Algebra & Number Theory

Volume 2

2008

No. 4

msp

Algebra & Number Theory

www.jant.org

PRODUCTION

ant@mathscipub.org

Paulo Ney de Souza, Production Manager

Silvio Levy, Senior Production Editor

See inside back cover or www.jant.org for submission instructions.

The subscription price for 2008 is US $120/year for the electronic version, and $180/year for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory (ISSN 1937-0652) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY
mathematical sciences publishers
http://www.mathscipub.org
A NON-PROFIT CORPORATION
Typeset in LaTeX

ALGEBRA AND NUMBER THEORY 2:4(2008)

Root systems and the quantum cohomology of ADE resolutions

Jim Bryan and Amin Gholampour

We compute the $\mathbb{C}^*$-equivariant quantum cohomology ring of Y, the minimal resolution of the DuVal singularity $\mathbb{C}^2/G$ where G is a finite subgroup of $SU(2)$. The quantum product is expressed in terms of an ADE root system canonically associated to G. We generalize the resulting Frobenius manifold to nonsimply laced root systems to obtain an n parameter family of algebra structures on the affine root lattice of any root system. Using the Crepant Resolution Conjecture, we obtain a prediction for the orbifold Gromov–Witten potential of $[\mathbb{C}^2/G]$.

1. Introduction

1.1. ***Overview.*** Let G be a finite subgroup of $SU(2)$, and let

$$Y \to \mathbb{C}^2/G$$

be the minimal resolution of the corresponding DuVal singularity. The classical McKay correspondence describes the geometry of Y in terms of the representation theory of G [McKay 1980; Gonzalez-Springberg and Verdier 1983; Reid 2002].

The geometry of Y gives rise to a Dynkin diagram of ADE type. The nodes of the diagram correspond to the irreducible components of the exceptional divisor of Y. Two nodes have a connecting edge if and only if the corresponding curves intersect.

Associated to every Dynkin diagram of ADE type is a simply laced root system. In this paper, we describe the $\mathbb{C}^*$-equivariant quantum cohomology of Y in terms of the associated root system. This provides a quantum version of the classical McKay correspondence.

1.2. ***Results.*** The set $\{E_1, \dots, E_n\}$ of irreducible components of the exceptional divisor of Y forms a basis of $H_2(Y, \mathbb{Z})$. The intersection matrix $E_i \cdot E_j$ defines a perfect pairing on $H_2(Y, \mathbb{Z})$. Let R be the simply laced root system associated to the Dynkin diagram of Y. We can identify $H_2(Y, \mathbb{Z})$ with the root lattice of R in a

MSC2000: 14N35.

Keywords: quantum cohomology, root system, ADE.

way so that $E_1, \dots, E_n$ correspond to simple roots $\alpha_1, \dots, \alpha_n$ and the intersection matrix is minus the Cartan matrix

$$E_i \cdot E_j = -\langle \alpha_i, \alpha_j \rangle.$$

Using the above pairing, we identify $H^2(Y, \mathbb{Z})$ with $H_2(Y, \mathbb{Z})$ (and hence with the root lattice). Since the scalar action of $\mathbb{C}^*$ on $\mathbb{C}^2$ commutes with the action of G, $\mathbb{C}^*$ acts on $\mathbb{C}^2/G$ and this action lifts to an action on Y. The cycles $E_1, \dots, E_n$ are $\mathbb{C}^*$ invariant, and so the classes $\alpha_1, \dots, \alpha_n$ have natural lifts to equivariant (co)homology. Additively, the equivariant quantum cohomology ring is thus a free module generated by the classes $\{1, \alpha_1, \dots, \alpha_n\}$. The ground ring is

$$\mathbb{Z}[t][\![q_1, \dots, q_n]\!]$$

where t is the equivariant parameter and $q_1, \dots, q_n$ are the quantum parameters associated to the curves $E_1, \dots, E_n$. So additively we have

$$QH^*_{\mathbb{C}^*}(Y) \cong H^*(Y, \mathbb{Z}) \otimes \mathbb{Z}[t][\![q_1, \dots, q_n]\!].$$

We extend the pairing $\langle \cdot, \cdot \rangle$ to a

$$\mathbb{Q}[t, t^{-1}][\![q_1, \dots, q_n]\!]$$

valued pairing on $QH^*_{\mathbb{C}^*}(Y)$ by making 1 orthogonal to α_i and setting

$$\langle 1, 1 \rangle = \frac{-1}{t^2 |G|}.$$

The product structure of $QH^*_{\mathbb{C}^*}(Y)$ is determined by our main theorem:

Theorem 1. *Let $v, w \in H^2(Y, \mathbb{Z})$ which we identify with the root lattice of R as above. Then the quantum product of v and w is given by*

$$v \star w = -t^2 |G| \, \langle v, w \rangle + \sum_{\beta \in R^+} \langle v, \beta \rangle \, \langle w, \beta \rangle \, t \, \frac{1 + q^\beta}{1 - q^\beta} \, \beta,$$

where the sum is over the positive roots of R and for $\beta = \sum_{i=1}^n b_i \, \alpha_i$, q^β is defined by

$$q^\beta = \prod_{i=1}^n q_i^{b_i}.$$

The quantum product satisfies the Frobenius condition

$$\langle v \star w, u \rangle = \langle v, w \star u \rangle \, ,$$

making $QH^*_{\mathbb{C}^*}(Y)$ a Frobenius algebra over $\mathbb{Q}[t, t^{-1}][\![q_1, \dots, q_n]\!]$.

Note that by a standard fact in root theory [Bourbaki 1968, VI.1.1 Proposition 3 and V.6.2 Corollary to Theorem 1], the formula in Theorem 1 can alternatively be written as

$$v \star w = \sum_{\beta \in R^+} \langle v, \beta \rangle \langle w, \beta \rangle \Big(-t^2 \frac{|G|}{h} + t \frac{1+q^\beta}{1-q^\beta} \beta \Big),$$

where $h = \frac{|R|}{n}$ is the Coxeter number of R.

We remark that we can regard $H^0(Y) \oplus H^2(Y)$ as the root lattice for the affine root system and consequently, we can regard $QH^*_{\mathbb{C}^*}(Y)$ as defining a family of algebra structures on the affine root lattice depending on variables $t, q_1, \dots, q_n$. We also remark that even though the product in Theorem 1 is expressed purely in terms of the root system, we know of no root theoretic proof of associativity, even in the "classical" limit $q_i \to 0$.

In Section 4, which can be read independently from the rest of this paper, we will generalize our family of algebras to root systems which are not simply-laced (Theorem 6). We will prove associativity of the product in the nonsimply laced case by reducing it to the simply laced case. Our formula also allows us to prove that the action of the Weyl group induces automorphisms of the Frobenius algebra (Corollary 7).

Our theorem is formulated as computing *small* quantum cohomology, but since the cohomology of Y is concentrated in degree 0 and degree 2, the large and small quantum cohomology rings contain equivalent information. The proof of Theorem 1 requires the computations of genus 0 equivariant Gromov–Witten invariants of Y. This is done in Section 2.

In Section 5, we use the Crepant Resolution Conjecture [Bryan and Graber 2008] and our computation of the Gromov–Witten invariants of Y, to obtain a prediction for the orbifold Gromov–Witten potential of $[\mathbb{C}^2/G]$ (Conjecture 11).

1.3. ***Relationship to other work.*** A certain specialization of the Frobenius algebra $QH^*_{\mathbb{C}^*}(Y)$ appears as the quantum cohomology of the G-Hilbert scheme resolution of $\mathbb{C}^3/G$ for $G \subset SO(3)$ [Bryan and Gholampour 2008]. The equivariant Gromov–Witten theory of Y in higher genus has been determined by recent work of Maulik [2008].

2. Gromov–Witten theory of Y

In this section we compute the equivariant genus zero Gromov–Witten invariants of Y. The invariants of nonzero degree are computed by relating them to the invariants of a certain threefold W constructed as the total space of a family of deformations of Y. The invariants of W are computed by the method of

Bryan, Katz, and Leung [2001]. The degree zero invariants are computed by localization.

2.1. ***Invariants of nonzero degree.*** $\mathrm{Def}\,(Y)$, the versal space of $\mathbb{C}^*$-equivariant deformations of Y, is naturally identified with the complexified root space of the root system R [Katz and Morrison 1992]. A generic deformation of Y is an affine variety and consequently has no compact curves. The hyperplane $D_\beta \subset \mathrm{Def}\,(Y)$ perpendicular to a positive root

$$\beta = \sum_{i=1}^{n} b_i \alpha_i$$

parameterizes those deformations of Y for which the curve

$$b_1 E_1 + \cdots + b_n E_n$$

also deforms. Moreover, for a generic point $t \in D_\beta$, the corresponding curve is a smooth $\mathbb{P}^1$ which generates the Picard group of the corresponding surface [Katz and Morrison 1992, Theorem 1; Bryan et al. 2001, Proposition 2.2].

Let

$$\iota : \mathbb{C} \to \mathrm{Def}\,(Y)$$

be a generic linear subspace. We obtain a threefold W by pulling back the universal family over $\mathrm{Def}\,(Y)$ by ι. The embedding ι can be made $\mathbb{C}^*$-equivariant by defining the action on $\mathbb{C}$ to have weight 2. This follows from [Katz and Morrison 1992, Theorem 1] after noting that the $\mathbb{C}^*$ action in that paper is the square of the action induced by the action on $\mathbb{C}^2/G$. Clearly $Y \subset W$ and the normal bundle $N_{Y/W}$ is isomorphic to $\mathcal{O}_Y$. However, the action of $\mathbb{C}^*$ is nontrivial of weight two and hence it has a nontrivial Chern class in equivariant cohomology:

$$c_1(N_{Y/W}) = 2t$$

(recall that t is the equivariant parameter).

The threefold W is Calabi–Yau and its Gromov–Witten invariants are well defined in the nonequivariant limit. This assertion follows from the fact that the moduli space of stable maps to W is compact. This in turn follows from the fact that W admits a birational map

$$W \to W_{\mathrm{aff}}$$

contracting $E_1 \cup \cdots \cup E_n$ such that W_{aff} is an affine variety [Katz and Morrison 1992; Bryan et al. 2001]. Consequently, all nonconstant stable maps to W must have image contained in the exceptional set of $W \to W_{\mathrm{aff}}$ and thus, in particular, all nonconstant stable maps to W have their image contained in Y.

There is a standard technique in Gromov–Witten theory for comparing the virtual class for stable maps to a submanifold to the virtual class for the stable maps to the ambient manifold when all the maps have image contained in the submanifold [Behrend and Fantechi 1997]. This allows us to compare the Gromov–Witten invariants of W and Y.

For any nonzero class

$$A \in H_2(Y) \cong H_2(W),$$

let

$$\langle\ \rangle^Y_A \quad \text{and} \quad \langle\ \rangle^W_A$$

denote the genus zero, degree A, zero insertion Gromov–Witten invariant of Y and W respectively. We have

$$\langle\ \rangle^W_A = \int_{[\overline{M}_{0,0}(Y,A)]^{vir}} e(-R^{\bullet}\pi_* f^* N_{Y/W})$$

where $\overline{M}_{0,0}(Y, A)$ is the moduli space of stable maps, $\pi : C \to \overline{M}_{0,0}(Y, A)$ is the universal curve, $f : C \to Y$ is the universal map, and e is the equivariant Euler class.

Since the line bundle $N_{Y/W}$ is trivial up to the $\mathbb{C}^*$ action, and π is a family of genus zero curves, we get

$$R^{\bullet}\pi_* f^* N_{Y/W} = R^0\pi_* f^* N_{Y/W} = \mathbb{O} \otimes \mathbb{C}_{2t}$$

where $\mathbb{C}_{2t}$ is the $\mathbb{C}^*$ representation of weight 2 so that we have

$$c_1(\mathbb{O} \otimes \mathbb{C}_{2t}) = 2t.$$

Consequently, we have

$$e(-R^{\bullet}\pi_* f^* N_{Y/W}) = \frac{1}{2t}$$

and so

$$\begin{aligned}\langle\ \rangle^W_A &= \int_{[\overline{M}_{0,0}(Y,A)]^{vir}} \frac{1}{2t}\\ &= \frac{1}{2t}\langle\ \rangle^Y_A .\end{aligned}$$

To compute $\langle\ \rangle^W_A$, we use the deformation invariance of Gromov–Witten invariants. Although W is noncompact, the moduli space of stable maps is compact, and the deformation of W is done so that the stable map moduli spaces are compact throughout the deformation. The technique is identical to the deformation argument used in [Bryan et al. 2001] where it is presented in greater detail.

We deform W to a threefold W' as follows. Let

$$\iota' : \mathbb{C} \to \mathrm{Def}\,(Y)$$

be a generic affine linear embedding and let W' be the pullback by ι' of the universal family over $\operatorname{Def}(Y)$. The threefold W' is a deformation of W since ι' is a deformation of ι.

Lemma 2. *The compact curves of W' consist of isolated $\mathbb{P}^1$s, each having normal bundle*

$$\mathcal{O}(-1) \oplus \mathcal{O}(-1),$$

one in each homology class $\beta \in H_2(W') \cong H_2(Y)$ corresponding to a positive root.

Proof. The map ι' intersects each hyperplane D_β transversely in a single generic point t. The surface S_t over the point t contains a single curve $C_t \cong \mathbb{P}^1$ of normal bundle $N_{C_t/S_t} \cong \mathcal{O}(-2)$ and this curve is in the class β. There is a short exact sequence

$$0 \to N_{C_t/S_t} \to N_{C_t/W'} \to \mathcal{O} \to 0$$

and since ι' intersects D_β transversely, C_β does not have any deformations (even infinitesimally) inside W'. Consequently, we must have

$$N_{C_\beta/W'} \cong \mathcal{O}(-1) \oplus \mathcal{O}(-1). \qquad \square$$

Since all the curves in W' are isolated $(-1,-1)$ curves, we can compute the Gromov–Witten invariants of W' using the Aspinwall–Morrison multiple cover formula. Combined with the deformation invariance of Gromov–Witten invariants, we obtain

Lemma 3. *For $A \neq 0$ we have*

$$\langle\ \rangle^Y_A = 2t\,\langle\ \rangle^W_A = 2t\,\langle\ \rangle^{W'}_A = \begin{cases} 2t\dfrac{1}{d^3} & \text{if } A = d\beta \text{ where } \beta \text{ is a positive root,} \\ 0 & \text{otherwise.} \end{cases}$$

Since all the cohomology of Y is in $H^0(Y)$ and $H^2(Y)$, the n-point Gromov–Witten invariants of nonzero degree are determined from the 0-point invariants by the divisor and the fundamental class axioms.

2.2. *Degree 0 invariants.* The only nontrivial degree zero invariants have 3 insertions and are determined by classical integrals on Y. They are given in the following lemma.

Lemma 4. *Let 1 be the generator of $H^0_{\mathbb{C}^*}(Y)$ and let $\{\alpha_1, \dots, \alpha_n\}$ be the basis for $H^2_{\mathbb{C}^*}(Y)$ which is also identified with the simple roots of R as in Section 1. Then the* *degree* 0, 3*-point Gromov–Witten invariants of Y are given as follows*:

$$\langle 1,1,1\rangle_0 = \frac{1}{t^2|G|}, \tag{2-1}$$

$$\langle \alpha_i,1,1\rangle_0 = 0, \tag{2-2}$$

$$\langle \alpha_i,\alpha_j,1\rangle_0 = -\langle \alpha_i,\alpha_j\rangle, \tag{2-3}$$

$$\langle \alpha_i,\alpha_j,\alpha_k\rangle_0 = -t \sum_{\beta\in R^+} \langle \alpha_i,\beta\rangle\langle \alpha_j,\beta\rangle\langle \alpha_k,\beta\rangle. \tag{2-4}$$

Proof. The degree zero, genus zero, 3-point Gromov–Witten invariants are given by integrals over Y:

$$\langle x,y,z\rangle_0 = \int_Y x\cup y\cup z.$$

Because Y is noncompact, the integral must be defined[1] via $\mathbb{C}^*$ localization and takes values in $\mathbb{Q}[t,t^{-1}]$, the localized equivariant cohomology ring of a point:

$$\begin{aligned} \int_Y :\quad & H^*_{\mathbb{C}^*}(Y) \longrightarrow \mathbb{Q}[t,t^{-1}],\\ & \phi \mapsto \int_F \frac{\phi|_F}{e(N_{F/Y})}. \end{aligned}$$

Here $F\subset Y$ is the (compact) fixed point locus of the action of $\mathbb{C}^*$ on Y.

By correspondence of residues [Bertram 2000], integrals over Y can be computed by first pushing forward to $\mathbb{C}^2/G$ followed by (orbifold) localization on $\mathbb{C}^2/G$. Equation (2-1) follows immediately:

$$\int_Y 1 = \int_{\mathbb{C}^2/G} 1 = \frac{1}{t^2|G|}.$$

The factor t^2 is the equivariant Euler class of the normal bundle of $[0/G]\subset[\mathbb{C}^2/G]$ and the factor $\frac{1}{|G|}$ accounts for the automorphisms of the point $[0/G]$.

Let $L_i\to Y$ be the $\mathbb{C}^*$ equivariant line bundle with

$$c_1(L_i)=\alpha_i.$$

Since α_i was defined to be dual to E_i via the intersection pairing, we have

$$\int_{E_j} c_1(L_i) = E_i\cdot E_j = -\langle \alpha_i,\alpha_j\rangle.$$

[1] This method of defining the Gromov–Witten invariants of a noncompact space does not affect the desired properties of quantum cohomology: the associativity still holds and the Frobenius structure still exists with the novelty that the pairing takes values in the ring $\mathbb{Q}[t,t^{-1}]$. See [Bryan and Graber 2008, section 1.4], for a discussion.

Computing the left hand side using localization, we see that the weight of the $\mathbb{C}^*$ action on L_i at a fixed point $p \in E_i$ must be the same as the weight of the $\mathbb{C}^*$ action on the normal bundle $N_{E_i/Y}$ at p, and the weight of the action on L_i is 0 over fixed points not on E_i.

Equations (2-3) and (2-2) then easily follow from localization.

To prove (2-4), we compute the left hand side by localization to get

$$\langle \alpha_i, \alpha_j, \alpha_k \rangle_0 = \begin{cases} 0 & \text{if } E_i \cup E_j \cup E_k = \varnothing, \\ -8t & \text{if } i = j = k, \\ w_{ijj} & \text{if } i \neq j = k \text{ and } E_i \cup E_j \neq \varnothing \end{cases}$$

where

$$w_{ijj} = c_1(N_{E_j/Y}|_{p_{ij}})$$

is the weight of the $\mathbb{C}^*$ action on the normal bundle of E_j at the point $p_{ij} = E_i \cup E_j$.

The normal weights w_{ijj} satisfy the following three conditions:

(1) Since K_Y is the trivial bundle with a $\mathbb{C}^*$ action of weight $2t$, the sum of the normal weights at $p = E_i \cap E_j$ is $2t$ and so

$$w_{ijj} + w_{jii} = 2t \quad \text{when } E_i \cap E_j \neq \varnothing \text{ and } i \neq j.$$

(2) Since E_i is $\mathbb{C}^*$ invariant, the sum of the tangent weights of any two distinct fixed points on E_i is zero. Combined with the above, we see that the sum of the normal weights at any two distinct fixed points is $4t$ so

$$w_{ikk} + w_{jkk} = 4t \quad \text{when } E_i \cap E_k \neq \varnothing,\ E_j \cap E_k \neq \varnothing, \text{ and } i \neq j \neq k.$$

(3) Since automorphisms of the Dynkin diagrams induce equivariant automorphisms of Y, the normal weights are invariant under such automorphisms.

