomorphisms of $\mathbb{k}$-algebras

$$\Delta_\tau : U_n \longrightarrow \prod_{\ell \in \Omega} \operatorname{End}_{\mathbb{k}}(V_\ell) \quad \text{and} \quad \Delta_\rho : \Lambda_S * \mathcal{M} \longrightarrow \prod_{\ell \in \Omega} \operatorname{End}_{\mathbb{k}}(V_\ell),$$

again $\operatorname{Im} \Delta_\tau \subset \operatorname{Im} \Delta_\rho$. But Δ_ρ is an embedding, since for every nonzero $x \in \Lambda_S * \mathcal{M}$ there exists V_ℓ, such that $x \cdot V_\ell \neq 0$. Hence the mappings (7.26) from Proposition 7.2 defines the homomorphism $i : U_n \to \Lambda_S * \mathcal{M}$. Note, that the elements in (7.26) belongs to $\mathcal{K}$, hence i defines $\imath : U_n \to \mathcal{K}$. To prove, that U_n is a Galois ring note, that it is a filtered algebra, $\operatorname{GKdim} U_n = n^2$ and

$$\operatorname{GKdim} \Gamma + \operatorname{growth} \mathcal{M} = \frac{n(n+1)}{2} + \frac{n(n-1)}{2} = n^2.$$

Applying Theorem 7.1 we conclude that $\imath$ is an embedding and thus U_n is a Galois ring.

Now we give two different proofs of the fact that U_n is a Galois order.

First method to prove that U_n is a Galois order is based on Proposition 5.3. Let $X = (x_{ij})$ be $n \times n$-matrix with indeterminates x_{ij}, X_k its submatrix of size $k \times k$, formed by the intersection of the first k rows and the first k columns of X, χ_{ki} $(i \leqslant k)$ i-th coefficient of the characteristic polynomial of X_k. In the case of U_n the corresponding graded algebra $\bar{U}_n$ can be identified with the polynomial algebra in the variables x_{ij}, $1 \leqslant i, j \leqslant n$ and the image of the canonical embedding $\imath : \operatorname{gr} \Gamma \hookrightarrow \operatorname{gr} U_n$ (see Proposition 5.3) is generated by χ_{ki}, $1 \leqslant k \leqslant n$; $1 \leqslant i \leqslant k$. The $\operatorname{Specm} \operatorname{gr} U_n$ in a natural way can be interpreted as the space $n \times n$ matrices. Besides the induces map $\imath^* : \operatorname{Specm} \operatorname{gr} U_n \to \operatorname{Specm} \operatorname{gr} \Gamma$ is the map

$$\mathbb{C}^{n^2} \longrightarrow \mathbb{C}^{n(n+1)/2}, \quad A \longmapsto \left(\chi_{ki}(A_k) \;\middle|\; k = 1, \ldots, n;\ i = 1, \ldots, k\right),$$

defined in [KW]. It is known, that this map is an epimorphism (see [KW], Theorem 1). Then Proposition 5.3 implies that U_n is a Galois order.

Another method is based on the paper [O1], where is was shown that the variety $(\imath^*)^{-1}(0)$ is an equidimensional variety of dimension $\frac{n(n-1)}{2}$. Further, from this fact in [FO1] it is deduced that U_n is free (both right and left) Γ-module. Applying now Corollary 5.2 we conclude that U_n is a Galois order. $\square$

Realization of U_n as a Galois order has some interesting consequences, in particular, the decomposition $\mathcal{K} \simeq \bigoplus_{\varphi \in \mathcal{M}/G} V(\varphi)$ of the localization $\mathcal{K}$ of U_n by $\Gamma \setminus \{0\}$; structure of the tensor category generated by $V(\varphi)$'s, etc. These results will be discussed elsewhere.

Remark 7.1. Realization of U_n as a Galois order is analogous to the embedding of U_n into a product of localized Weyl algebras constructed in [Kh].