The normal weights are completely determined by the above three conditions. Indeed, it is clear that once one normal weight is known, then properties (1) and (2) determine the rest. Moreover, in the case of Dynkin diagrams of type D_n or E_n, the curve corresponding to the trivalent vertex of the Dynkin graph must be fixed by $\mathbb{C}^*$ and so its tangent weights are zero. In the A_n case, condition (3) provides the needed extra equation.

To summarize the above, the three point degree zero invariants $\langle \alpha_i, \alpha_j, \alpha_k \rangle_0$ satisfy the following conditions and are uniquely determined by them.

(i) $\langle \alpha_i, \alpha_j, \alpha_k \rangle_0$ is symmetric in $\{i, j, k\}$;

(ii) $\langle \alpha_i, \alpha_j, \alpha_k \rangle_0$ is invariant under any permutation of indices induced by a Dynkin diagram automorphism;

(iii) $\langle \alpha_i, \alpha_j, \alpha_k \rangle_0 = 0$ if $\langle \alpha_j, \alpha_k \rangle = 0$;

(iv) $\langle \alpha_i, \alpha_j, \alpha_k\rangle_0 = -8t$ if $i = j = k$;

(v) $\langle \alpha_i, \alpha_i, \alpha_j\rangle_0 + \langle \alpha_j, \alpha_j, \alpha_i\rangle_0 = 2t$ if $\langle\alpha_i, \alpha_j\rangle = -1$;

(vi) $\langle \alpha_i, \alpha_k, \alpha_k\rangle_0 + \langle \alpha_j, \alpha_k, \alpha_k\rangle_0 = 4t$ if $i \neq j$ and $\langle\alpha_i, \alpha_k\rangle = \langle\alpha_j, \alpha_k\rangle = -1$.

So to finish the proof of Lemma 4, it suffices to show that the right hand side of (2-4) also satisfies all the above properties. This is precisely the content of Proposition 10, a root theoretic result which we prove in Section 4. □

3. Proof of the main theorem

Having computed all the Gromov–Witten invariants of Y, we can proceed to compute the quantum product and prove our main theorem.

Proof. The quantum product $\star$ is defined in terms of the genus 0, 3-point invariants of Y by

$$-\langle x \star y, z\rangle = \sum_{A\in H_2(Y,\mathbb{Z})} \langle x, y, z\rangle_A\, q^A$$

where the strange looking minus sign is due to the fact that the pairing $\langle\,\cdot\,,\cdot\,\rangle$, which coincides with the Cartan pairing on the roots, is the negative of the cohomological pairing.

To prove our formula for $v \star w$, it suffices to check that the formula holds after pairing both sides with 1 and with any $u \in H^2(Y)$.

By definition and Lemma 4 we have

$$\begin{aligned} -\langle v \star w, 1\rangle &= \sum_{A\in H_2(Y)} \langle v, w, 1\rangle_A\, q^A \\ &= \langle v, w, 1\rangle_0 \\ &= -\langle v, w\rangle\,, \end{aligned}$$

which is in agreement with the right hand side of the formula in Theorem 1 when paired with 1 since 1 is orthogonal to $H^2(Y)$ and

$$\langle 1, 1\rangle = -\frac{1}{t^2|G|}.$$

For $u \in H^2(Y)$ we apply the divisor axiom to get

$$\begin{aligned} -\langle v \star w, u\rangle &= \sum_{A\in H_2(Y)} \langle v, w, u\rangle_A\, q^A \\ &= \langle v, w, u\rangle_0 - \sum_{A\neq 0} \langle v, A\rangle\, \langle w, A\rangle\, \langle u, A\rangle\, \langle\ \rangle_A\, q^A. \end{aligned}$$

Applying Lemmas 4 and 3 we get

$$\begin{aligned}
-\langle v\star w,u\rangle &= -t\sum_{\beta\in R^+}\langle v,\beta\rangle\,\langle w,\beta\rangle\langle u,\beta\rangle\\
&\qquad -\sum_{\beta\in R^+}\sum_{d=1}^{\infty}\langle v,d\beta\rangle\,\langle w,d\beta\rangle\,\langle u,d\beta\rangle\,\frac{2t}{d^3}q^{d\beta}\\
&= -t\sum_{\beta\in R^+}\langle v,\beta\rangle\,\langle w,\beta\rangle\,\langle u,\beta\rangle\left(1+\frac{2q^\beta}{1-q^\beta}\right)\\
&= -t\sum_{\beta\in R^+}\langle v,\beta\rangle\,\langle w,\beta\rangle\,\langle u,\beta\rangle\left(\frac{1+q^\beta}{1-q^\beta}\right).
\end{aligned}$$

Pairing the right hand side of the formula in Theorem 1 with u, we find agreement with the above and the formula for $\star$ is proved.

To prove that the Frobenius condition holds, we only need to observe that the pairing on $QH^*_{\mathbb{C}^*}(Y)$ is induced by the three point invariant with one insertion of 1:

$$-\langle x,y\rangle=\langle x,y,1\rangle_0\,.$$

This indeed follows from (2-1), (2-2), and (2-3). □

4. The algebra for arbitrary root systems

In this section we construct a Frobenius algebra QH_R associated to any irreducible, reduced root system R (Theorem 6). This section can be read independently from the rest of the paper.

4.1. ***Root system notation.*** Let R be an irreducible, reduced, rank n root system. That is,

$$R=\{R,V,\langle\cdot,\cdot\rangle\}$$

consists of a finite subset R of a real inner product space V of dimension n satisfying

(1) R spans V;

(2) if $\alpha\in R$ then $k\alpha\in R$ implies $k=\pm1$;

(3) for all $\alpha\in R$, the reflection s_α about $\alpha^\perp$, the hyperplane perpendicular to α leaves R invariant;

(4) for any $\alpha,\beta\in R$, the number $\frac{2\langle\alpha,\beta\rangle}{\langle\alpha,\alpha\rangle}$ is an integer; and

(5) V is irreducible as a representation of W, the Weyl group (that is, the group generated by the reflections s_α, for $\alpha\in R$).

We will also assume that the inner product $\langle \cdot , \cdot \rangle$ takes values in $\mathbb{Z}$ on R.

Let $\{\alpha_1, \dots, \alpha_n\}$ be a system of simple roots, namely a subset of R spanning V and such that for every $\beta = \sum_{i=1}^{n} b_i \alpha_i$ in R the coefficients b_i are either all nonnegative or all nonpositive. As is customary, we define

$$\alpha^\vee = \frac{2\alpha}{\langle \alpha, \alpha \rangle}.$$

We will also require a certain constant ϵ_R which depends on the root system and scales linearly with the inner product.

Definition 5. Let n_i be the i-th coefficient of the largest root

$$\widetilde{\alpha} = \sum_{i=1}^{n} n_i \alpha_i .$$

We define

$$\epsilon_R = \tfrac{1}{2} \langle \widetilde{\alpha}, \widetilde{\alpha} \rangle + \tfrac{1}{2} \sum_{i=1}^{n} n_i^2 \langle \alpha_i, \alpha_i \rangle .$$

Note that in the case where R is as in Section 1, namely of ADE type and the roots have a norm square of 2, then

$$\epsilon_R = 1 + \sum_{i=1}^{n} n_i^2$$

and we have that

$$\epsilon_R = |G|$$

where G is the corresponding finite subgroup of $SU(2)$. This is a consequence of the McKay correspondence, part of which implies that $1, n_1, \dots, n_n$ are the dimensions of the irreducible representations of G [Gonzalez-Sprinberg and Verdier 1983, page 411].

4.2. *The algebra QH_R.*

Let

$$H_R = \mathbb{Z} \oplus \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$$

be the affine root lattice and let QH_R be the free module over $\mathbb{Z}[t][\![q_1, \dots, q_n]\!]$ generated by $1, \alpha_1, \dots, \alpha_n$,

$$QH_R = H_R \otimes \mathbb{Z}[t][\![q_1, \dots, q_n]\!].$$

We extend the pairing $\langle \cdot , \cdot \rangle$ to a $\mathbb{Q}[t, t^{-1}][\![q_1, \dots, q_n]\!]$ valued pairing on QH_R by making 1 orthogonal to α_i and setting

$$\langle 1, 1 \rangle = \frac{-1}{t^2 \epsilon_R}.$$

For $\beta = \sum_{i=1}^{n} b_i \alpha_i$, we use the notation

$$q^{\beta} = \prod_{i=1}^{n} q_i^{b_i}.$$

Theorem 6. *Define a product operation* $\star$ *on* QH_R *by letting* 1 *be the identity and defining*

$$\alpha_i \star \alpha_j = -t^2 \epsilon_R \langle \alpha_i, \alpha_j \rangle + \sum_{\beta \in R^+} \langle \alpha_i, \beta \rangle \, \langle \alpha_j, \beta^{\vee} \rangle \, t \frac{1+q^{\beta}}{1-q^{\beta}} \beta.$$

Then the product is associative, and moreover, it satisfies the Frobenius condition

$$\langle x \star y, z \rangle = \langle x, y \star z \rangle$$

making QH_R *into a Frobenius algebra over the ring* $\mathbb{Q}[t, t^{-1}][\![q_1, \dots, q_n]\!]$.

Corollary 7. *The Weyl group acts on* QH_R (*and thus on* $QH^*_{\mathbb{C}^*}(Y)$) *by automorphisms. Namely, if we define*

$$g(q^{\beta}) = q^{g\beta}$$

for $g \in W$, *then for* $v, w \in QH_R$ *we have*

$$g(v \star w) = (gv) \star (gw).$$

Proof. Let s_k be the reflection about the hyperplane orthogonal to α_k. By [Bourbaki 1968, VI.1.6 Corollary 1], s_k permutes the positive roots other than α_k. And since the terms

$$\frac{1+q^{\beta}}{1-q^{\beta}} \beta \quad \text{and} \quad \langle \alpha_i, \beta \rangle \langle \alpha_j, \beta^{\vee} \rangle$$

remain unchanged under $\beta \mapsto -\beta$, the effect of applying s_k to the formula for $\alpha_i \star \alpha_j$ is to permute the order of the sum:

$$\begin{aligned} s_k(\alpha_i \star \alpha_j) &= -t^2 \epsilon_R \langle \alpha_i, \alpha_j \rangle + \sum_{\beta \in R^+} \langle \alpha_i, \beta \rangle \langle \alpha_j, \beta^{\vee} \rangle \, t \frac{1+q^{s_k\beta}}{1-q^{s_k\beta}} s_k\beta \\ &= -t^2 \epsilon_R \langle s_k\alpha_i, s_k\alpha_j \rangle + \sum_{\beta \in R^+} \langle \alpha_i, s_k\beta \rangle \langle \alpha_j, s_k\beta^{\vee} \rangle \, t \frac{1+q^{\beta}}{1-q^{\beta}} \beta \\ &= s_k(\alpha_i) \star s_k(\alpha_j). \end{aligned}$$

The Corollary follows. □

4.3. ***The proof of Theorem 6.*** When R is of ADE type and the pairing is normalized so that the roots have a norm square of 2, then QH_R coincides with $QH^*_{\mathbb{C}^*}(Y)$ and so Theorem 6 for this case then follows from Theorem 1.

For any R, the Frobenius condition follows immediately from the formulas for $\star$ and $\langle \cdot, \cdot \rangle$.

So what needs to be established in general is the associativity of the $\star$ product. This is equivalent to the expression

$$\mathrm{Ass}^R_{xyuv} = \frac{1}{t^2}\,\langle (x \star y) \star u, v\rangle$$

being fully symmetric in $\{x, y, u, v\}$. Written out, we have

$$\begin{aligned}\mathrm{Ass}^R_{xyuv} &= -\epsilon_R\,\langle x, y\rangle\,\langle u, v\rangle\\ &\quad + \sum_{\beta,\gamma\in R^+} \langle x,\beta\rangle\,\langle y,\beta\rangle\,\langle u,\gamma\rangle\,\langle v,\gamma\rangle\,\Big(\frac{1+q^\beta}{1-q^\beta}\Big)\Big(\frac{1+q^\gamma}{1-q^\gamma}\Big)\langle\beta^\vee,\gamma^\vee\rangle.\end{aligned}$$

Recalling that ϵ_R scales linearly with the pairing, we see that if Ass^R_{xyuv} is fully symmetric in $\{x, y, u, v\}$, then it remains so for any rescaling of the pairing.

To prove the associativity of QH_R for root systems not of ADE type, we reduce the nonsimply laced case to the simply laced case.

Let $\{R, V, \langle\cdot,\cdot\rangle\}$ be an ADE root system and let Φ be a group of *admissible automorphisms* of the Dynkin diagram. An automorphism g of a graph is admissible if there is no edge joining two vertices in the same g-orbit [Lusztig 1993, Definition 12.1.1]. We construct a new root system

$$\big\{R_\Phi, V^\Phi, \langle\cdot,\cdot\rangle_\Phi\big\}$$

as follows. A somewhat similar construction can be found in [Springer 1998, Section 10.3.1]. Let

$$V^\Phi \subset V$$

be the Φ invariant subspace equipped with $\langle\cdot,\cdot\rangle_\Phi$, the restriction of $\langle\cdot,\cdot\rangle$ to V^Φ, and let the roots of R_Φ be the Φ averages of the roots of R:

$$R_\Phi = \bigg\{\bar\alpha = \frac{1}{|\Phi|}\sum_{g\in\Phi} g\alpha,\ \alpha\in R\bigg\}.$$

Then it is easily checked that $\{R_\Phi, V^\Phi, \langle\cdot,\cdot\rangle_\Phi\}$ is an irreducible root system, specifically of type given by

R	A_{2n-1}	D_{n+1}	E_6	D_4
Φ	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_3$
R_Φ	C_n	B_n	F_4	G_2

Thus all the irreducible, reduced root systems arise in this way.

We will frequently use the fact that if $y \in V^\Phi$, then

$$\langle x, y\rangle = \langle\bar x, y\rangle$$

which easily follows from the equalities $\langle x, y\rangle = \langle gx, gy\rangle = \langle gx, y\rangle$ for $g \in \Phi$.

We will also need the following two lemmas which we will prove at the end of the section.

Lemma 8. *The constants defined in Definition 5 coincide for the root systems R and R_Φ:*

$$\epsilon_{R_\Phi} = \epsilon_R.$$

Lemma 9. *Let $\beta \in R^+$ and let $\Phi\beta$ be the Φ orbit of β. Then*

$$\sum_{\beta' \in \Phi\beta} \beta' = \overline{\beta}^\vee.$$

The simple roots of R_Φ are given by $\overline{\alpha}_i$, the averages of the simple roots of R. Thus if $I = \{1, \dots, n\}$ is the index set for the simple roots of R, then Φ acts on I and

$$J = I/\Phi$$

is the natural index set for the simple roots of R_Φ. For $[i] \in J$, we let $\overline{\alpha}_{[i]} \in R_\Phi$ denote the simple root given by $\overline{\alpha}_i$.

We specialize the variables $\{q_i\}_{i \in I}$ to variables $\{\overline{q}_{[i]}\}_{[i] \in J}$ by setting

$$q_i = \overline{q}_{[i]} \tag{4-1}$$

and it is straightforward to see that under the above specialization,

$$q^\beta = \overline{q}^{\overline{\beta}}.$$

Now let R be an ADE root system whose roots have norm square 2. Then Ass^R_{xyuv} is fully symmetric in $\{x, y, u, v\}$. We specialize the q variables to the $\overline{q}$ variables as in (4-1) and we assume that $x, y, v, u \in V^\Phi$. Then

$$\begin{aligned}
&\mathrm{Ass}^R_{xyuv} + \epsilon_R \langle x, y\rangle \langle u, v\rangle \\
&\quad = \sum_{\beta,\gamma \in R^+} \langle x, \beta\rangle \langle y, \beta\rangle \langle u, \gamma\rangle \langle v, \gamma\rangle \left(\frac{1+q^\beta}{1-q^\beta}\right)\left(\frac{1+q^\gamma}{1-q^\gamma}\right) \langle \beta^\vee, \gamma^\vee\rangle \\
&\quad = \sum_{\beta,\gamma \in R^+} \langle x, \overline{\beta}\rangle \langle y, \overline{\beta}\rangle \langle u, \overline{g}\rangle \langle v, \overline{g}\rangle \left(\frac{1+\overline{q}^{\overline{\beta}}}{1-\overline{q}^{\overline{\beta}}}\right)\left(\frac{1+\overline{q}^{\overline{g}}}{1-\overline{q}^{\overline{g}}}\right) \langle \beta, \gamma\rangle \\
&\quad = \sum_{\overline{\beta},\overline{g} \in R^+_\Phi} \langle x, \overline{\beta}\rangle \langle y, \overline{\beta}\rangle \langle u, \overline{g}\rangle \langle v, \overline{g}\rangle \left(\frac{1+\overline{q}^{\overline{\beta}}}{1-\overline{q}^{\overline{\beta}}}\right)\left(\frac{1+\overline{q}^{\overline{g}}}{1-\overline{q}^{\overline{g}}}\right) \left\langle \sum_{\beta' \in \Phi\beta} \beta', \sum_{\gamma' \in \Phi\gamma} \gamma'\right\rangle \\
&\quad = \sum_{\overline{\beta},\overline{g} \in R^+_\Phi} \langle x, \overline{\beta}\rangle_\Phi \langle y, \overline{\beta}\rangle_\Phi \langle u, \overline{g}\rangle_\Phi \langle v, \overline{g}\rangle_\Phi \left(\frac{1+\overline{q}^{\overline{\beta}}}{1-\overline{q}^{\overline{\beta}}}\right)\left(\frac{1+\overline{q}^{\overline{g}}}{1-\overline{q}^{\overline{g}}}\right) \langle \overline{\beta}^\vee, \overline{g}^\vee\rangle_\Phi \\
&\quad = \mathrm{Ass}^{R_\Phi}_{xyuv} + \epsilon_{R_\Phi} \langle x, y\rangle_\Phi \langle u, v\rangle_\Phi
\end{aligned}$$

and thus

$$\mathrm{Ass}^{R_\Phi}_{xyuv} = \mathrm{Ass}^{R}_{xyuv}$$

is fully symmetric in $\{x, y, u, v\}$ and the theorem is proved once we establish Lemmas 8 and 9.

4.4. ***Proofs of Lemmas 8 and 9.*** We prove Lemma 9 first. If β is fixed by Φ, the lemma is immediate. We claim that if β is not fixed then $\langle\beta, g\beta\rangle = 0$ for nontrivial $g \in \Phi$. For simple roots, this follows from the admissibility condition: a node is never adjacent to a node in its orbit. For other roots this can also be seen from a direct inspection of the positive roots (listed, for example, in [Bourbaki 1968, Plates I, IV–VII]). For β not fixed by Φ we then have

$$\langle\overline{\beta}, \overline{\beta}\rangle = \frac{1}{|\Phi|^2}\Big\langle\sum_g g\beta, \sum_h h\beta\Big\rangle = \frac{1}{|\Phi|^2}\sum_g \langle g\beta, g\beta\rangle = \frac{2}{|\Phi|},$$

and Lemma 9 follows.

The preceding formula generalizes to all roots $\overline{\beta}$ by

$$\langle\overline{\beta}, \overline{\beta}\rangle = 2\frac{\mathrm{stab}(\beta)}{|\Phi|},$$

where $\mathrm{stab}(\beta)$ is the order of the stabilizer of the action of Φ on β.

To prove Lemma 8 we must find the coefficients of the longest root of R_Φ. Since the longest root of R is unique, it is fixed by Φ and so it coincides with the longest root of R_Φ:

$$\overline{\widetilde{\alpha}} = \widetilde{\alpha} = \sum_{i\in I} n_i\alpha_i = \sum_{[i]\in J} n_{[i]} \sum_{i'\in\Phi i} \alpha_i = \sum_{[i]\in J} n_{[i]}\,\overline{\alpha}^\vee_{[i]} = \sum_{[i]\in J} \frac{2n_{[i]}}{\langle\overline{\alpha}_{[i]}, \overline{\alpha}_{[i]}\rangle}\overline{\alpha}_{[i]}.$$

Thus we have

$$\begin{aligned}
2\epsilon_{R_\Phi} &= \langle\overline{\widetilde{\alpha}}, \overline{\widetilde{\alpha}}\rangle + \sum_{[i]\in J}\Big(\frac{2n_{[i]}}{\langle\overline{\alpha}_{[i]}, \overline{\alpha}_{[i]}\rangle}\Big)^2\langle\overline{\alpha}_{[i]}, \overline{\alpha}_{[i]}\rangle \\
&= \langle\widetilde{\alpha}, \widetilde{\alpha}\rangle + \sum_{i\in I}\frac{\mathrm{stab}(\alpha_i)}{|\Phi|}\,\frac{4n_i^2}{\langle\overline{\alpha}_i, \overline{\alpha}_i\rangle} \\
&= \langle\widetilde{\alpha}, \widetilde{\alpha}\rangle + \sum_{i\in I} 2n_i^2 \\
&= 2\epsilon_R
\end{aligned}$$

and Lemma 8 is proved.

4.5. ***The root theoretic formula for triple intersections.*** Here we prove the root theoretic result required to finish the proof of (2-4). Recall that R is a root system of ADE type normalized so that the roots have norm square 2. We write

$$g_{ij} = \langle \alpha_i, \alpha_j \rangle.$$

Proposition 10. *Let*

$$G_{ijk} = -\sum_{\beta \in R^+} \langle \alpha_i, \beta \rangle \langle \alpha_j, \beta \rangle \langle \alpha_k, \beta \rangle .$$

(i) *G_{ijk} is symmetric in $\{i, j, k\}$.*

(ii) *G_{ijk} is invariant under any permutation of indices induced by a Dynkin diagram automorphism.*

(iii) *$G_{ijk} = 0$ if $g_{jk} = 0$.*

(iv) *$G_{ijk} = -8$ if $i = j = k$.*

(v) *$G_{iij} + G_{jji} = 2$ if $g_{ij} = -1$.*

(vi) *$G_{ikk} + G_{jkk} = 4$ if $i \neq j$ and $g_{ik} = g_{jk} = -1$.*

Proof. From the definition of G_{ijk}, properties (i) and (ii) are clearly satisfied.

Let s_k be reflection about the hyperplane perpendicular to α_k so that

$$s_k \alpha_i = \alpha_i - g_{ik} \alpha_k.$$

Since s_k permutes the positive roots other than α_k [Bourbaki 1968, VI.1.6 Corollary 1], we get the following expression for G_{ijk}:

$$\begin{aligned} G_{ijk} &= -2 g_{ik} g_{jk} g_{kk} - \sum_{\beta \in R^+} \langle \alpha_i, s_k\beta \rangle \langle \alpha_j, s_k\beta \rangle \langle \alpha_k, s_k\beta \rangle \\ &= -4 g_{ik} g_{jk} - \sum_{\beta \in R^+} \langle \alpha_i - g_{ik}\alpha_k, \beta \rangle \langle \alpha_j - g_{jk}\alpha_k, \beta \rangle \langle -\alpha_k, \beta \rangle \\ &= -4 g_{ik} g_{jk} - G_{ijk} + g_{ik} G_{jkk} + g_{jk} G_{ikk} - g_{ik} g_{jk} G_{kkk} \end{aligned}$$

and so

$$G_{ijk} = -2 g_{ik} g_{jk} + \tfrac{1}{2}(g_{ik} G_{jkk} + g_{jk} G_{ikk} - g_{ik} g_{jk} G_{kkk}). \tag{4-2}$$

Setting $i = j = k = n$ we obtain property (iv):

$$G_{nnn} = -8$$

which we can substitute back into (4-2) and then specialize $i = j = a$ to get

$$G_{aak} = 2 g_{ak}^2 + g_{ak} G_{akk}. \tag{4-3}$$

Property (iii) then follows from (4-2) and (4-3) and property (v) follows from (4-3).

For property (vi), observe that if $g_{ik} = g_{jk} = -1$ then $g_{ij} = 0$ and so $G_{ijk} = 0$ and (4-2) then simplifies to prove property (vi). □

5. Predictions for the orbifold invariants via the Crepant Resolution Conjecture

Let $G \subset SU(2)$ be a finite subgroup and let

$$\mathscr{X} = [\mathbb{C}^2/G]$$

be the orbifold quotient of $\mathbb{C}^2$ by G. Recall that

$$\pi : Y \to X$$

is the minimal resolution of X, the singular variety underlying the orbifold $\mathscr{X}$.

The Crepant Resolution Conjecture [Bryan and Graber 2008] asserts that F_Y, the genus zero Gromov–Witten potential of Y, coincides with $F_{\mathscr{X}}$, the genus zero orbifold Gromov–Witten potential of $\mathscr{X}$ after specializing the quantum parameters of Y to certain roots of unity and making a linear change of variables in the cohomological parameters.

Using the Gromov–Witten computations of Section 2, we obtain a formula for F_Y. By making an educated guess for the change of variables and roots of unity, and then applying the conjecture, we obtain a prediction for the orbifold Gromov–Witten potential of $\mathscr{X}$ (Conjecture 11). This prediction has been verified in the cases where G is $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$ in [Bryan and Graber 2008; Bryan et al. 2008; Bryan and Jiang $\geq$ 2008] respectively, and recently it has been verified for all $\mathbb{Z}_n$ by Coates, Corti, Iritani, and Tseng [Coates et al. 2007].

5.1. ***The statement of the conjecture.*** The variables of the potential function F_Y are the quantum parameters

$$\{q_1, \dots, q_n\}$$

and cohomological parameters

$$\{y_0, \dots, y_n\}$$

corresponding the generators $\{1, \alpha_1, \dots, \alpha_n\}$ for $H^*_{\mathbb{C}^*}(Y)$.

The potential function is the natural generating function for the genus 0 Gromov–Witten invariants of Y. It is defined by

$$F_Y(q_1, \dots, q_n, y_0, \dots, y_n) = \sum_{k_0,\dots,k_n} \sum_{A \in H_2(Y)} \langle 1^{k_0} \alpha_1^{k_1} \cdots \alpha_n^{k_n} \rangle_A^Y \frac{y_0^{k_0}}{k_0!} \cdots \frac{y_n^{k_n}}{k_n!} q^A.$$

The potential function for the orbifold $\mathscr{X} = [\mathbb{C}^2/G]$ depends on variables

$$\{x_0, \dots, x_n\}$$

which correspond to a basis $\{1, \gamma_1, \dots, \gamma_n\}$ of $H^*_{\mathrm{orb}}(\mathscr{X})$, the orbifold cohomology of $\mathscr{X}$. The orbifold cohomology of $[\mathbb{C}^2/G]$ has a natural basis which is indexed by conjugacy classes of G. If $g \in G$ is an element of the group, we will write $x_{[g]}$ for the variable corresponding to the conjugacy class of g. There are no curve classes in $\mathscr{X}$ and hence no quantum parameters so the potential function is given by

$$F_{\mathscr{X}}(x_0, \dots, x_n) = \sum_{k_0,\dots,k_n} \left\langle 1^{k_0} \gamma_1^{k_1} \cdots \gamma_n^{k_n} \right\rangle^{\mathscr{X}} \frac{x_0^{k_0}}{k_0!} \cdots \frac{x_n^{k_n}}{k_n!}.$$

The conjecture states that there exists roots of unity $\omega_1, \dots, \omega_n$ and an analytic continuation of F_Y to the points

$$q_i = \omega_i$$

such that the equality

$$F_Y(\omega_1, \dots, \omega_n, y_0, \dots, y_n) = F_{\mathscr{X}}(x_0, \dots, x_n)$$

holds after making a (grading preserving) linear change of variables

$$x_i = \sum_{j=0}^{n} L_i^j y_j.$$

Thus to obtain a prediction for the potential $F_{\mathscr{X}}$, we must determine the roots of unity ω_i and the change of variables matrix[2] L.

5.2. ***The prediction.*** The only nontrivial invariants involving 1 are degree zero three point invariants. We split up the potentials $F_{\mathscr{X}}$ and F_Y into terms involving x_0 and y_0 respectively and terms without x_0 and y_0 respectively.

Let F_Y^0 be the part of F_Y with nonzero y_0 terms. It follows from Lemma 4 that F_Y^0 is given by

$$F_Y^0 = \frac{1}{t^2|G|} \frac{y_0^3}{3!} - \frac{y_0}{2} \sum_{i,j=1}^{n} \langle \alpha_i, \alpha_j \rangle y_i y_j.$$

Let $F_{\mathscr{X}}^0$ be the part of $F_{\mathscr{X}}$ with nonzero x_0 terms. An easy localization computation shows that $F_{\mathscr{X}}^0$ is given by

$$F_{\mathscr{X}}^0 = \frac{1}{t^2|G|} \frac{x_0^3}{3!} + \frac{x_0}{2} \frac{1}{|G|} \sum_{g \in G, g \neq Id} x_{[g]} x_{[g^{-1}]}.$$

Since the change of variables respects the grading, the terms in F_Y which are linear and cubic in y_0 must match up with the terms in $F_{\mathscr{X}}$ which are linear and

[2] Our matrix L here is the inverse of the matrix called L in [Bryan and Graber 2008].

cubic in x_0. Consequently we must have $x_0 = y_0$ and moreover, the change of variables must take the quadratic form

$$\frac{1}{|G|}\sum_{g\in G, g\neq Id} x_{[g]}x_{[g^{-1}]} \tag{5-1}$$

to the quadratic form

$$\sum_{i,j=1}^{n} -\langle \alpha_i, \alpha_j\rangle y_i y_j. \tag{5-2}$$

We can rewrite the above quadratic form in terms of the representation theory of G using the classical McKay correspondence [1980] as follows. The simple roots $\alpha_1, \dots, \alpha_n$, which correspond to nodes of the Dynkin diagram, also correspond to nontrivial irreducible representations of G, and hence to their characters $\chi_1, \dots, \chi_n$. Under this correspondence, the Cartan paring can be expressed in terms of $\langle \cdot | \cdot \rangle$, the natural pairing on the characters of G:

$$-\langle \alpha_i, \alpha_j\rangle = \langle (\chi_V - 2)\chi_i | \chi_j\rangle = \frac{1}{|G|}\sum_{g\in G}(\chi_V(g)-2)\chi_i(g)\overline{\chi}_j(g),$$

where V is the two-dimensional representation induced by the embedding $G \subset SU(2)$.

This discussion leads to an obvious candidate for the change of variables. That is, if we substitute

$$x_{[g]} = \sqrt{\chi_V(g)-2}\,\sum_{i=1}^{n}\chi_i(g)y_i \tag{5-3}$$

into (5-1) we obtain (5-2). Since $\chi_V(g)$ is always real and less than or equal to 2, we can fix the sign of the square root by making it a positive multiple of i.

Thus we have seen that

$$F^0_Y = F^0_{\mathscr{X}}$$

under the change of variables given by (5-3) and $x_0 = y_0$. So from here on, we set $x_0 = y_0 = 0$ and deal with just the part of the potentials $F_{\mathscr{X}}$ and F_Y not involving x_0 and y_0.

We apply the divisor axiom and the computations of Section 2:

$$\begin{aligned} &F_Y(y_1, \dots, y_n, q_1, \dots, q_n) \\ &= \frac{1}{6}\sum_{i,j,k=1}^{n}\langle \alpha_i, \alpha_j, \alpha_k\rangle_0 y_i y_j y_k + \sum_{\substack{A\in H_2(Y)\\ A\neq 0}} \langle\ \rangle_A\, q^A e^{\sum_{i=1}^{n} y_i \int_A \alpha_i} \\ &= \frac{-t}{6}\sum_{i,j,k=1}^{n}\sum_{\beta\in R^+}\langle\alpha_i,\beta\rangle\,\langle\alpha_j,\beta\rangle\,\langle\alpha_k,\beta\rangle\, y_i y_j y_k + \sum_{d=1}^{\infty}\sum_{\beta\in R^+}\frac{2t}{d^3}q^{d\beta}e^{\sum_{i=1}^{n} -d\langle\alpha_i,\beta\rangle y_i}. \end{aligned}$$

Taking triple derivatives we get

$$\begin{aligned}\frac{\partial^3 F_Y}{\partial y_i \partial y_j \partial y_k} &= -t \sum_{\beta\in R^+} \langle\alpha_i,\beta\rangle\,\langle\alpha_j,\beta\rangle\,\langle\alpha_k,\beta\rangle \left(1+\frac{2q^\beta e^{\sum_i -\langle\beta,\alpha_i\rangle y_i}}{1-q^\beta e^{\sum_i -\langle\beta,\alpha_i\rangle y_i}}\right)\\ &= -t \sum_{\beta\in R^+} \langle\alpha_i,\beta\rangle\,\langle\alpha_j,\beta\rangle\,\langle\alpha_k,\beta\rangle\,\frac{1+q^\beta e^{\sum_i -\langle\beta,\alpha_i\rangle y_i}}{1-q^\beta e^{\sum_i -\langle\beta,\alpha_i\rangle y_i}}.\end{aligned}$$

We specialize the quantum parameters to roots of unity by

$$q_j = \exp\Big(\frac{2\pi i n_j}{|G|}\Big)$$

where n_j is the j-th coefficient of the largest root as in Definition 5. Note that n_j is also the dimension of the corresponding representation.

After specializing the quantum parameters, the triple derivatives of the potential F_Y can be expressed in terms of the function

$$H(u) = \frac{1}{2i}\Big(\frac{1+e^{i(u-\pi)}}{1-e^{i(u-\pi)}}\Big) = \frac{1}{2}\tan\Big(\frac{-u}{2}\Big)$$

as follows:

$$\frac{\partial^3 F_Y}{\partial y_i \partial y_j \partial y_k} = -2it \sum_{\beta\in R^+} \langle\alpha_i,\beta\rangle\,\langle\alpha_j,\beta\rangle\,\langle\alpha_k,\beta\rangle\, H(Q_\beta)$$

where for $\beta = \sum_{j=1}^n b_j\alpha_j$ we define

$$Q_\beta = \pi + \sum_{j=1}^n \Big(\frac{2\pi n_j b_j}{|G|} + i\langle\beta,\alpha_j\rangle y_j\Big).$$

It then follows that

$$F_Y(y_1,\dots,y_n) = 2t \sum_{\beta\in R^+} h(Q_\beta)$$

where $h(u)$ is a series satisfying

$$h'''(u) = \tfrac{1}{2}\tan\Big(\frac{-u}{2}\Big).$$

We can now make the change of variables given by (5-3):

$$\begin{aligned}\sum_{j=1}^n i\langle\beta,\alpha_j\rangle y_j = \sum_{j,k=1}^n ib_k\langle\alpha_k,\alpha_j\rangle y_j &= \sum_{j,k=1}^n \frac{-ib_k}{|G|}\sum_{g\in G}(\chi_V(g)-2)\,\overline{\chi}_k(g)\chi_j(g)y_j\\ &= \sum_{k=1}^n \frac{b_k}{|G|}\sum_{g\in G}\sqrt{2-\chi_V(g)}\;\,\overline{\chi}_k(g)x_{[g]}.\end{aligned}$$

Substituting this back into Q_β we arrive at our conjectural formula for $F_{\mathscr{X}}$.

Conjecture 11. *Let $F_{\mathscr{X}}(x_1,\dots,x_n)$ denote the $\mathbb{C}^*$ equivariant genus zero orbifold Gromov–Witten potential of the orbifold $\mathscr{X}=[\mathbb{C}^2/G]$ where we have set the unit parameter x_0 equal to zero. Let R be the root system associated to G as in Section 1. Then*

$$F_{\mathscr{X}}(x_1,\dots,x_n)=2t\sum_{\beta\in R^+}h(Q_\beta)$$

where $h(u)$ is a series with

$$h'''(u)=\tfrac{1}{2}\tan\Bigl(\frac{-u}{2}\Bigr)$$

and

$$Q_\beta=\pi+\sum_{k=1}^{n}\frac{b_k}{|G|}\Bigl(2\pi n_k+\sum_{g\in G}\sqrt{2-\chi_V(g)}\;\overline{\chi}_k(g)x_{[g]}\Bigr)$$

where b_k are the coefficients of $\beta\in R^+$, n_k are the coefficients of the largest root, and V is the two-dimensional representation induced by the embedding $G\subset SU(2)$.

Note that the index set $\{1,\dots,n\}$ in the above formula corresponds to

(1) simple roots of R,

(2) nontrivial irreducible representations of G, and

(3) nontrivial conjugacy classes of G.

The index of a conjugacy class containing a group element g is denoted by $[g]$. Finally note that the terms of degree less than three are ill-defined for both the potential $F_{\mathscr{X}}$ and our conjectural formula for it.

The above conjecture has been proved in the cases where G is $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$ in [Bryan and Graber 2008; Bryan et al. 2008; Bryan and Jiang $\geq$ 2008] respectively, and recently it has been verified for all $\mathbb{Z}_n$ by Coates, Corti, Iritani, and Tseng [2007].

We have also performed a number of checks of the conjecture for nonabelian G. Many of the orbifold invariants must vanish by monodromy considerations, and our conjecture is consistent with this vanishing. One can geometrically derive a relationship between some of the orbifold invariants of $[\mathbb{C}^2/G]$ and certain combinations of the orbifold invariants of $[\mathbb{C}^2/H]$ when H is a normal subgroup of G. This leads to a simple relationship between the corresponding potential functions. We have checked that this relationship is consistent with our conjecture.

References

[Behrend and Fantechi 1997] K. Behrend and B. Fantechi, "The intrinsic normal cone", *Invent. Math.* **128**:1 (1997), 45–88. MR 98e:14022 Zbl 0909.14006

[Bertram 2000] A. Bertram, "Another way to enumerate rational curves with torus actions", *Invent. Math.* **142**:3 (2000), 487–512. MR 2001m:14077 Zbl 1031.14027

[Bourbaki 1968] N. Bourbaki, *Groupes et algèbres de Lie, Chapitres IV–VI*, Actualités scientifiques et industrielles **1337**, Hermann, Paris, 1968. MR 39 #1590 Zbl 0186.33001

[Bryan and Gholampour 2008] J. Bryan and A. Gholampour, "The quantum McKay correspondence for polyhedral singularities", preprint, 2008. arXiv 0803.3766

[Bryan and Graber 2008] J. Bryan and T. Graber, "The crepant resolution conjecture", in *Algebraic Geometry* (Seattle, 2005), 2008. To appear. arXiv math.AG/0610129

[Bryan and Jiang $\geq$ 2008] J. Bryan and Y. Jiang, "The Crepant Resolution Conjecture for the orbifold $\mathbf{C}^2/\mathbf{Z}_4$". In preparation.