Remark 7.2. The developed techniques can be used effectively in the case of finite W-algebras. Let $\mathfrak{g} = \mathfrak{gl}_m$, $f \in \mathfrak{g}$, $\mathfrak{g} = \bigoplus_{j \in \mathbb{Z}} \mathfrak{g}_j$ a *good grading* for f, i.e. $f \in \mathfrak{g}_2$ and *ad* f is injective on $\mathfrak{g}_j$ for $j \leqslant -1$ and surjective for $j \geqslant -1$. A non-degenerate invariant symmetric bilinear form (.,.) on $\mathfrak{g}$ induces a non-degenerate skew-symmetric form on $\mathfrak{g}_{-1}$ defined by $\langle x, y \rangle = ([x, y], f)$. Let $\mathcal{I} \subset \mathfrak{g}_{-1}$ be a maximal isotropic subspace and set $\mathfrak{t} = \bigoplus_{j \leqslant -2} \mathfrak{g}_j \oplus \mathcal{I}$. Let $\chi : U(\mathfrak{t}) \to C$ be the one-dimensional representation such that $x \mapsto (x, f)$ for any $x \in \mathfrak{t}$, $I_\chi = \operatorname{Ker} \chi$ and $Q_\chi = U(\mathfrak{g})/U(\mathfrak{g}) I_\chi$. Then

$$\operatorname{End}_{U(\mathfrak{g})}(Q_\chi)^{op}$$

is the finite W-algebra associated to the nilpotent element $f \in \mathfrak{g}$.

It was shown in [BK] that any finite W-algebra (of type A) is isomorphic to a certain quotient of the *shifted Yangian*. It is parametrized by a sequence $\pi = (p_1, \dots, p_n)$ with $p_1 \leqslant \dots \leqslant p_n$. We denote the corresponding W-algebra by $W(\pi)$. Let $\pi_k = (p_1, \dots, p_k)$, $k \in \{1, \dots, n\}$. Then we have the chain of subalgebras

$$W(\pi_1) \subset W(\pi_2) \subset \dots \subset W(\pi_n) = W(\pi).$$

Denote by Γ the subalgebra of $W(\pi)$ generated by the centers of $W(\pi_k)$ for $k = 1, \dots, n$.

Theorem 7.3. *(See [FMO], Theorem 6.6.) $W(\pi)$ is a Galois order with respect to Γ.*

7.3. *Rings of invariant differential operators*

In this section we construct some Galois rings of invariant differential operators on n-dimensional torus $\mathbb{k}^n \setminus \{0\}$. Let A_1 be the first Weyl algebra over $\mathbb{k}$ generated by x and ∂ and $\tilde{A}_1$ its localization by x. Denote $t = \partial x$. Then

$$\tilde{A}_1 \simeq \mathbb{k}\big[t, \sigma^{\pm 1}\big] \simeq \mathbb{k}[t] * \mathbb{Z},$$

where $\sigma \in \operatorname{Aut} \mathbb{k}[t]$, $\sigma(t) = t - 1$ and the first isomorphism is given by: $x \mapsto \sigma$, $\partial \mapsto t\sigma^{-1}$. Let $\tilde{A}_n$ be the n-th tensor power of $\tilde{A}_1$,

$$\tilde{A}_n \simeq \mathbb{k}\big[t_1, \dots, t_n, \sigma_1^{\pm 1}, \dots, \sigma_n^{\pm 1}\big] \simeq \mathbb{k}[t_1, \dots, t_n] * \mathbb{Z}^n,$$

where x_i, ∂_i are natural generators of the n-th Weyl algebra A_n, $t_i = \partial_i x_i$, $\sigma_i(t_j) = t_j - \delta_{ij}$, $i = 1, \dots, n$. Let $S = \mathbb{k}[t_1, \dots, t_n] \setminus \{0\}$. Then in particular we have

$$A_n\big[S^{-1}\big] \simeq \mathbb{k}(t_1, \dots, t_n) * \mathbb{Z}^n.$$

7.3.1. *Symmetric differential operators on a torus*

The symmetric group S_n acts naturally on $\tilde{A}_n$ by permutations. Denote $\Gamma = \mathbb{k}[t_1, \dots, t_n]^{S_n}$. Then we immediately have

Proposition 7.3. *$\tilde{A}_n^{S_n}$ is a Galois ring with respect to Γ in $(\mathbb{k}(t_1, \dots, t_n) * \mathbb{Z}^n)^{S_n}$, where $\mathbb{Z}^n$ acts on the field of rational functions by corresponding shifts.*

7.3.2. Orthogonal differential operators on a torus

The algebra $\tilde{A}_1$ has an involution ε such that $\varepsilon(x) = x^{-1}$ and $\varepsilon(\partial) = -x^2\partial$. On the other hand $\Bbbk[t]*\mathbb{Z}$ has an involution: $\sigma \mapsto \sigma$, $t \mapsto 2-t$. Then $\tilde{A}_1$ and $\Bbbk[t]*\mathbb{Z}$ are isomorphic as involutive algebras and the isomorphism is given by: $x \mapsto \sigma$, $\partial \mapsto t\sigma^{-1} + 1 - \sigma^{-2}$. Similarly we have an isomorphism of involutive algebras $\tilde{A}_n \simeq \Bbbk[t_1, \dots, t_n, \sigma_1^{\pm 1}, \dots, \sigma_n^{\pm 1}]$ and $\Bbbk[t_1, \dots, t_n] * \mathbb{Z}^n$.

Let W_n be the Weyl group of the orthogonal Lie algebra $\mathcal{O}_n$. If $n = 2p+1$ then the group $W_{2p+1} = S_p \ltimes \mathbb{Z}_2^p$ acts on $\tilde{A}_p$ where S_p acts by the permutations of the components and the normal subgroup $\mathbb{Z}_2^p$ is generated by the involutions described above. Consider a homomorphism $\tau : \mathbb{Z}_2^p \to \mathbb{Z}_2$ such that $(g_1, \dots, g_p) \mapsto g_1 + \dots + g_p$ and let $N = \operatorname{Ker} \tau \simeq \mathbb{Z}_2^{p-1}$. If $n = 2p$ then $W_{2p} \simeq S_p \ltimes N$ with a natural action on $\tilde{A}_p$. These actions induce an action of W_n on $\Bbbk(t_1, \dots, t_n) * \mathbb{Z}^n$ for any n. Let $\Gamma = \Bbbk[t_1, \dots, t_n]^{W_n}$. Then we immediately have

Proposition 7.4. *Algebra* $\tilde{A}_n^{W_n}$ *of* orthogonal differential operators on a torus *is a Galois ring with respect to Γ in $(\Bbbk(t_1, \dots, t_n) * \mathbb{Z}^n)^{W_n}$, where $\mathbb{Z}^n$ acts on the field of rational functions by corresponding shifts.*

7.4. Galois orders of finite rank

The following example provides a link between the theory of Galois orders and the theory of orders in the classical sense.

Let Λ be a commutative domain integrally closed in its fraction field L, $\mathcal{G} \subset \operatorname{Aut} L$ a finite subgroup, which splits into a semi-direct product of its subgroups $\mathcal{G} = G \ltimes \mathcal{M}$. Denote $\Gamma = \Lambda^G$ and $K = L^G$. Then Λ is just the integral closure of Γ in L and the action of G on $L * \mathcal{M}$ is defined. A Galois order $U \subset \mathcal{K}$ with respect to Γ will be called a *Galois order of finite rank*.

Proposition 7.5. *Let $U \subset \mathcal{K}$ be a Galois algebra of finite rank with respect to Γ and $E = L^{\mathcal{G}}$. Then $\mathcal{K}$ is a simple central algebra over E and* $\dim_E \mathcal{K} = |\mathcal{M}|^2$.

Proof. Theorem 4.1, (4) gives the statement about the center, while Corollary 4.2 gives the statement about the simplicity. From (2.1), (2.6) and Section 2.3 we obtain

$$\dim_K \mathcal{K} = \sum_{\varphi \in \mathcal{M}/G} \dim_K (K * \mathcal{M})_\varphi^G = \sum_{\varphi \in \mathcal{M}/G} |\mathcal{O}_\varphi| = |\mathcal{M}| \tag{7.27}$$

both as a left and as a right K-space structure. On other hand, $\dim_E K = |\mathcal{M}|$, that completes the proof. □

Acknowledgments

The first author is supported in part by the CNPq grant (processo 301743/2007-0) and by the Fapesp grant (processo 2005/60337-2). The second author is grateful to Fapesp for the financial support (processos 2004/02850-2 and 2006/60763-4) and to the University of São Paulo for the hospitality during his visits.