[Bryan et al. 2001] J. Bryan, S. Katz, and N. C. Leung, "Multiple covers and the integrality conjecture for rational curves in Calabi–Yau threefolds", *J. Algebraic Geom.* **10**:3 (2001), 549–568. MR 2002j:14047 Zbl 1045.14019

[Bryan et al. 2008] J. Bryan, T. Graber, and R. Pandharipande, "The orbifold quantum cohomology of $\mathbb{C}^2/Z_3$ and Hurwitz–Hodge integrals", *J. Algebraic Geom.* **17**:1 (2008), 1–28. MR 2357679 Zbl 1129.14075

[Coates et al. 2007] T. Coates, A. Corti, H. Iritani, and H.-H. Tseng, "The Crepant Resolution Conjecture for type A surface singularities", preprint, 2007. arXiv 0704.2034

[Gonzalez-Springberg and Verdier 1983] G. Gonzalez-Sprinberg and J.-L. Verdier, "Construction géométrique de la correspondance de McKay", *Ann. Sci. École Norm. Sup.* (4) **16**:3 (1983), 409–449. MR 85k:14019 Zbl 0538.14033

[Katz and Morrison 1992] S. Katz and D. R. Morrison, "Gorenstein threefold singularities with small resolutions via invariant theory for Weyl groups", *J. Algebraic Geom.* **1**:3 (1992), 449–530. MR 93b:14030 Zbl 0788.14036

[Lusztig 1993] G. Lusztig, *Introduction to quantum groups*, Progress in Mathematics **110**, Birkhäuser, Boston, 1993. MR 94m:17016 Zbl 0788.17010

[Maulik 2008] D. Maulik, "Gromov–Witten theory of A-resolutions", preprint, 2008, arXiv:0802.2681

[McKay 1980] J. McKay, "Graphs, singularities, and finite groups", pp. 183–186 in *The Santa Cruz Conference on Finite Groups* (Santa Cruz, 1979), edited by B. Cooperstein and G. Mason, Proc. Sympos. Pure Math. **37**, Amer. Math. Soc., Providence, R.I., 1980. MR 82e:20014 Zbl 0451.05026

[Reid 2002] M. Reid, "La correspondance de McKay", *Astérisque* 276 (2002), 53–72. MR 2003h:14026 Zbl 0996.14006

[Springer 1998] T. A. Springer, *Linear algebraic groups*, 2nd ed., Progress in Mathematics **9**, Birkhäuser, Boston, 1998. MR 99h:20075 Zbl 0927.20024

Communicated by Ravi Vakil
Received 2007-08-10 Revised 2008-05-09 Accepted 2008-05-09

jbryan@math.ubc.ca
1984 Mathematics Road, Vancouver, BC V6T 1Z2, Canada
http://www.math.ubc.ca/~jbryan/

agholamp@caltech.edu
Mathematics 253-37, Caltech, Pasadena, CA 91125, United States
http://www.its.caltech.edu/~agholamp/

ALGEBRA AND NUMBER THEORY 2:4 (2008)
dx.doi.org/10.2140/ant.2008.2.391

Mass formulas for local Galois representations to wreath products and cross products

Melanie Matchett Wood

Bhargava proved a formula for counting, with certain weights, degree n étale extensions of a local field, or equivalently, local Galois representations to S_n. This formula is motivation for his conjectures about the density of discriminants of S_n-number fields. We prove there are analogous "mass formulas" that count local Galois representations to any group that can be formed from symmetric groups by wreath products and cross products, corresponding to counting towers and direct sums of étale extensions. We obtain as a corollary that the above mentioned groups have rational character tables. Our result implies that D_4 has a mass formula for certain weights, but we show that D_4 does not have a mass formula when the local Galois representations to D_4 are weighted in the same way as representations to S_4 are weighted in Bhargava's mass formula.

1. Introduction

Bhargava [2007] proved the following mass formula for counting isomorphism classes of étale extensions of degree n of a local field K:

$$\sum_{[L:K]=n \text{ étale}} \frac{1}{|\operatorname{Aut}(K)|} \cdot \frac{1}{\operatorname{Norm}(\operatorname{Disc}_K L)} = \sum_{k=0}^{n-1} p(k, n-k) q^{-k}, \tag{1-1}$$

where q is the cardinality of the residue field of K, and $p(k, n-k)$ denotes the number of partitions of k into at most $n-k$ parts. Equation (1-1) is proven using the beautiful mass formula of Serre [1978] which counts totally ramified degree n extensions of a local field. Equation (1-1) is at the heart of [Bhargava 2007, Conjecture 1] for the asymptotics of the number of S_n-number fields with discriminant $\leq X$, and also [Bhargava 2007, Conjectures 2–3] for the relative asymptotics of S_n-number fields with certain local behaviors specified. These conjectures are theorems for $n \leq 5$ [Davenport and Heilbronn 1971; Bhargava 2005; $\geq$ 2008].

MSC2000: primary 11S15; secondary 11R45.
Keywords: local field, mass formula, counting field extensions.

Kedlaya [2007, Section 3] has translated Bhargava's formula into the language of Galois representations so that the sum in (1-1) becomes a sum over Galois representations to S_n as follows:

$$\frac{1}{n!}\sum_{\rho:\mathrm{Gal}(K^{\mathrm{sep}}/K)\to S_n}\frac{1}{q^{c(\rho)}}=\sum_{k=0}^{n-1}p(k,n-k)q^{-k}, \tag{1-2}$$

where $c(\rho)$ denotes the Artin conductor of ρ composed with the standard representation $S_n \to \mathrm{GL}_n(\mathbb{C})$.

What is remarkable about the mass formulas in (1-1) and (1-2) is that the right hand side only depends on q and, in fact, is a polynomial (independent of q) evaluated at q^{-1}. A priori, the left hand sides could depend on the actual local field K, and even if they only depended on q, it is not clear there should be a uniform way to write them as a polynomial function of q^{-1}. This motivates the following definitions. Given a local field K and a finite group Γ, let $S_{K,\Gamma}$ denote the set of continuous homomorphisms $\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \Gamma$ (for the discrete topology on Γ) and let q_K denote the size of the residue field of K. Given a function $c\colon S_{K,\Gamma} \to \mathbb{Z}_{\geq 0}$, we define the *total mass* of (K, Γ, c) to be

$$M(K,\Gamma,c) := \sum_{\rho\in S_{K,\Gamma}}\frac{1}{q_K^{c(\rho)}}.$$

(If the sum diverges, we could say the mass is ∞ by convention. In most interesting cases, for example see [Kedlaya 2007, Remark 2.3], and all cases we consider in this paper, the sum will be convergent.) Kedlaya gave a similar definition, but one should note that our definition of mass differs from that in [Kedlaya 2007] by a factor of $|\Gamma|$. In [Kedlaya 2007], $c(\rho)$ is always taken to be the Artin conductor of the composition of ρ and some $\Gamma \to \mathrm{GL}_n(\mathbb{C})$. We refer to such c as the *counting function attached to the representation* $\Gamma \to \mathrm{GL}_n(\mathbb{C})$. In this paper, we consider more general c.

Given a group Γ, a *counting function for* Γ is any function

$$c\colon \bigcup_K S_{K,\Gamma} \to \mathbb{Z}_{\geq 0}$$

where the union is over all isomorphism classes of local fields, such that

$$c(\rho) = c(\gamma\rho\gamma^{-1})$$

for every $\gamma \in \Gamma$. (Since an isomorphism of local fields only determines an isomorphism of their absolute Galois groups up to conjugation, we need this condition in order for the counting functions to be sensible.) Let c be a counting function for Γ and S be a class of local fields. We say that (Γ, c) has a *mass formula* for S if there exists a polynomial $f(x) \in \mathbb{Z}[x]$ such that for all local fields $K \in S$ we have

$$M(K, \Gamma, c) = f\Big(\frac{1}{q_K}\Big).$$

We also say that Γ has a mass formula for S if there is a c such that (Γ, c) has a mass formula for S.

Kedlaya [2007, Theorem 8.5] proved that $(W(B_n), c_{B_n})$ has a mass formula for all local fields, where $W(B_n)$ is the Weyl group of B_n and c_{B_n} is the counting function attached to the Weyl representation of B_n. This is in analogy with (1-2) which shows that $(W(A_n), c_{A_n})$ has a mass formula for all local fields, where $W(A_n) \cong S_n$ is the Weyl group of A_n and c_{A_n} is the counting function attached to the Weyl representation of A_n. Kedlaya's analogy is very attractive, but he found that it does not extend to the Weyl groups of D_4 or G_2 when the counting function is the one attached to the Weyl representation; he showed that mass formulas for all local fields do not exist for those groups and those particular counting functions.

The main result of this paper is the following.

Theorem 1.1. *Any permutation group that can be constructed from the symmetric groups S_n using wreath products and cross products has a mass formula for all local fields.*

The mass formula of Kedlaya [2007, Theorem 8.5] for $W(B_n) \cong S_2 \wr S_n$ was the inspiration for this result, and it is now a special case of Theorem 1.1.

Bhargava [2007, Section 8.2] asks whether his conjecture for S_n-extensions about the relative asymptotics of the number of global fields with specified local behaviors holds for other Galois groups. Ellenberg and Venkatesh [2005, Section 4.2] suggest that we can try to count extensions of global fields by quite general invariants of Galois representations. In [Wood 2008], it is shown that when counting by certain invariants of abelian global fields, such as conductor, Bhargava's question can be answered affirmatively. It is also shown in [Wood 2008] that when counting abelian global fields by discriminant, the analogous conjectures fail in at least some cases. In light of the fact that Bhargava's conjectures for the asymptotics of the number of S_n-number fields arise from his mass formula (1-1) for counting by discriminant, one naturally looks for mass formulas that use other ways of counting, such as Theorem 1.1, which might inspire conjectures for the asymptotics of counting global fields with other Galois groups.

In Section 2, we prove that if groups A and B have certain refined mass formulas, then $A \wr B$ and $A \times B$ also have such refined mass formulas, which inductively proves Theorem 1.1. Bhargava's mass formula for S_n, given in (1-2), is our base case. In Section 3, as a corollary of our main theorem, we see that any group formed from symmetric groups by taking wreath and cross products has a rational character table. This result, at least in such simple form, is not easily found in the literature.

In order to suggest what our results say in the language of field extensions, in Section 4 we mention the relationship between Galois representations to wreath products and towers of field extensions.

In Section 5, we discuss some situations in which groups have mass formulas for one way of counting but not another. In particular, we show that $D_4 \cong S_2 \wr S_2$ does not have a mass formula for all local fields when $c(\rho)$ is the counting function attached to the standard representation of S_4 restricted to $D_4 \subset S_4$. Consider quartic extensions M of K, whose Galois closure has group D_4, with quadratic subfield L. The counting function that gives the mass formula for D_4 of Theorem 1.1 corresponds to counting such extensions M weighted by

$$\left|\operatorname{Disc}(L|K)N_{L|K}(\operatorname{Disc}(M|L))\right|^{-1},$$

whereas the counting function attached to the standard representation of S_4 restricted to $D_4 \subset S_4$ corresponds to counting such extensions M weighted by

$$|\operatorname{Disc}(M|K)|^{-1} = \left|\operatorname{Disc}(L|K)^2 N_{L|K}(\operatorname{Disc}(M|L))\right|^{-1}.$$

So this change of exponent in the $\operatorname{Disc}(L|K)$ factor affects the existence of a mass formula for all local fields.

Notation. Throughout this paper, K is a local field and $G_K := \operatorname{Gal}(K^{\mathrm{sep}}/K)$ is the absolute Galois group of K. All maps in this paper from G_K or subgroups of G_K are continuous homomorphisms, with the discrete topology on all finite groups. We let I_K denote the inertia subgroup of G_K. Recall that $S_{K,\Gamma}$ is the set of maps $G_K \to \Gamma$, and q_K is the size of residue field of K. Also, Γ will always be a permutation group acting on a finite set.

2. Proof of Theorem 1.1

In order to prove Theorem 1.1, we prove finer mass formulas first. Instead of summing over all representations of G_K, we stratify the representations by *type* and prove mass formulas for the sum of representations of each type. Let $\rho\colon G_K \to \Gamma$ be a representation such that the action of G_K has r orbits $m_1, \dots, m_r$. If, under restriction to the representation $\rho : I_K \to \Gamma$, orbit m_i breaks up into f_i orbits of size e_i, then we say that ρ is of *type* $(f_1^{e_1} f_2^{e_2} \cdots f_r^{e_r})$ (where the terms $f_i^{e_i}$ are unordered formal symbols, as in [Bhargava 2007, Section 2]). Let L_i be the fixed field of the stabilizer of an element in m_i. So, $[L_i\colon K] = |m_i|$. Since $I_{L_i} = G_{L_i} \cap I_K$ is the stabilizer in I_K of an element in m_i, we conclude that $e_i = [I_K : I_{L_i}]$, which is the ramification index of L_i/K. Thus, f_i is the inertial degree of L_i/K.

Given Γ, a counting function c for Γ, and a type

$$\sigma = (f_1^{e_1} f_2^{e_2} \cdots f_r^{e_r}),$$

we define the *total mass* of (K, Γ, c, σ) to be

$$M(K, \Gamma, c, \sigma) := \sum_{\substack{\rho \in S_{K,\Gamma} \\ \text{type } \sigma}} \frac{1}{q_K^{c(\rho)}}.$$

We say that (Γ, c) has *mass formulas for S by type* if for every type σ there exists a polynomial $f_{(\Gamma,c,\sigma)}(x) \in \mathbb{Z}[x]$ such that for all local fields $K \in S$ we have

$$M(K, \Gamma, c, \sigma) = f_{(\Gamma,c,\sigma)}\Big(\frac{1}{q_K}\Big).$$

Bhargava [2007, Proposition 1] actually proved that S_n has mass formulas for all local fields by type. Of course, if (Γ, c) has mass formulas by type, then we can sum over all types to obtain a mass formula for (Γ, c).

The key step in the proof of Theorem 1.1 is the following.

Theorem 2.1. *If A and B are finite permutation groups, S is some class of local fields, and (A, c_A) and (B, c_B) have mass formulas for S by type, then there exists a counting function c (given in* (2-3)*) such that $(A \wr B, c)$ has mass formulas for S by type.*

Proof. Let K be a local field in S. Let A act on the left on the set $\mathcal{A}$ and B act on the left on the set $\mathcal{B}$. We take the natural permutation action of $A \wr B$ acting on a disjoint union of copies of $\mathcal{A}$ indexed by elements of $\mathcal{B}$. Fix an ordering on $\mathcal{B}$ so that we have canonical orbit representatives in $\mathcal{B}$. Given $\rho : G_K \to A \wr B$, there is a natural quotient $\bar{\rho} : G_K \to B$. Throughout this proof, we use j as an indexing variable for the set $\mathcal{B}$ and i as an indexing variable for the r canonical orbit representatives in $\mathcal{B}$ of the $\rho(G_K)$ action. Let i_j be the index of the orbit representative of j's orbit. Let $S_j \subset G_K$ be the stabilizer of j, and let S_j have fixed field L_j. We define $\rho_j : G_{L_j} \to A$ to be the given action of G_{L_j} on the j-th copy of $\mathcal{A}$. We say that ρ has *wreath type*

$$\Sigma = (f_1^{e_1}(\sigma_1) \cdots f_r^{e_r}(\sigma_r)) \tag{2-1}$$

if $\bar{\rho}$ has type $\sigma = (f_1^{e_1} \cdots f_r^{e_r})$ (where $f_i^{e_i}$ corresponds to the orbit of i) and ρ_i has type σ_i. Note that type is a function of wreath type; if ρ has wreath type Σ as above where

$$\sigma_i = \big(f_{i,1}^{e_{i,1}} \cdots f_{i,r_i}^{e_{i,r_i}}\big),$$

then ρ has type $((f_i f_{i,k})^{e_i e_{i,k}})_{1 \le i \le r,\, 1 \le k \le r_i}$.

We consider the function c defined as follows:

$$c(\rho) = c_B(\bar{\rho}) + \sum_{j \in \mathcal{B}} \frac{c_A(\rho_j)}{|\{\bar{\rho}(I_K)j\}|}. \tag{2-2}$$

Since $c_B(\bar{\rho})$ only depends on the B-conjugacy class of $\bar{\rho}$ and $c_A(\rho_j)$ depends only on the A-conjugacy class of ρ_j, we see that conjugation by elements of $A \wr B$ does not affect the right hand side of (2-3) except by reordering the terms in the sum. Thus c is a counting function.

Since ρ_j and ρ_{i_j} are representations of conjugate subfields of G_K and since c_A is invariant under A-conjugation, $c_A(\rho_j) = c_A(\rho_{i_j})$. There are $f_i e_i$ elements in the orbit of i under $\bar{\rho}(G_K)$ and e_{i_j} elements in the orbit of j under $\bar{\rho}(I_K)$, so

$$c(\rho) = c_B(\bar{\rho}) + \sum_{i=1}^{r} \frac{f_i e_i}{e_i} c_A(\rho_i)$$

and thus

$$c(\rho) = c_B(\bar{\rho}) + \sum_{i=1}^{r} f_i c_A(\rho_i). \tag{2-3}$$

Using this expression for $c(\rho)$, we will prove that $(A \wr B, c)$ has mass formulas by wreath type. Then, summing over wreath types that give the same type, we will prove that $(A \wr B, c)$ has mass formulas by type.

Remark 2.2. For a permutation group Γ, let d_Γ be the counting function attached to the permutation representation of Γ (which is the discriminant exponent of the associated étale extension). Then we can compute

$$d_{A \wr B} = |\mathcal{A}|\, d_B(\bar{\rho}) + \sum_{i=1}^{r} f_i\, d_A(\rho_i),$$

which is similar to the expression given in (2-3) but differs by the presence of $|\mathcal{A}|$ in the first term. In particular, when we have mass formulas for (A, d_A) and (B, d_B), the mass formula for $A \wr B$ that we find in this paper is not with the counting function $d_{A \wr B}$. We will see in Section 5, when A and B are both S_2, that $S_2 \wr S_2 \cong D_4$ does not have a mass formula with $d_{A \wr B}$.