References

[Ba] V. Bavula, Generalized Weyl algebras and their representations, Algebra i Analiz 4 (1992) 75–97. English translation: St. Petersburg Math. J. 4 (1993) 71–92.
[BavO] V. Bavula, F. Oystaeyen, Simple Modules of the Witten–Woronowicz algebra, J. Algebra 271 (2004) 827–845.
[Bl] R. Block, The irreducible representations of the Lie algebra *sl*(2) and of the Weyl algebra, Adv. Math. 39 (1981) 69–110.
[BL] D.J. Britten, F.W. Lemire, Irreducible representations of an with a 1-dimensional weight space, Trans. Amer. Math. Soc. 273 (1983) 509–540.
[BK] J. Brundan, A. Kleshchev, Representations of shifted Yangians and finite W-algebras, Mem. Amer. Math. Soc. 196 (918) (2008), 107 pp.

[DFO1] Yu.A. Drozd, S.A. Ovsienko, V.M. Futorny, On Gelfand–Zetlin modules, Rend. Circ. Mat. Palermo Suppl. 26 (1991) 143–147.
[DFO2] Yu. Drozd, S. Ovsienko, V. Futorny, Harish-Chandra subalgebras and Gelfand–Zetlin modules, in: Finite Dimensional Algebras and Related Topics, in: NATO ASI Ser. C., Math. Phys. Sci., vol. 424, 1994, pp. 79–93.
[DK] Yu.A. Drozd, V.V. Kirichenko, Finite Dimensional Algebras, with appendix by Vlastimil Dlab, Springer-Verlag, Berlin, 1994, 249 pp.
[Ex] R. Exel, Partial actions of groups and actions of inverse monoids, Proc. Amer. Math. Soc. 126 (1998) 3481–3494.
[FMO] V. Futorny, A. Molev, S. Ovsienko, Harish-Chandra modules for Yangians, Repr. Theory AMS 9 (2005) 426–454.
[FMO1] V. Futorny, A. Molev, S. Ovsienko, The Gelfand–Kirillov Conjecture and Gelfand–Tsetlin modules for finite W-algebras, Adv. Math. 223 (2010) 773–796.
[FO] V. Futorny, S. Ovsienko, Galois algebras I: Structure theory, RT-MAT 2006-13, 52 p.
[FO1] V. Futorny, S. Ovsienko, Kostant's theorem for special filtered algebras, Bull. Lond. Math. Soc. 37 (2005) 1–13.
[FO2] V. Futorny, S. Ovsienko, Fibers of characters in Harish-Chandra categories, arXiv:math/0610071.
[GTs] I.M. Gelfand, M.S. Tsetlin, Finite dimensional representations of the group of unimodular matrices, Doklady Akad. Nauk SSSR 71 (1950) 1017–1020.
[HGK] M. Hazewinkel, N. Gubareni, V.V. Kirichenko, Algebras, Rings and Modules, I, Math. Appl., Kluwer A.P., Dordrecht, Boston, London, 2004.
[Kh] A. Khomenko, Some applications of Gelfand–Zetlin modules, in: Representations of Algebras and Related Topics, in: Fields Inst. Commun., vol. 45, Amer. Math. Soc., Providence, RI, 2005, pp. 205–213.
[KW] B. Kostant, N. Wallach, Gelfand–Zeitlin theory from the perspective of classical mechanics, I, in: Studies in Lie Theory Dedicated to A. Joseph on His Sixtieth Birthday, in: Progr. Math., vol. 243, 2006, pp. 319–364.
[Kr] A. Krieg, Hecke algebras, Mem. Amer. Math. Soc. 87 (435) (1990).
[Mat] H. Matsumura, Commutative Ring Theory, Cambridge Stud. Adv. Math., vol. 8, Cambridge University Press, 1997.
[MCR] J.C. McConnell, J.C. Robson, Noncommutative Noetherian Rings, Wiley, Chichester, 1987.
[OV] A. Okunkov, A. Vershik, A new approach to representation theory of symmetric groups, Selecta Math. (N.S.) 2 (1996) 581–605.
[O] S. Ovsienko, Finiteness statements for Gelfand–Tsetlin modules, in: Algebraic Structures and Their Applications, Math. Inst., Kiev, 2002.
[O1] S. Ovsienko, Strongly nilpotent matrices and Gelfand–Tsetlin modules, Linear Algebra Appl. 365 (2003) 349–367.
[Zh] D.P. Zhelobenko, Compact Lie Groups and Their Representations, Nauka, Moscow, 1970; Transl. Math. Monogr., vol. 40, Amer. Math. Soc., Providence, RI, 1973.