Lemma 2.3. *The correspondence $\rho \mapsto (\bar{\rho}, \rho_1, \dots, \rho_r)$ described above gives a function Ψ from $S_{K, A \wr B}$ to tuples $(\phi, \phi_1, \dots, \phi_r)$ where $\phi : G_K \to B$, the groups S_i are the stabilizers of canonical orbit representatives of the action of ϕ on B, and $\phi_i : S_i \to A$. The map Ψ is $(|A|^{|\mathcal{B}|-r})$-to-one and surjective.*

Proof. Lemma 2.3 holds when G_K is replaced by any group. It suffices to prove the lemma when $\bar{\rho}$ and ϕ are transitive because the general statement follows by multiplication. Let $b \in \mathcal{B}$ be the canonical orbit representative. Given a

$$\phi \colon G_K \to B \quad (\text{or a } \bar{\rho} \colon G_K \to B)$$

for all $j \in \mathcal{B}$, choose a $\sigma_j \in G_K$ such that $\phi(\sigma_j)$ takes b to j. Given a $\rho \colon G_K \to A \wr B$, let α_j be the element of A such that $\rho(\sigma_j)$ acts on the b-th copy of $\mathcal{A}$ by α_j and then moves the b-th copy of $\mathscr{A}$ to the j-th copy. Then for $g \in G_K$, the map ρ is given by

$$\rho(g) = \bar{\rho}(g)(a_j)_{j\in\mathscr{B}} \in BA^{|\mathscr{B}|} = A \wr B, \tag{2-4}$$

where

$$a_j = \alpha_{\bar{\rho}(g)(j)}\rho_1\bigl(\sigma^{-1}_{\bar{\rho}(g)(j)} g \sigma_j\bigr)\,\alpha_j^{-1},$$

and $a_j \in A$ acts on the j-th copy of $\mathscr{A}$. For any transitive maps $\phi \colon G_K \to B$ and $\phi_b : S_b \to A$ and for any choices of $\alpha_j \in A$ for all $j \in \mathscr{B}$ such that $\alpha_b = \phi_b(\sigma_b)$, we can check that (2-4) for $\bar{\rho} = \phi$ and $\rho_1 = \phi_b$ gives a homomorphism $\rho \colon G_K \to A \wr B$ with $(\bar{\rho}, \rho_1) = (\phi, \phi_b)$, which proves the lemma. □

If Σ is as in (2-1), then

$$\sum_{\substack{\rho:G_K\to A\wr B\\ \text{wreath type }\Sigma}} \frac{1}{q_K^{c(\rho)}} = |A|^{|\mathscr{B}|-r} \sum_{\substack{\phi:G_K\to B\\ \text{type }\sigma}} \sum_{\substack{\phi_1:S_1\to A\\ \text{type }\sigma_1}} \sum_{\substack{\phi_2:S_2\to A\\ \text{type }\sigma_2}} \cdots \sum_{\substack{\phi_r:S_r\to A\\ \text{type }\sigma_r}} \frac{1}{q_K^{c_B(\phi)+\sum_{i=1}^r f_i c_A(\phi_i)}} \tag{2-5}$$

where S_i is the stabilizer under ϕ of a canonical orbit representative of the action of ϕ on $\mathscr{B}$. The right hand side of (2-5) factors, and $S_i \subset G_K$ has fixed field L_i with residue field of size $q_K^{f_i}$. We conclude that

$$\begin{aligned}\sum_{\substack{\rho:G_K\to A\wr B\\ \text{wreath type }\Sigma}} \frac{1}{q_K^{c(\rho)}} &= |A|^{|\mathscr{B}|-r} \sum_{\substack{\phi:G_K\to B\\ \text{type }\sigma}} \frac{1}{q_K^{c_A(\phi)}} \sum_{\substack{\phi_1:G_{L_1}\to A\\ \text{type }\sigma_1}} \frac{1}{q_K^{f_1 c_B(\phi_1)}} \cdots \sum_{\substack{\phi_r:G_{L_r}\to A\\ \text{type }\sigma_r}} \frac{1}{q_K^{f_r c_B(\phi_r)}}\\ &= |A|^{|\mathscr{B}|-r} f_{(B,c_B,\sigma)}\Bigl(\frac{1}{q_K}\Bigr) \prod_{i=1}^{r} f_{(A,c_A,\sigma_i)}\Bigl(\frac{1}{q_K^{f_i}}\Bigr).\end{aligned}$$

So, $(A \wr B, c)$ has mass formulas by wreath type, and thus by type. □

Kedlaya [2007, Lemma 2.6] noted that if (Γ, c) and (Γ', c') have mass formulas f and f', then $(\Gamma\times\Gamma', c'')$ has mass formula ff', where $c''(\rho\times\rho') = c(\rho)+c'(\rho')$. We can strengthen this statement to mass formulas by type using a much easier version of our argument for wreath products. We define the *product type* of a representation $\rho \times \rho' : G_K \to \Gamma \times \Gamma'$ to be (σ, σ'), where σ and σ' are the types of ρ and ρ' respectively. Then

$$\sum_{\substack{\rho\times\rho':G_K\to\Gamma\times\Gamma'\\ \text{product type }(\sigma,\sigma')}} \frac{1}{q_K^{c''(\rho\times\rho')}} = \sum_{\substack{\phi:G_K\to\Gamma\\ \text{type }\sigma}} \frac{1}{q_K^{c(\rho)}} \sum_{\substack{\phi_1:G_{L_1}\to\Gamma'\\ \text{type }\sigma'}} \frac{1}{q_K^{c'(\rho')}}.$$

If Γ and Γ' have mass formulas by type, then the above gives mass formulas of $\Gamma \times \Gamma'$ by product type. Since type is a function of product type, we can sum the mass formulas by product type to obtain mass formulas by type for $\Gamma \times \Gamma'$.

This, combined with Theorem 2.1 and Bhargava's mass formula for S_n by type [Bhargava 2007, Proposition 1], proves Theorem 1.1.

3. Groups with rational character tables

Kedlaya [2007, Proposition 5.3, Corollary 5.4, Corollary 5.5] showed that if $c(\rho)$ is the counting function attached to $\Gamma \to \mathrm{GL}_n(\mathbb{C})$, then the following statement holds: (Γ, c) has a mass formula for all local fields K with q_K relatively prime to $|\Gamma|$ if and only if the character table of Γ has all rational entries. The proofs of [Kedlaya 2007, Proposition 5.3, Corollary 5.4, Corollary 5.5] hold for any counting function c that is determined by $\rho(I_K)$. This suggests that we define a *proper* counting function to be a counting function c that satisfies the following: if we have

$$\rho : G_K \to \Gamma \quad \text{and} \quad \rho' : G_{K'} \to \Gamma$$

with $q_K, q_{K'}$ relatively prime to $|\Gamma|$, and if $\rho(I_K) = \rho'(I_{K'})$, then $c(\rho) = c(\rho')$.

For proper counting functions, we always have partial mass formulas proven as in [Kedlaya 2007, Corollary 5.4].

Proposition 3.1. *Let a be an invertible residue class mod $|\Gamma|$ and c be a proper counting function. Then (Γ, c) has a mass formula for all local fields K with $q_K \in a$.*

The following proposition says exactly when these partial mass formulas agree, again proven as in [Kedlaya 2007, Corollary 5.5].

Proposition 3.2. *Let c be a proper counting function for Γ. Then (Γ, c) has a mass formula for all local fields K with q_K relatively prime to $|\Gamma|$ if and only if Γ has a rational character table.*

So, when looking for a group and a proper counting function with mass formulas for all local fields, we should look among groups with rational character tables (which are relatively rare, for example including only 14 of the 93 groups of order < 32 [Conway 2006]). All specific counting functions that have been so far considered in the literature are proper. It is not clear if there are any interesting nonproper counting functions.

Our proof of Theorem 2.1 has the following corollary.

Corollary 3.3. *Any permutation group that can be constructed from the symmetric groups using wreath products and cross products has a rational character table.*

Proof. We first show that the counting function c defined in (2-2) is proper if c_A and c_B are proper. We consider only fields K with q_K relatively prime to $|\Gamma|$. Since $c_B(\bar{\rho})$ only depends on $\bar{\rho}(I_K)$, it is clear that the $c_B(\bar{\rho})$ term only depends on $\rho(I_K)$.

Since $I_{L_j} = I_K \cap S_j$, we have

$$\rho_j(I_{L_j}) = \rho(I_{L_j}) = \rho(I_K) \cap \mathrm{Stab}(j).$$

Since $c_A(\rho_j)$ depends only on $\rho_j(I_{L_j})$, we see that it depends only on $\rho(I_K)$. The sum in (2-2) then depends only on $\rho(I_K)$. So the c defined in (2-2) is proper. Clearly the $c''(\rho \times \rho')$ defined for cross products is proper if c and c' are proper. The counting function in Bhargava's mass formula for S_n (see (1-2)) is an Artin conductor and thus is proper. So we can prove Theorem 1.1 with a proper counting function and conclude the corollary.

One can show in a similar way that even in wild characteristics, the counting function c defined in (2-3) depends only on the images of the higher ramification groups G_K^m, that is, if

$$\rho : G_K \to A \wr B \quad \text{and} \quad \rho' : G'_K \to A \wr B$$

have $\rho(G_K^m) = \rho'(G_{K'}^m)$ for all $m \in [0, \infty)$, then $c(\rho) = c(\rho')$, as long as the same is true for c_A and c_B. □

So, for example, $((S_7 \wr S_4) \times S_3) \wr S_8$ has a rational character table. Corollary 3.3 does not seem to be a well-reported fact in the literature; the corollary shows that all Sylow 2-subgroups of symmetric groups (which are cross products of wreath products of S_2's) have rational character table, which was posed as an open problem in [Mazurov and Khukhro 1999, Problem 15.25] and solved in [Revin 2004; Kolesnikov 2005]. However, since

$$A \wr (B \wr C) = (A \wr B) \wr C \quad \text{and} \quad A \wr (B \times C) = (A \wr B) \times (A \wr C),$$

any of the groups of Corollary 3.3 can be constructed only using the cross product and $\wr S_n$ operations. It is well known that the cross product of two groups with rational character tables has a rational character table. Furthermore, Pfeiffer [1994] explains how GAP computes the character table of $G \wr S_n$ from the character table of G, and one can check that if G has rational character table then all of the values constructed in the character table of $G \wr S_n$ are rational, which implies Corollary 3.3.

One might hope that all groups with rational character tables have mass formulas by type, but this is not necessarily the case. For example, considering

$$(C_3 \times C_3) \rtimes C_2$$

(where C_2 acts nontrivially on each factor separately) in the tame case in type $(1^3\, 2^1\, 1^1)$, one can check that for $q \equiv 1 \pmod 3$ the mass is zero and for $q \equiv 2 \pmod 3$ the mass is nonzero.

4. Towers and direct sums of field extensions

Kedlaya explains the correspondence between Galois permutation representations and étale extensions in [Kedlaya 2007, Lemma 3.1]. We have seen this correspondence already in other terms. If we have a representation $\rho : G_K \to \Gamma$ with r orbits, S_i is the stabilizer of an element in the i-th orbit, and L_i is the fixed field of S_i, then ρ corresponds to $L = \bigoplus_{i=1}^r L_i$. For a local field F, let $\wp_F$ be the prime of F. In this correspondence, if c is the counting function attached to the permutation representation of Γ, then c is the discriminant exponent of the extension L/K [Kedlaya 2007, Lemma 3.4]. In other words,

$$\wp_K^{c(\rho)} = \mathrm{Disc}(L|K).$$

We can interpret the representations $\rho : G_K \to A \wr B$ as towers of étale extensions $M/L/K$. If we take $\bar{\rho} : G_K \to B$, then $L = \bigoplus_{i=1}^r L_i$ is just the étale extension of K corresponding to $\bar{\rho}$. Then if M is the étale extension of K corresponding to ρ, we see that $M = \bigoplus_{i=1}^r M_i$, where M_i is the étale extension of L_i corresponding to $\rho_i : G_{L_i} \to A$. So we see that M is an étale extension of L, though L might not be a field.

Let c be the counting function of our mass formula for wreath products, given by (2-3). From (2-3), we obtain

$$\wp_K^{c(\rho)} = \wp_K^{c_B(\bar{\rho})} \prod_{i=1}^{r} N_{L_i|K}\big(\wp_{L_i}^{c_A(\rho_i)}\big).$$

For example, if c_A and c_B are both given by the discriminant exponent (or equivalently, attached to the permutation representation), then

$$\wp_K^{c(\rho)} = \mathrm{Disc}(L|K) \prod_{i=1}^{r} N_{L_i|K}(\mathrm{Disc}(M_i|L_i)). \tag{4-1}$$

For comparison,

$$\mathrm{Disc}(M|K) = \mathrm{Disc}(L|K)^{[M:L]} \prod_{i=1}^{r} N_{L_i|K}(\mathrm{Disc}(M_i|L_i)).$$

As we will see for $\Gamma = D_4$ in the next section, representations $\rho : G_K \to \Gamma$ can give not only field extensions of K whose Galois closure has Galois group Γ, but also field extensions whose Galois closure has Galois group a proper subgroup of Γ, as well as direct sums of field extensions. One could say that representations $\rho : G_K \to A \wr B$ correspond to towers of "A-extensions" over "B-extensions" and further relate iterated wreath products to iterated towers. Similarly, one could say that a representation $\rho : G_K \to A \times B$ corresponds to a direct sum of an "A-extension" and a "B-extension." The quotes indicate that the extensions do not necessarily have Galois closure with group A or B. In fact, it seems the most convenient way to define "A-extensions" or isomorphisms of "A-extensions" is simply to use the language of Galois representations as we have in this paper.

5. Masses for D_4

By Proposition 3.2 we know, at least for proper counting functions, that the existence of a mass formula for a group Γ for fields with q_K relatively prime to $|\Gamma|$ does not depend on the choice of the counting function. However, in wild characteristic this is not the case. For example, D_4, the dihedral group with 8 elements, is isomorphic to $S_2 \wr S_2$, so by Theorem 1.1 there is a c (given in (2-3)) for which D_4 has a mass formula for all local fields. An expression for c in terms of étale extensions can be read off from (4-1). In particular, for a surjective representation $\rho : G_K \to D_4$ corresponding to a quartic field extension M of K with a quadratic subextension L,

$$\wp_K^{c(\rho)} = \mathrm{Disc}(L|K) N_{L|K}(\mathrm{Disc}(M|L)). \tag{5-1}$$

For this c, for all local fields K, we have that

$$M(K, D_4, c) := \sum_{\rho \in S_{K,D_4}} \frac{1}{q_K^{c(\rho)}} = 8 + \frac{16}{q_K} + \frac{16}{q_K^2}.$$

From the definition of c given in (2-2) and the description of the absolute tame Galois group of a local field, we can compute $M(K, D_4, c)$ for a field K with q_K odd. By Theorem 2.1 we know the formula holds for all K.

However, the counting function for D_4 that has been considered when counting global extensions (for example in [Cohen et al. 2002]) is the one attached the faithful permutation representation of D_4 on a four element set (equivalently the discriminant exponent of the corresponding étale extension). We call this counting function d, and in comparison with (5-1) we have

$$\wp_K^{d(\rho)} = \mathrm{Disc}(M|K) = \mathrm{Disc}(L|K)^2 N_{L|K}(\mathrm{Disc}(M|L)).$$

With d, we now show that D_4 does not have a mass formula for all local fields.

Using the correspondence of Section 4, we can analyze the representations

$$\rho : G_K \to D_4 \subset S_4$$

in Table 1, where

$$I = \mathrm{image}(\rho), \quad j = \left|\left\{ s \in S_4 \;\middle|\; sIs^{-1} \subset D_4 \right\}\right| \quad \text{and} \quad k = |\,\mathrm{Centralizer}_{S_4}(I)|.$$

We take the D_4 in S_4 generated by $(1\,2\,3\,4)$ and $(1\,3)$.

I	j	k	L
D_4	8	2	degree 4 field whose Galois-closure$/K$ has group D_4
C_4	8	4	degree 4 field Galois$/K$ with group $C_4 \cong \mathbb{Z}/4$
$\langle(1\,2)(3\,4),\,(1\,3)(2\,4)\rangle$	24	4	degree 4 field Galois$/K$ with group $V_4 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$
$\langle(1\,3),\,(2\,4)\rangle$	8	4	$L_1 \oplus L_2$ with $[L_i : K]$=2 and L_i distinct fields
$\langle(1\,3)(2\,4)\rangle$, $\langle(1\,2)(3\,4)\rangle$ or $\langle(1\,4)(2\,3)\rangle$	24	8	$L_1 \oplus L_2$ with $[L_i : K]$=2 and $L_1 \cong L_2$ fields
$\langle(2\,4)\rangle$ or $\langle(1\,3)\rangle$	8	4	$L_1 \oplus K \oplus K$ with $[L_1 : K]$=2 and L_1 a field
1	24	24	$K \oplus K \oplus K \oplus K$

Table 1

Each isomorphism class of algebras appears $\frac{j}{k}$ times from a representation $\rho : G_K \to D_4$ (see [Kedlaya 2007, Lemma 3.1]). Let $S(K, G, m)$ be the set of isomorphism classes of degree m field extensions of K whose Galois closure over K has group G. Then from the above table we see that

$$M(K, D_4, d) = \sum_{F\in S(K,D_4,4)} \frac{4}{|\operatorname{Disc} F|} + \sum_{F\in S(K,C_4,4)} \frac{2}{|\operatorname{Disc} F|} + \sum_{F\in S(K,V_4,4)} \frac{6}{|\operatorname{Disc} F|}$$
$$+ \sum_{\substack{F_1,F_2\in S(K,C_2,2)\\ F_1\ncong F_2}} \frac{2}{|\operatorname{Disc} F_1||\operatorname{Disc} F_2|} + \sum_{F\in S(K,C_2,2)} \frac{3}{|\operatorname{Disc} F|^2}$$
$$+ \sum_{F\in S(K,C_2,2)} \frac{2}{|\operatorname{Disc} F|} + 1,$$

where if $\wp_F$ is the prime of F and $\operatorname{Disc} F = \wp_F^m$, then $|\operatorname{Disc} F| = q_F^m$. Using the Database of Local Fields [Jones and Roberts 2006] we can compute that $M(\mathbb{Q}_2, D_4, d) = \frac{121}{8}$. For fields with $2 \nmid q_K$, the structure of the tame quotient of the absolute Galois group of a local field allows us to compute the mass to be

$$8 + \frac{8}{q_K} + \frac{16}{q_K^2} + \frac{8}{q_K^3}$$

(also see [Kedlaya 2007, Corollary 5.4]) which evaluates to 17 for $q_K = 2$. Thus (D_4, d) does not have a mass formula for all local fields.

As another example, Kedlaya [2007, Proposition 9.3] found that $W(G_2)$ does not have a mass formula for all local fields of residual characteristic 2 when c is the Artin conductor of the Weyl representation. However, $W(G_2) \cong S_2 \times S_3$ and thus it has a mass formula for all local fields with counting function the sum of the Artin conductors of the standard representations of S_2 and S_3.

It would be interesting to study what the presence or absence of mass formulas tells us about a counting function, in particular with respect to how global fields can be counted asymptotically with that counting function. As in Bhargava [2007, Section 8.2], we can form an Euler series

$$M_c(\Gamma, s) = C(\Gamma)\Bigg(\sum_{\rho\in S_{\mathbb{R},\Gamma}} \frac{1}{|\Gamma|}\Bigg)\prod_p\Bigg(\frac{1}{|\Gamma|}\sum_{\rho\in S_{\mathbb{Q}_p,\Gamma}} \frac{1}{p^{c(\rho)s}}\Bigg) = \sum_{n\geq 1} m_n n^{-s},$$

where $C(\Gamma)$ is some simple, yet to be explained, rational constant. (We work over $\mathbb{Q}$ for simplicity, and the product is over rational primes.) For a representation $\rho : G_{\mathbb{Q}} \to \Gamma$, let ρ_p be the restriction of ρ to $G_{\mathbb{Q}_p}$. The idea is that m_n should be a heuristic of the number of Γ-extensions of $\mathbb{Q}$ (that is, surjective $\rho : G_{\mathbb{Q}} \to \Gamma$) with

$$\prod_p p^{c(\rho_p)} = n,$$

though m_n is not necessarily an integer.

Bhargava [2007, Section 8.2] asks the following question.

Question 5.1. Does

$$\lim_{X\to\infty} \frac{\sum_{n=1}^{X} m_n}{\big|\big\{\text{isom. classes of surjective } \rho : G_{\mathbb{Q}} \to \Gamma \text{ with } \prod_p p^{c(\rho_p)} \leq X\big\}\big|} = 1?$$

Bhargava in fact asks more refined questions in which some local behaviors are fixed. With the counting function d for D_4 attached to the permutation representation (that is, the discriminant exponent), we can form $M_d(D_4, s)$ and compute numerically the above limit. We use the work of Cohen, Diaz y Diaz, and Oliver on counting D_4-extensions by discriminant (see [Cohen et al. 2006] for a recent value of the relevant constants) to calculate the limit of the denominator, and we use standard Tauberian theorems (see [Narkiewicz 1983, Corollary, p. 121]) and PARI/GP [2006] to calculate the limit of the numerator. Of course, $C(D_4)$ has not been decided, but it does not appear (by using the `algdep` function in PARI/GP) that any simple rational $C(D_4)$ will give an affirmative answer to the above question.

In light of our mass formula for a different counting function c for D_4, we naturally wonder about Question 5.1 in the case of D_4 and that c. Answering this question would require counting D_4 extensions M with quadratic subfield L by

$$\operatorname{Disc}(L \mid \mathbb{Q})\, N_{L|\mathbb{Q}}(\operatorname{Disc}(M|L))$$

instead of by discriminant, which is

$$\operatorname{Disc}(L|\mathbb{Q})^2 N_{L|\mathbb{Q}}(\operatorname{Disc}(M|L)).$$

Acknowledgements

I would like to thank Manjul Bhargava for his guidance while I was doing this research and thorough and helpful comments on earlier versions of this manuscript. I would also like to thank Kiran Kedlaya for providing me an early version of [Kedlaya 2007] and for answers to my questions about that paper. The referee gave suggestions for additions and improvements to the paper that were incorporated and much appreciated.

This work was supported by a National Defense Science and Engineering Graduate Fellowship.

References

[Bhargava 2005] M. Bhargava, "The density of discriminants of quartic rings and fields", *Ann. of Math.* (2) **162**:2 (2005), 1031–1063. MR 2006m:11163 Zbl 05042692

[Bhargava 2007] M. Bhargava, "Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants", *Int. Math. Res. Not.* **2007**:17 (2007), rnm052. MR 2354798 Zbl 05215305

[Bhargava ≥ 2008] M. Bhargava, "The density of discriminants of quintic rings and fields", *Ann. of Math.*. To appear.

[Cohen et al. 2002] H. Cohen, F. Diaz y Diaz, and M. Olivier, "Enumerating quartic dihedral extensions of $\mathbb{Q}$", *Compositio Math.* **133**:1 (2002), 65–93. MR 2003f:11167 Zbl 1050.11104

[Cohen et al. 2006] H. Cohen, F. Diaz y Diaz, and M. Olivier, "Counting discriminants of number fields", *J. Théor. Nombres Bordeaux* **18**:3 (2006), 573–593. MR 2008d:11127 Zbl 05186992

[Conway 2006] J. H. Conway, personal communication, 2006.

[Davenport and Heilbronn 1971] H. Davenport and H. Heilbronn, "On the density of discriminants of cubic fields. II", *Proc. Roy. Soc. London Ser. A* **322**:1551 (1971), 405–420. MR 58 #10816 Zbl 0212.08101

[Ellenberg and Venkatesh 2005] J. S. Ellenberg and A. Venkatesh, "Counting extensions of function fields with bounded discriminant and specified Galois group", pp. 151–168 in *Geometric methods in algebra and number theory* (Miami, 2003), edited by F. Bogomolov and Y. Tschinkel, Progr. Math. **235**, Birkhäuser, Boston, 2005. MR 2006f:11139 Zbl 1085.11057

[Jones and Roberts 2006] J. W. Jones and D. P. Roberts, "A database of local fields", *J. Symbolic Comput.* **41**:1 (2006), 80–97. MR 2006k:11230 Zbl 05203425

[Kedlaya 2007] K. S. Kedlaya, "Mass formulas for local Galois representations", *Int. Math. Res. Not.* **2007**:17 (2007), rnm021. MR 2354797 Zbl 05215145

[Kolesnikov 2005] S. G. Kolesnikov, "On the rationality and strong reality of Sylow 2-subgroups of Weyl and alternating groups", *Algebra Logika* **44**:1 (2005), 44–53, 127. MR 2006d:20012 Zbl 05041622

[Mazurov and Khukhro 1999] V. D. Mazurov and E. I. Khukhro (editors), *The Kourovka notebook. Unsolved problems in group theory*, 14th augmented ed., Russian Academy of Sciences Siberian Division Institute of Mathematics, Novosibirsk, 1999. MR 2000h:20001a Zbl 0943.20004

[Narkiewicz 1983] W. Narkiewicz, *Number theory*, World Scientific Publishing Co., Singapore, 1983. Translated from the Polish by S. Kanemitsu. MR 85j:11002 Zbl 0528.10001

[PAR 2006] *PARI/GP*, 2.3.2, 2006, Available at http://pari.math.u-bordeaux.fr.

[Pfeiffer 1994] G. Pfeiffer, "Character tables of Weyl groups in GAP", *Bayreuth. Math. Schr.* 47 (1994), 165–222. MR 95d:20027 Zbl 0830.20023

[Revin 2004] D. O. Revin, "The characters of groups of type $X \wr \mathbb{Z}_p$", *Sib. Èlektron. Mat. Izv.* **1** (2004), 110–116. MR 2005m:20025 Zbl 1079.20011

[Serre 1978] J.-P. Serre, "Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local", *C. R. Acad. Sci. Paris Sér. A-B* **286**:22 (1978), A1031–A1036. MR 80a:12018 Zbl 0388.12005

[Wood 2008] M. M. Wood, "On the probabilities of local behaviors in abelian field extensions", preprint, 2008.

Communicated by Hendrik W. Lenstra
Received 2007-11-28 Revised 2008-03-31 Accepted 2008-04-28

melanie.wood@math.princeton.edu *Princeton University, Department of Mathematics,
Fine Hall, Washington Road, Princeton, NJ 08544,
United States*

Operad of formal homogeneous spaces and Bernoulli numbers

Sergei A. Merkulov

It is shown that for any morphism, $\phi : \mathfrak{g} \to \mathfrak{h}$, of Lie algebras the vector space underlying the Lie algebra $\mathfrak{h}$ is canonically a $\mathfrak{g}$-homogeneous formal manifold with the action of $\mathfrak{g}$ being highly nonlinear and twisted by Bernoulli numbers. This fact is obtained from a study of the 2-coloured operad of formal homogeneous spaces whose minimal resolution gives a new conceptual explanation of both Ziv Ran's Jacobi–Bernoulli complex and Fiorenza–Manetti's L_∞-algebra structure on the mapping cone of a morphism of two Lie algebras. All these constructions are iteratively extended to the case of a morphism of arbitrary L_∞-algebras.

1. Introduction

1.1. The theory of operads and props gives a universal approach to the deformation theory of many algebraic and geometric structures [Merkulov and Vallette 2007]. It also gives a conceptual explanation of the well-known "experimental" observation that a deformation theory is controlled by a differential graded (dg, for short) Lie algebra or, more generally, a L_∞-algebra. What happens is the following:

(I) an algebraic or a (germ of) geometric structure, $\mathfrak{s}$, on a vector space V (which is an *object* in the corresponding category, $\mathfrak{S}$, of algebraic or geometric structures) can often be interpreted as a *morphism*, $\alpha_{\mathfrak{s}} : \mathcal{O}^{\mathfrak{S}} \to \mathcal{E}nd_V$, in the category of operads (or props), where $\mathcal{O}^{\mathfrak{S}}$ and $\mathcal{E}nd_V$ are operads (or props) canonically associated to the category $\mathfrak{S}$ and the vector space V;

(II) the operad/prop $\mathcal{O}^{\mathfrak{S}}$ often admits a unique minimal[1] dg resolution, $\mathcal{O}^{\mathfrak{S}}_\infty$, which, by definition, is a free dg operad/prop generated by some $\mathbb{S}$-(bi)module E together with a epimorphism $\pi : \mathcal{O}^{\mathfrak{S}}_\infty \to \mathcal{O}^{\mathfrak{S}}$ which induces an isomorphism on cohomology; it was proven in [Merkulov and Vallette 2007] (in two different ways) that the set of *all* possible morphisms, $\mathcal{O}^{\mathfrak{S}}_\infty \to \mathcal{E}nd_V$, can be identified with the set of Maurer–Cartan elements of a uniquely defined Lie (or, more generally, filtered

MSC2000: primary 18D50; secondary 11B68, 55P48.
Keywords: operad, Lie algebra, Bernoulli number.

[1] In fact there is no need to work with *minimal* resolutions: any free resolution of $\mathcal{O}^{\mathfrak{S}}$ will do.

L_∞-) algebra $\mathcal{G} := \mathrm{Hom}_{\mathbb{S}}(E, \mathcal{E}nd_V)[-1]$ whose Lie brackets can be read directly from the generators and differential of the minimal resolution $\mathcal{O}_\infty^{\mathfrak{S}}$;

(III) thus, to our algebraic or geometric structure $\mathfrak{s}$ there corresponds a Maurer–Cartan element $\gamma_{\mathfrak{s}} := \pi \circ \alpha_{\mathfrak{s}}$ in $\mathcal{G}$; twisting $\mathcal{G}$ by $\gamma_{\mathfrak{s}}$ one obtains finally a Lie (or L_∞-) algebra $\mathcal{G}_{\mathfrak{s}}$ which controls the deformation theory of the structure $\mathfrak{s}$ we began with.

Many important dg Lie algebras in homological algebra and geometry (such as Hochschild, Schouten and Frölicher–Nijenhuis algebras) are proven in [Kontsevich and Soibelman 2000; Merkulov 2006; 2005; Merkulov and Vallette 2007; van der Laan 2002] to be of this operadic or propic origin. For example, if $\mathfrak{s}$ is a structure of an associative algebra on a vector space V, then,

(i) there is an operad, $\mathcal{A}ss$, uniquely associated with the category of associative algebras, and the structure $\mathfrak{s}$ corresponds to a morphism, $\alpha_{\mathfrak{s}} : \mathcal{A}ss \to \mathcal{E}nd_V$, of operads;

(ii) there is a unique minimal resolution, $\mathcal{A}ss_\infty$, of $\mathcal{A}ss$ which is generated by the $\mathbb{S}$-module $E = \{\mathbb{K}[\mathbb{S}_n][n-2]\}$ and whose representations, $\pi : \mathcal{A}ss_\infty \to \mathcal{E}nd_V$, in a dg space V are in one-to-one correspondence with Maurer–Cartan elements in the Lie algebra,

$$\left(\mathcal{G} := \mathrm{Hom}_{\mathbb{S}}(E, \mathcal{E}nd_V)[-1] = \bigoplus_{n\geq 1} \mathrm{Hom}_{\mathbb{K}}(V^{\otimes n}, V)[1-n],\ [\ ,\ ]_G\right),$$

where $[\ ,\ ]_G$ are Gerstenhaber brackets (see, for example, [Kontsevich and Soibelman 2000; Merkulov and Vallette 2007]);

(iii) therefore, the particular associative algebra structure $\mathfrak{s}$ on V gives rise to the associated Maurer–Cartan element $\gamma_{\mathfrak{s}} := \alpha_{\mathfrak{s}} \circ \pi$ in $\mathcal{G}$; twisting $\mathcal{G}$ by $\gamma_{\mathfrak{s}}$ gives the Hochschild dg Lie algebra,

$$\mathcal{G}_{\mathfrak{s}} = \left(\bigoplus_n \mathrm{Hom}_{\mathbb{K}}(V^{\otimes n}, V)[1-n],\ [\ ,\ ]_G, d_H := [\gamma_{\mathfrak{s}},\ ]_G\right),$$

which indeed controls the deformation theory of $\mathfrak{s}$.

1.2. Recently Ziv Ran introduced a so-called *Jacobi–Bernoulli* deformation complex and used it to study deformations of pairs of geometric structures such as a given complex manifold X and the moduli space, $\mathcal{M}_X$, of vector bundles on X, a complex manifold X and its complex compact submanifold Y, and others [Ran 2006; 2004]. The differential in this complex is, rather surprisingly, twisted by Bernoulli numbers. Fiorenza and Manetti [2007] discovered independently the same thing under the name of L_∞-algebra structure on the mapping cone of a morphism of Lie algebras using completely different approach based on explicit homotopy transfer formulae of Kontsevich and Soibelman [2000] and Merkulov [1999]; they also showed its relevance to the deformation theory of complex submanifolds in complex manifolds using the earlier results of Manetti [2005].

In view of the above paradigm one can raise a question: which operad gives rise to a deformation complex with such an unusual differential?

We suggest an answer in this paper. Surprisingly, this answer is not a straightforward operadic translation of the notion of *Lie atom* introduced and studied in [Ran 2006; 2004] but is based instead on another algebraic+geometric structure which we call a *formal homogeneous space* and which is, by definition, a triple, $(\mathfrak{g}, \mathfrak{h}, F)$, consisting of a Lie algebra $\mathfrak{g}$, a vector space $\mathfrak{h}$, and a morphism,

$$F : \mathfrak{g} \longrightarrow \mathcal{T}_{\mathfrak{h}}$$

of Lie algebras, where $\mathcal{T}_{\mathfrak{h}}$ is the Lie algebra of smooth formal vector fields on the space $\mathfrak{h}$. Let $\mathcal{HS}$ be the 2-coloured operad whose representations are formal homogeneous spaces, $(\mathfrak{g}, \mathfrak{h}, F)$, and let $\mathcal{LP}$ be the 2-coloured operad whose representations are *Lie pairs*, that is, the triples, $(\mathfrak{g}, \mathfrak{h}, \phi)$, consisting of Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$ as well as a morphism,

$$\phi : \mathfrak{g} \to \mathfrak{h}$$

of Lie algebras. We prove in Theorem 4.1.1 below that there exists a *unique* nontrivial morphism of coloured operads,

$$JB : \mathcal{HS} \longrightarrow \mathcal{LP},$$

which we call the *Jacobi–Bernoulli* morphism because it involves Bernoulli numbers and eventually explains the differential in Ziv Ran's Jacobi–Bernoulli complex. It means the following: given a morphism of Lie algebras, $\phi : \mathfrak{g} \to \mathfrak{h}$, there is a canonically associated morphism of other Lie algebras, $F_\phi : \mathfrak{g} \to \mathcal{T}_{\mathfrak{h}}$, which is determined by ϕ and the Lie algebra brackets [,] in $\mathfrak{h}$. It means, therefore, that there is always a canonically associated nonlinear action of $\mathfrak{g}$ on the space $\mathfrak{h}$ which is twisted by Bernoulli numbers (and is given in local coordinates by (11)).

Thus one can think of the deformation theory of any given Lie pair, $\phi : \mathfrak{g} \to \mathfrak{h}$, in two different worlds:

(1) the world of algebraic morphisms of Lie algebras which allows deformations of three things — of a Lie algebra structure on $\mathfrak{g}$, of a Lie algebra structure on $\mathfrak{h}$ and of a morphism ϕ — and which is governed by the well-known 2-coloured dg operad, $\mathcal{LP}_\infty$, describing pairs of L_∞-algebras and L_∞-morphisms between them, and

(2) the world of formal $\mathfrak{g}$-homogeneous spaces $\mathfrak{h}$ which allows deformations of two things — of a Lie algebra structure on $\mathfrak{g}$ and of its action, $F_\phi : \mathfrak{g} \to \mathcal{T}_\mathfrak{h}$, on $\mathfrak{h}$ — which is governed by the minimal resolution, $\mathcal{HS}_\infty$, of the 2-coloured operad of formal homogeneous spaces which we explicitly describe below in Theorem 2.6.1.

These two worlds have very different deformation theories. The first one is controlled by the L_∞-algebra associated with $\mathcal{LP}_\infty$ as explained in [Merkulov and Vallette 2007, § 5.8]. The second one, as we show in Section 4 below, naturally gives rise to Ziv Ran's Jacobi–Bernoulli complex. This part of our story develops as follows: with a given Lie pair, $\phi : \mathfrak{g} \to \mathfrak{h}$, the Jacobi–Bernoulli morphism *JB* associates a Maurer–Cartan element, γ_ϕ, in the Lie algebra, $\mathfrak{G}_{\mathfrak{g},\mathfrak{h}}$, which describes all possible morphisms, $\mathcal{HS}_\infty \to \mathcal{E}nd_{\mathfrak{g},\mathfrak{h}}$, of 2-coloured operads; this algebra $\mathfrak{G}_{\mathfrak{g},\mathfrak{h}}$ is proven to be a Lie subalgebra of the Lie algebra of coderivations of the graded commutative coalgebra $\bigodot^\bullet(\mathfrak{g}[1] \oplus \mathfrak{h})$ (see Proposition 2.7.1); hence the Maurer–Cartan element γ_ϕ equips this coalgebra with an associated codifferential, d_ϕ, and the resulting complex coincides precisely with the Jacobi–Bernoulli complex of Ran [2004], or, equivalently, with L_∞-structure on $\mathfrak{g} \oplus \mathfrak{h}[-1]$ of Fiorenza and Manetti [2007].

We also briefly discuss in our paper a strong homotopy extension of all the above constructions. It is proven that there exits a morphism of 2-coloured dg operads,

$$JB_\infty : \mathcal{HS}_\infty \longrightarrow \mathcal{LP}_\infty,$$

which associates a formal homogeneous$_\infty$ space to any triple, $(\mathfrak{g}, \mathfrak{h}, \phi_\infty)$, consisting of L_∞-algebras $\mathfrak{g}$ and $\mathfrak{h}$ and a L_∞-morphism $\phi_\infty : \mathfrak{g} \to \mathfrak{h}$. Hence there exists an associated Jacobi–Bernoulli$_\infty$ complex which has the same graded vector space structure as Ziv Ran's Jacobi–Bernoulli complex but a more complicated differential (and hence a more complicated L_∞-algebra structure on the mapping cone of ϕ_∞). We first show an iterative procedure for computing JB_∞ in full generality and then, motivated by the deformation quantization of Poisson structures [Kontsevich 2003], give explicit formulae for the natural composition

$$JB_{\frac{1}{2}\infty} : \mathcal{HS}_\infty \xrightarrow{JB_\infty} \mathcal{LP}_\infty \to \mathcal{LP}_{\frac{1}{2}\infty},$$

where $\mathcal{LP}_{\frac{1}{2}\infty}$ is the 2-coloured operad describing L_∞-morphisms, $\phi_\infty : \mathfrak{g} \to \mathfrak{h}$, between ordinary dg Lie algebras.

1.3. In this paper we extensively use the language of (coloured) operads. For an introduction of the theory of operads we refer to [Markl et al. 2002; Merkulov 2008b] and especially to [Berger and Moerdijk 2007; Kontsevich and Soibelman 2000; Longoni and Tradler 2003]. Some key ideas of this language can be grasped by looking at the basic example of the 2-coloured *endomorphism* operad, $\mathcal{E}nd_{\mathfrak{g},\mathfrak{h}}$, canonically associated to an arbitrary pair of vector spaces $\mathfrak{g}$ and $\mathfrak{h}$ as follows: (a) as an $\mathbb{S}$-module the operad $\mathcal{E}nd_{\mathfrak{g},\mathfrak{h}}$ is given, by definition, by a collection of vector spaces,

$$\left\{ \bigoplus_{m+n=N} \mathbb{K}[\mathbb{S}_N] \otimes_{\mathbb{S}_m \times \mathbb{S}_n} \mathrm{Hom}\big(\mathfrak{g}^{\otimes m} \otimes \mathfrak{h}^{\otimes n},\ \mathfrak{g} \oplus \mathfrak{h}\big) \right\}_{N \geq 1}$$

on which the permutation groups $\mathbb{S}_N$ naturally act; (b) the operadic compositions in $\mathcal{E}nd_{\mathfrak{g},\mathfrak{h}}$ are given, by definition, by plugging the output of one linear map into a particular input (of the same "colour" $\mathfrak{g}$ or $\mathfrak{h}$) of another map. These compositions satisfy numerous "associativity" conditions which, when axiomatized, are used as the definition of an arbitrary 2-coloured operad.

1.4. ***Notations.*** If $V = \bigoplus_{i \in \mathbb{Z}} V^i$ is a graded vector space, then $V[k]$ is the graded vector space with $V[k]^i := V^{i+k}$. For any pair of natural numbers $m < n$ the ordered set $\{m, m+1, \ldots, n-1, n\}$ is denoted by $[m, n]$. The ordered set $[1, n]$ is further abbreviated to $[n]$. For a finite set J the symbol $(-1)^J$ stands for $(-1)^{\text{cardinality of } J}$. For a subdivison, $[n] = I_1 \sqcup I_2 \sqcup \ldots \sqcup I_k$, of the naturally ordered set $[n]$ into k disjoint naturally ordered subsets, we denote by $\sigma(I_1 \sqcup I_2 \sqcup \ldots \sqcup I_k)$ the associated permutation $[n] \to I_1 \sqcup I_2 \sqcup \ldots \sqcup I_k$ and by $(-1)^{\sigma(I_1 \sqcup \ldots \sqcup I_k)}$ the sign of the latter. We work throughout over a field $\mathbb{K}$ of characteristic zero.

2. Operad of Lie actions and its minimal resolution

2.1. ***Motivation.*** Ran [2006; 2004] introduced a notion of Lie atom as a means to describe relative deformation problems in which deformations (controlled by some Lie algebra, say, $\mathfrak{g}$) of a geometric object leave some (controlled by another Lie algebra, say, $\mathfrak{h}$) aspect invariant. More precisely, a *Lie atom* (for *algebra to module* [Ran 2006]) is defined as a collection of data $(\mathfrak{g}, \mathfrak{h}, \langle\ ,\ \rangle, \phi)$ consisting of

(i) a Lie algebra $\mathfrak{g}$ with Lie brackets $[\ ,\ ]$,

(ii) a vector space $\mathfrak{h}$ equipped with a $\mathfrak{g}$-module structure, that is, with a linear map,

$$\begin{array}{rccc} \langle\ ,\ \rangle: & \mathfrak{g} \otimes \mathfrak{h} & \longrightarrow & \mathfrak{h}, \\ & a \otimes m & \mapsto & \langle a, m \rangle, \end{array}$$

satisfying the equation,

$$\langle [a, b], m \rangle = \langle a, \langle b, m \rangle\rangle - (-1)^{ab} \langle b, \langle a, m \rangle\rangle,$$

and

(iii) a morphism, $\phi : \mathfrak{g} \to \mathfrak{h}$, of $\mathfrak{g}$-modules, that is, a linear map from $\mathfrak{g}$ to $\mathfrak{h}$ satisfying the equation

$$\phi([a, b]) = \langle a, \phi(b) \rangle = -(-1)^{ab} \langle b, \phi(a) \rangle$$

for any $a, b \in \mathfrak{g}$.

According to a general philosophy of the deformation theory outlined in Section 1.1, one might attempt to introduce a 2-coloured operad of Lie atoms, resolve it and then study the associated deformation complex of Lie atoms. It is easy to see, however, that the resulting deformation complex must be much larger than the Jacobi–Bernoulli complex and the theory of operads, if pushed in that direction, does not explain the results of Ran [2006; 2004].

This fact forces us to work with different versions of atoms which we call *formal (affine) homogeneous spaces.*

2.2. *Definition.* An *affine homogeneous space* is a collection of data $(\mathfrak{g}, \mathfrak{h}, \langle\ ,\ \rangle, \phi)$ consisting of

(i) a Lie algebra $\mathfrak{g}$ with Lie brackets $[\ ,\ ]$,

(ii) a vector space $\mathfrak{h}$ equipped with a $\mathfrak{g}$-module structure, $\langle\ ,\ \rangle : \mathfrak{g}\otimes\mathfrak{h}\to\mathfrak{h}$, and

(iii) a linear map, $\phi:\mathfrak{g}\to\mathfrak{h}$, satisfying the equation

$$\phi([a,b]) = \langle a, \phi(b)\rangle - (-1)^{ab}\langle b, \phi(a)\rangle$$

for any $a, b\in\mathfrak{g}$.

The only difference between the definition of Lie atom in Section 2.1 and the present one lies in item (iii). This difference is substantial: for example, a pair of Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$ together with a morphism, $\phi:\mathfrak{g}\to\mathfrak{h}$, of Lie algebras makes a Lie atom, $(\mathfrak{g}, \mathfrak{h}, \langle\ ,\ \rangle, \phi)$, with $\langle a, m\rangle := [\phi(a), m]$ but does *not* make an affine homogeneous space as the condition (iii) in Section 2.2 is not satisfied.

The terminology is justified by the following lemma.

Lemma 2.2.1. *An affine homogeneous space structure on a pair*, $(\mathfrak{g}, \mathfrak{h})$, *consisting of a Lie algebra* $\mathfrak{g}$ *and a vector space* $\mathfrak{h}$ *is the same as a morphism of Lie algebras*,

$$F:\mathfrak{g}\longrightarrow \mathcal{T}_{\mathfrak{h}}^{\mathrm{aff}},$$

where $\mathcal{T}_{\mathfrak{h}}^{\mathrm{aff}}$ *is the Lie algebra of affine vector fields on* $\mathfrak{h}$.

Proof. A Lie algebra, $\mathcal{T}_{\mathfrak{h}}$, of smooth formal vector fields on $\mathfrak{h}$ is, by definition, the Lie algebra of derivations of the graded commutative ring,

$$\mathcal{O}_{\mathfrak{h}} := \prod_{n\geq 0}\bigodot^{n}\mathfrak{h}^*,$$

of smooth formal functions on $\mathfrak{h}$. Its subalgebra, $\mathcal{T}_{\mathfrak{h}}^{\mathrm{aff}}$, consists, by definition, of those vector fields, $V\in\mathcal{T}_{\mathfrak{h}}$, whose values, $V(\lambda)$, on arbitrary linear functions, $\lambda\in\mathfrak{h}^*$, lie in the subspace $\mathbb{K}\oplus\mathfrak{h}^*\subset\mathcal{O}_{\mathfrak{h}}$. Thus,

$$\mathcal{T}_{\mathfrak{h}}^{\mathrm{aff}} = \mathsf{End}(\mathfrak{h})\oplus\mathfrak{h},$$

and the map $F : \mathfrak{g} \longrightarrow \mathcal{T}^{\text{aff}}_{\mathfrak{h}}$ gives rise to a pair of linear maps,

$$F_0 : \mathfrak{g} \to \mathfrak{h} \quad \text{and} \quad F_1 : \mathfrak{g} \to \mathsf{End}(\mathfrak{h}).$$

The map F_1 can be equivalently interpreted as a linear map $\hat{F}_1 : \mathfrak{g} \otimes \mathfrak{h} \to \mathfrak{h}$. Now it is a straightforward to check that the conditions for F to be a morphism of Lie algebras are precisely conditions (ii) and (iii) in Section 2.2 for the maps $\phi := F_0$ and $\langle\ ,\ \rangle := -\hat{F}_1$. □

Example 2.2.2. Let $\mathfrak{g}$ and $\mathfrak{h}$ be Lie algebras. And $\psi_t : \mathfrak{g} \to \mathfrak{h}$ is a smooth 1-parameter family of morphisms of Lie algebras, with $-\varepsilon < t < \varepsilon$ and $\varepsilon > 0$. There is a naturally associated affine homogeneous space $(\mathfrak{g}, \mathfrak{h}, \langle\ ,\ \rangle, \phi)$ with

$$\langle a, m\rangle := [\psi_0(a), m] \quad \text{and} \quad \phi := \left.\frac{d\psi_t}{dt}\right|_{t=0}$$

for any $a \in \mathfrak{g}$, $m \in \mathfrak{h}$. Indeed, the condition (ii) in Section 2.2 is obviously satisfied, while the differentiation of the equality,

$$\psi_t([a, b]) = [\psi_t(a), \psi_t(b)],$$

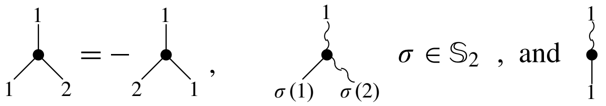
at $t = 0$ gives the condition (iii).

Example 2.2.3. Let $(\mathfrak{g} = \bigoplus_{i\in\mathbb{Z}} \mathfrak{g}^i, [\ ,\ ], d)$ be a nilpotent dg Lie algebra. There is an associated *gauge* action of the nilpotent group $G_0 := \{e^g | g \in \mathfrak{g}^0\}$ on the subspace $\mathfrak{g}^1$ given by

$$\begin{array}{rccl} R: & G_0 \times \mathfrak{g}^1 & \longrightarrow & \mathfrak{g}^1, \\ & (e^g, \Gamma) & \mapsto & e^{ad_g}\Gamma - \dfrac{e^{ad_g} - 1}{ad_g} dg, \end{array}$$

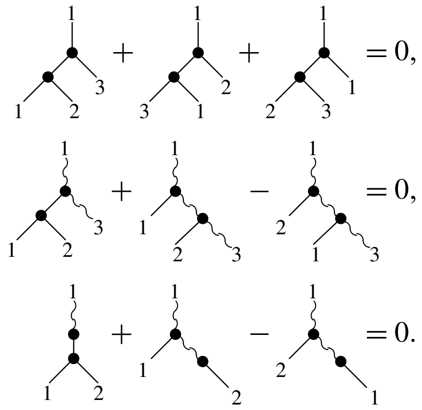
where ad_g stands for the adjoint action by g. This action makes the pair $(\mathfrak{g}^0, \mathfrak{g}^1)$ into an affine homogeneous space.

2.3. Operad of affine homogeneous spaces. This is a 2-coloured operad generated by the labelled corollas[2]



[2] All our graphs are by default directed with the flow running from the bottom to the top.

representing the operations $[\ ,\ ] : \bigwedge^2 \mathfrak{g} \to \mathfrak{g}$, $-\langle\ ,\ \rangle : \mathfrak{g} \otimes \mathfrak{h} \to \mathfrak{h}$ and $\phi : \mathfrak{g} \to \mathfrak{h}$, modulo the obvious relations



The interpretation in Lemma 2.2.1 of the notion of affine homogeneous space prompts us to introduce its generalization.

2.4. *Definition.* A *formal homogeneous space* is a triple, $(\mathfrak{g}, \mathfrak{h}, F)$, consisting of a Lie algebra $\mathfrak{g}$, a vector space $\mathfrak{h}$ and a morphism of Lie algebras,

$$F : \mathfrak{g} \longrightarrow \mathcal{T}_{\mathfrak{h}},$$

where $\mathcal{T}_{\mathfrak{h}}$ is the Lie algebra of smooth formal vector fields on $\mathfrak{h}$.

Example 2.4.1. Let a Lie group G with the Lie algebra $\mathfrak{g}$ act on a vector space $\mathfrak{h}$ viewed as a smooth manifold (that is, the action may not necessarily preserve the linear structure on $\mathfrak{h}$). Then there is an associated formal homogeneous space, $\mathfrak{g} \to \mathcal{T}_{\mathfrak{h}}$.

Example 2.4.2. Let $\mathfrak{g}$ be the Lie algebra of formal vector fields on $\mathbb{R}^n$, and let $\mathbb{R}^{coor}$ be the space of infinite jets of smooth maps, $\mathbb{R}^n \to \mathbb{R}^n$. There is a canonical morphism of Lie algebras,

$$\mathfrak{g} \longrightarrow \mathcal{T}_{\mathbb{R}^{coor}},$$

which, for any point t in $\mathbb{R}^{coor}$, restricts to an isomorphism of vector spaces, $\mathfrak{g} \to (\mathcal{T}_{\mathbb{R}^{coor}})_t$, where $(\mathcal{T}_{\mathbb{R}^{coor}})_t$ is tangent vector space at t. This observation lies in the heart of the so-called *formal geometry* which provides us with a formal homogeneous space approach to many problems in differential geometry such as pseudogroup structures, foliations, characteristic classes, and so on (see [Bernšteĭn and Rosenfel′d 1973] and references cited there).

Example 2.4.3. Let $X \subset \mathfrak{h}$ be an analytic submanifold of $\mathfrak{h} = \mathbb{K}^n$. There is an associated formal homogeneous space $(\mathfrak{g}, \mathfrak{h})$ with $\mathfrak{g}$ being the Lie subalgebra of $\mathcal{T}_{\mathfrak{h}}$ consisting of analytic vector fields on $\mathfrak{h}$ tangent to X along X.

Example 2.4.4. It will be proven below in Theorem 4.1.1 that for any morphism of Lie algebras, $\phi : \mathfrak{g} \to \mathfrak{h}$, there is a canonically associated formal homogeneous space $F_\phi : \mathfrak{g} \to \mathcal{T}_\mathfrak{h}$ with F_ϕ uniquely and rather nontrivially determined by both ϕ and the Lie algebra brackets [,] in $\mathfrak{h}$.

In accordance with the general operadic paradigm [Merkulov and Vallette 2007, § 1], in order to obtain the deformation theory of formal homogeneous spaces one has to first describe the associated operad, $\mathcal{HS}$, and then compute its minimal dg resolution $\mathcal{HS}_\infty$. The first step is very easy.

2.5. ***Operad of formal homogeneous spaces.*** An arbitrary formal vector field, $h \in \mathcal{T}_\mathfrak{h}$, on a vector space $\mathfrak{h}$ is uniquely determined by its Taylor components, $\left\{h_n \in \mathrm{Hom}_\mathbb{K}(\mathfrak{h}^{\odot n}, \mathfrak{h})\right\}_{n\geq 0}$, with

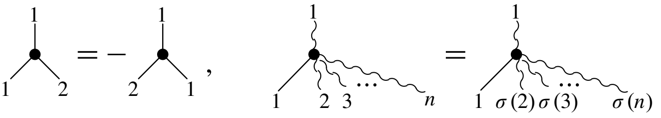
$$h = \sum_a h^a(x)\frac{\partial}{\partial x^a} \quad \overset{1-1}{\longleftrightarrow} \quad \left\{h_n \simeq \frac{1}{n!}\frac{\partial^n h^a(x)}{\partial x^{b_1}\dots\partial x^{b_n}}\bigg|_{x=0}\right\}_{n\geq 0}$$

implying that an arbitrary linear map $F : \mathfrak{g} \to \mathcal{T}_\mathfrak{h}$ is uniquely described by a collection of its components $\left\{F_n \in \mathrm{Hom}_\mathbb{K}(\mathfrak{g}\otimes\mathfrak{h}^{\odot n}, \mathfrak{h})\right\}_{n\geq 0}$. Thus a 2-coloured operad, $\mathcal{HS}$, whose representations,

$$\rho : \mathcal{HS} \longrightarrow \mathcal{E}nd_{\mathfrak{g},\mathfrak{h}},$$

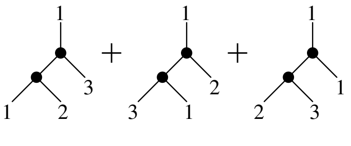
in an arbitrary pair of vector spaces $(\mathfrak{g}, \mathfrak{h})$ are the same as formal homogeneous space structures on $(\mathfrak{g}, \mathfrak{h})$, can be described as follows.

Definition 2.5.1. The *operad formal homogeneous spaces*, $\mathcal{HS}$, is a 2-coloured operad generated[3] by corollas



$\forall\sigma \in \mathbb{S}_{n-1}, n \geq 0,$ (1)

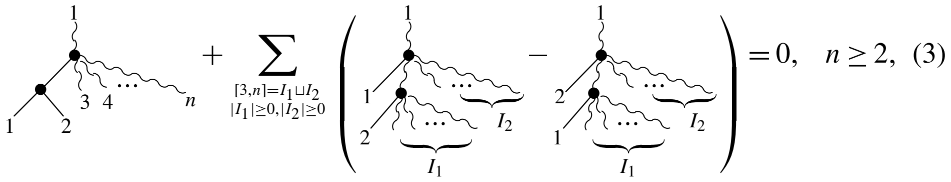
which correspond to the Lie brackets, [,], in $\mathfrak{g}$ and, respectively, to the Taylor component, F_n, of the map F, modulo the relations,



$=0,$ (2)

[3] That is, spanned by all possible graphs built from the corollas described in (1) by gluing the output leg of one corolla to an input leg (with the *same* — "straight" or "wavy" — colour) of another corolla.

corresponding to the Jacobi identities for [,], and



corresponding to the compatibility of F_n with the Lie algebra structures in $\mathfrak{g}$ and $\mathcal{T}_{\mathfrak{h}}$. Here the summation runs over all splittings of the ordered set $[3,n] := \{3,4,\dots,n\}$ into two (possibly empty) disjoint subsets I_1 and I_2.

2.5.2. Dilation symmetry. For any $\lambda \in \mathbb{K}^* := \mathbb{K} \setminus \{0\}$ let

$$\begin{aligned} \psi_\lambda : \mathfrak{h} &\longrightarrow \mathfrak{h}, \\ x &\mapsto \lambda x, \end{aligned}$$

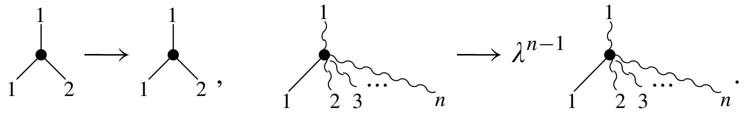
be the associated dilation automorphism of $\mathfrak{h}$. It induces an automorphism of the Lie algebra of formal vector fields,

$$d\psi_\lambda : \mathcal{T}_{\mathfrak{h}} \longrightarrow \mathcal{T}_{\mathfrak{h}}.$$

Therefore, the group $\mathbb{K}^*$ acts on the set of Lie action structures on a given pair, $(\mathfrak{g}, \mathfrak{h})$, of vector spaces,

$$\phi : \mathfrak{g} \to \mathcal{T}_{\mathfrak{h}} \quad \longrightarrow \quad \phi_\lambda := d\psi_\lambda \circ \phi : \mathfrak{g} \to \mathcal{T}_{\mathfrak{h}}.$$

It implies that the group $\mathbb{K}^*$ acts as an automorphism group of the operad $\mathcal{HS}$ as follows:



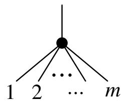
2.6. ***Minimal resolution of*** $\mathcal{HS}$. This is, by definition, a free[4] 2-coloured operad, $\mathcal{HS}_\infty$, equipped with a decomposable differential δ and with an epimorphism of dg operads,

$$\pi : (\mathcal{HS}_\infty, \delta) \longrightarrow (\mathcal{HS}, 0),$$

which induces an isomorphism in cohomology. Here we understand $(\mathcal{HS}, 0)$ as a dg operad with the trivial differential. A minimal resolution is defined uniquely up to an isomorphism.

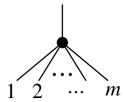
[4] That is, generated by a family of corollas with *no* relations.

Theorem 2.6.1. *The minimal resolution, $\mathcal{HS}_\infty$, is a free 2-coloured operad generated by m-corollas,*

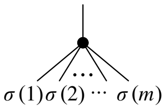


$$m \geq 2, \tag{4}$$

of degree $2 - m$ with skewsymmetric input legs,

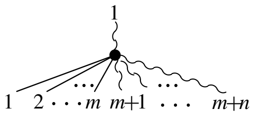


$= (-1)^\sigma$



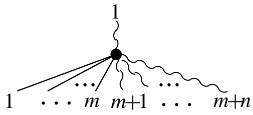
$\forall\, \sigma \in \mathbb{S}_n$,

and (m,n)-corollas,

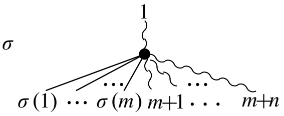


$$m \geq 1, n \geq 0, m+n \geq 2, \tag{5}$$

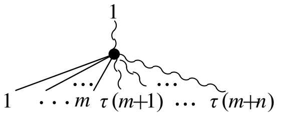
of degree $1 - m$ with skewsymmetric m input legs in "straight" colour and symmetric n input legs in "wavy" colour,



$= (-1)^\sigma$

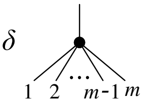


$=$

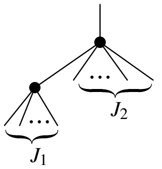


for any $\sigma \in \mathbb{S}_n$ and any $\tau \in \mathbb{S}_m$. The differential is given on the generating corollas by

δ

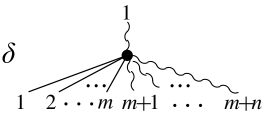


$$= \sum_{\substack{[m]=J_1\sqcup J_2\\ |J_1|\geq 2, |J_2|\geq 1}} (-1)^{J_1(J_2+1)+\sigma(J_1\sqcup J_2)}$$

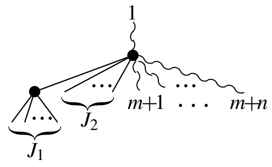


and

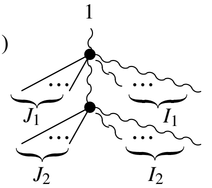
δ



$$= \sum_{\substack{[m]=J_1\sqcup J_2\\ |J_1|\geq 2, |J_2|\geq 0}} (-1)^{(J_1+1)J_2+\sigma(J_1\sqcup J_2)}$$

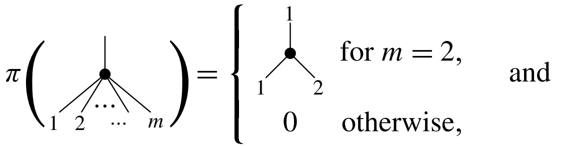


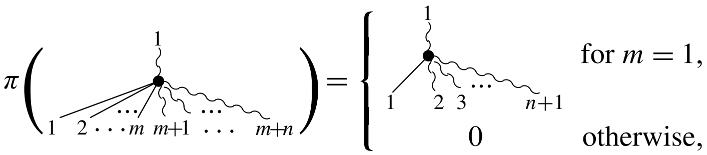
$$- \sum_{\substack{[m]=J_1\sqcup J_2\\ [m+1,m+n]=I_1\sqcup I_2\\ |J_1|\geq 1, |J_2|\geq 1\\ |I_1|\geq 0, |I_2|\geq 0}} (-1)^{J_1(J_2+1)+\sigma(J_1\sqcup J_2)}$$



where $(-1)^{\sigma(J_1\sqcup J_2)}$ is the sign of the permutation $[m] \to [J_1 \sqcup J_2]$.

Proof. It is a straightforward but tedious calculation to check that $\delta^2 = 0$. We define a projection $\pi : \mathcal{HS}_\infty \to \mathcal{HS}$ by its values on the generators,



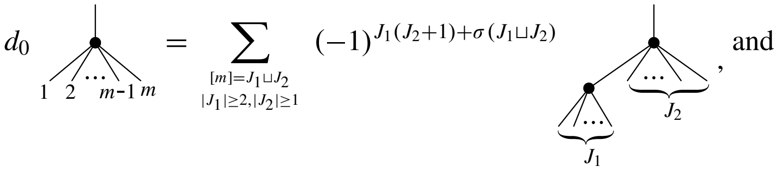


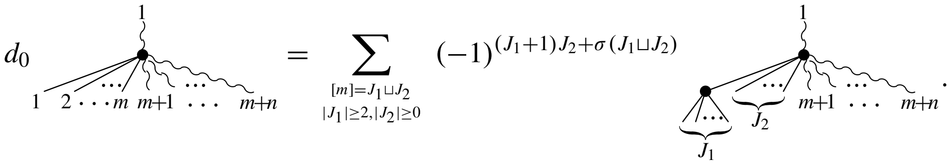
and notice that it commutes with the differentials and induces a surjection in cohomology. Thus to prove that π is a quasiisomorphism it is enough to show that the cohomology $H(\mathcal{HS}_\infty)$ is contained in $\mathcal{HS}$.

Let

$$\ldots \subset F_{-p} \subset F_{-p+1} \subset \ldots \subset F_0 = \mathcal{HS}_\infty$$

be a filtration with F_{-p} being a subspace of $\mathcal{HS}_\infty = \{\mathcal{HS}_\infty(n)\}_{n\geq 1}$ spanned by graphs with at least p wavy internal edges. This filtration is exhaustive and, as each $\mathcal{HS}_\infty(n)$ is a finite-dimensional vector space, bounded, and hence the associated spectral sequence $(E_r, d_r)_{r\geq 0}$ is convergent to $H(\mathcal{HS}_\infty)$. The 0-th term of this sequence has the differential given by



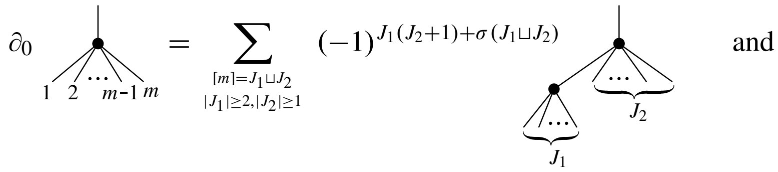


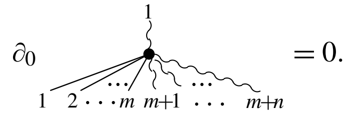
To compute the cohomology $H(E_0, d_0) = E_1$ we consider an increasing filtration,

$$0 \subset \mathcal{F}_0 \subset \ldots \subset \mathcal{F}_p \subset \mathcal{F}_{p+1} \subset \ldots,$$

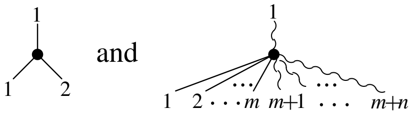
of E_0 with $\mathcal{F}_p$ being a subspace spanned by graphs whose vertices of type (5) have total homological degree $\geq -p$. It is again bounded and exhaustive so the associated spectral sequence, $\{\mathcal{E}_r, \partial_r\}_{r\geq 0}$, converges to E_1. The differential in $\mathcal{E}_0$

is given by

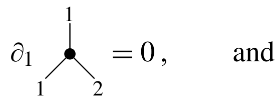

∂_0
1 2 m-1 m
$=\sum_{\substack{[m]=J_1\sqcup J_2\\ |J_1|\geq 2, |J_2|\geq 1}} (-1)^{J_1(J_2+1)+\sigma(J_1\sqcup J_2)}$
J_1
J_2
and

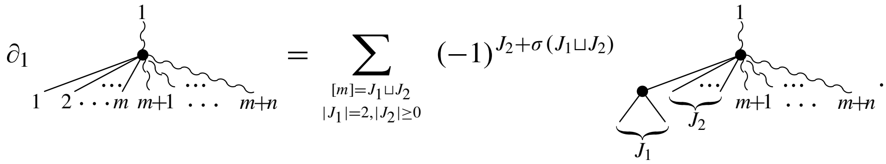


Thus modulo actions of finite groups, the complex $(\mathscr{E}_0, \partial_0)$ is isomorphic to the direct sum of tensor powers of the well-known complex $(\mathscr{L}_\infty, \delta)$, the minimal resolution of the operad of Lie algebras, tensored with trivial complexes. We conclude immediately that $\mathscr{E}_1 = H(\mathscr{E}_0, \partial_0)$ is a 2-coloured operad generated by corollas

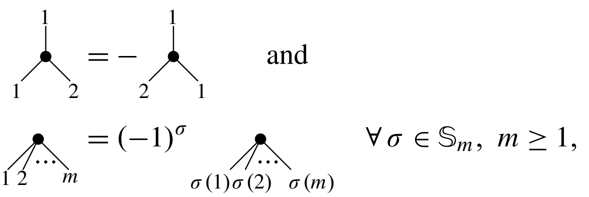


modulo relations (2). The differential ∂_1 in $\mathscr{E}_1$ is given on generators by

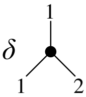


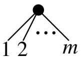
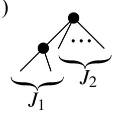

∂_1
1
1 2 ⋯ m m+1 ⋯ m+n
$=\sum_{\substack{[m]=J_1\sqcup J_2\\ |J_1|=2, |J_2|\geq 0}} (-1)^{J_2+\sigma(J_1\sqcup J_2)}$
1
J_1
J_2
m+1 ⋯ m+n
.

Thus, modulo actions of finite groups, the complex $(\mathscr{E}_1, \partial_1)$ is isomorphic to the direct sum of tensor products of trivial complexes with tensor powers of the dg properad $(\mathscr{S}, \delta)$ which is, by definition, generated by corollas


1
1 2
$=-$
1
2 1
and
1 2 m
$=(-1)^\sigma$
$\sigma(1)\sigma(2)$ $\sigma(m)$
$\forall\,\sigma \in \mathbb{S}_m,\ m\geq 1,$

of degrees 0 and, respectively, $1-m$ modulo relation (2). The differential in $\mathcal{S}$ is given by

δ  $=0\,, \qquad$ and

δ  $= \sum_{\substack{[m]=J_1\sqcup J_2\\ |J_1|=2,|J_2|\geq 0}} (-1)^{J_2+\sigma(J_1\sqcup J_2)}$  .

This complex (more precisely, a complex isomorphic to $\mathcal{S}$) was studied in [Merkulov 2008a, § 4.1.1] where it was proven that

$$H(\mathcal{S},\delta)=\mathrm{span}\langle ⫯ \rangle.$$

Thus $\mathcal{E}_2$ is concentrated in degree 0 so all the other terms of both our spectral sequences degenerate and we get $\mathcal{E}_2=\mathcal{E}_\infty=E_1=E_\infty\simeq H(\mathcal{HS}_\infty)$. This fact implies that $H(\mathcal{HS}_\infty)$ is generated by corollas (1) modulo relations (2) and (3) completing thereby the proof. □

Corollary 2.6.2. *The operad, $\mathcal{HS}$, of formal homogeneous spaces is Koszul.*

Proof. By Theorem 2.6.1, the operad $\mathcal{HS}$ admits a quadratic minimal model. The claim then follows from a straightforward analogue of [Merkulov and Vallette 2007, Theorem 34] (see also [Vallette 2007]) for coloured operads. □

2.7. *$\mathcal{HS}_\infty$-algebras as Maurer–Cartan elements.* An *$\mathcal{HS}_\infty$-algebra* structure on a pair of dg vector spaces $(\mathfrak{g},\mathfrak{h})$ is, by definition, a morphism of 2-coloured dg operads, $\rho:(\mathcal{HS}_\infty,\delta)\to(\mathcal{E}nd_{\mathfrak{g},\mathfrak{h}},d)$. First we give an explicit algebraic description of such a structure.

Proposition 2.7.1. *There is a one-to-one correspondence between $\mathcal{HS}_\infty$-algebra structures on a pair of dg vector spaces $(\mathfrak{g},\mathfrak{h})$ and degree 1 codifferentials, D, in the free graded cocommutative coalgebra without counit, $\bigodot^{\bullet\geq 1}(\mathfrak{g}[1]\oplus\mathfrak{h})$, such that*

(a) *D respects the subcoalgebra $\bigodot^{\geq 1}(\mathfrak{g}[1])$, that is*

$$D\Big(\bigodot^{\geq 1}(\mathfrak{g}[1])\Big)\subset\bigodot^{\geq 1}(\mathfrak{g}[1]);$$

(b) *D respects the natural epimorphism of coalgebras,*

$$c:\bigodot^{\bullet\geq 1}(\mathfrak{g}[1]\oplus\mathfrak{h})\to\bigodot^{\geq 1}(\mathfrak{g}[1]),$$

that is, $D\circ c=c\circ D$;

(c) *D is trivial on the subcoalgebra $\bigodot^{\geq 1}\mathfrak{h}$, that is*

$$D\Big(\bigodot^{\geq 1}\mathfrak{h}\Big)=0.$$

Proof. An arbitrary degree 1 coderivation, D, of $\bigodot^{\bullet\geq 1}(\mathfrak{g}[1]\oplus\mathfrak{h})$ is uniquely determined by two collections of degree 1 linear maps,

$$\left\{D'_n:\bigodot^{n}(\mathfrak{g}[1]\oplus\mathfrak{h})=\bigoplus_{p+q=n}\bigwedge^{p}\mathfrak{g}\otimes\bigodot^{q}\mathfrak{h}[p]\to\mathfrak{g}[1]\right\}_{n\geq 1}\quad\text{and}$$

$$\left\{D''_n:\bigodot^{n}(\mathfrak{g}[1]\oplus\mathfrak{h})=\bigoplus_{p+q=n}\bigwedge^{p}\mathfrak{g}\otimes\bigodot^{q}\mathfrak{h}[p]\to\mathfrak{h}\right\}_{n\geq 1}.$$

Conditions (a) and (b) say that D' is zero on all components $\bigwedge^p\mathfrak{g}\otimes\bigodot^q\mathfrak{h}[p]$ with $q\neq 0$, while condition (c) says that D'' is zero on all components $\bigwedge^p\mathfrak{g}\otimes\bigodot^q\mathfrak{h}[p]$ with $p=0$. Thus there is a one-to-one correspondence between degree 1 coderivations, D, in the coalgebra $\bigodot^{\bullet\geq 1}(\mathfrak{g}[1]\oplus\mathfrak{h})$, and morphisms of *non*-differential 2-coloured operads, $\rho:\mathcal{HS}_\infty\to\mathcal{E}nd_{\mathfrak{g},\mathfrak{h}}$, with D'_n being the values of ρ on corollas (4) and D''_n the values of ρ on corollas (5). Having established an explicit correspondence between coderivations D and morphisms ρ, it is now a straightforward computation (which we leave to the reader as an exercise) to check that the compatibility of ρ with the differentials, that is, the equation $\rho\circ\delta=d\circ\rho$, translates precisely into the equation $D^2=0$. □

Recall that a L_∞-*structure* on a vector space V is, by definition, a degree 1 codifferential μ in the free cocommutative coalgebra $\bigodot^{\geq 1}(V[1])$. It is often represented as a collection of linear maps,

$$\left\{\mu_n:\bigwedge^{n}V\to V[2-n]\right\}_{n\geq 1},$$

satisfying a system of quadratic equations which encode the relation $\mu^2=0$. Hence we can reformulate Proposition 2.7.1 in this language as follows.

Corollary 2.7.2. *There is a one-to-one correspondence between $\mathcal{HS}_\infty$-algebra structures on a pair of dg vector spaces $(\mathfrak{g},\mathfrak{h})$ and L_∞-structures, $\{\mu_n:\bigwedge^n V\to V[2-n]\}_{n\geq 1}$, on the vector space $V:=\mathfrak{g}\oplus\mathfrak{h}[-1]$ such that, for any $g_1,\dots,g_p\in\mathfrak{g}$ and $h_1,\dots,h_q\in\mathfrak{g}$ one has*

$$\pi_{\mathfrak{g}}\circ\mu_{p+q}(g_1,\dots,g_p,h_1,\dots,h_q)=0\quad\text{if } q\neq 1,\text{ and}$$
$$\pi_{\mathfrak{h}}\circ\mu_{p+q}(g_1,\dots,g_p,h_1,\dots,h_q)=0\quad\text{if } p=0,$$

where $\pi_{\mathfrak{g}}:V\to\mathfrak{g}$ and $\pi_{\mathfrak{h}}:V\to\mathfrak{h}[-1]$ are the natural projections.

It is straightforward to check that, for any dg spaces $\mathfrak{g}$ and $\mathfrak{h}$, the space of coderivations of the coalgebra $\bigodot^{\bullet\geq 1}(\mathfrak{g}[1]\oplus\mathfrak{h})$ which satisfy conditions (a)–(c) of Proposition 2.7.1 is closed with respect to the ordinary commutator, [,], of coderivations. Let us denote the Lie algebra of such coderivations by $(\mathcal{G}_{\mathfrak{g},\mathfrak{h}}, [\ ,\ ])$. As a vector space,

$$\mathcal{G}_{\mathfrak{g},\mathfrak{h}} \simeq \bigoplus_{n\geq 1}\mathrm{Hom}\Big(\bigwedge^{n}\mathfrak{g},\mathfrak{g}\Big)[2-n] \ \oplus \bigoplus_{n\geq 1, p\geq 0}\mathrm{Hom}\Big(\bigwedge^{n}\mathfrak{g}\otimes\bigodot^{p}\mathfrak{h},\mathfrak{h}\Big)[1-n].$$

Hence we get another useful reformulation of Proposition 2.7.1.

Corollary 2.7.3. *There is a one-to-one correspondence between $\mathcal{HS}_\infty$-algebra structures on a pair of dg vector spaces* $(\mathfrak{g},\mathfrak{h})$ *and Maurer–Cartan elements in the Lie algebra* $(\mathcal{G}_{\mathfrak{g},\mathfrak{h}}, [\ ,\ ])$.

Note that

$$\mathcal{G}_{\mathfrak{g},\mathfrak{h}} = \mathrm{Hom}_{\mathbb{S}}(E, \mathcal{E}nd_{\mathfrak{g},\mathfrak{h}})[-1]$$

where E is the $\mathbb{S}$-bimodule spanned as a vector space by corollas (4) and (5). The Lie algebra we got above in Corollary 2.7.3 is an independent confirmation of the general principle (II) in Section 1.1 (which is the same as [Merkulov and Vallette 2007, Theorem 58]). Hence, applying next principle (III) (or [Merkulov and Vallette 2007, Proposition 66]) we may conclude this subsection with the following observation.

Fact 2.7.4. Let γ be an $\mathcal{HS}_\infty$-algebra structure, $\mathcal{HS}_\infty \xrightarrow{\gamma} \mathcal{E}_{\mathfrak{g},\mathfrak{h}}$, on a pair of dg spaces $\mathfrak{g}$ and $\mathfrak{h}$. The deformation theory of γ is then controlled by the dg Lie algebra $(\mathcal{G}_{\mathfrak{g},\mathfrak{h}}, [\ ,\ ], d := [\gamma,\ ])$.

2.8. ***Geometric interpretations of $\mathcal{HS}_\infty$-algebras.*** There are two ways to understand $\mathcal{HS}_\infty$-algebras geometrically.

The first one uses the language of formal manifolds [Kontsevich 2003]. Let $\mathcal{X}$ be a formal manifold associated with the coalgebra $\bigodot^{\bullet\geq 1}(\mathfrak{g}[1])$ and let $\mathcal{E}$ be a formal manifold associated with the total space of the trivial bundle over $\mathcal{X}$ with typical fiber $\mathfrak{h}$. The structure sheaf of $\mathcal{E}$ is then the coalgebra $\bigodot^{\bullet\geq 1}(\mathfrak{g}[1]\oplus\mathfrak{h})$. We have a natural projection of formal manifolds $\pi : \mathcal{E}\to\mathcal{X}$ and an embedding, $\mathcal{X}\subset\mathcal{E}$, of $\mathcal{X}$ into $\mathcal{E}$ as a zero section. Then a $\mathcal{HS}_\infty$-algebra structure on a pair of vector spaces $\mathfrak{g}$ and $\mathfrak{h}$ is the same as a homological vector field on $\mathcal{E}$ which is tangent to the submanifold $\mathcal{X}$ and vanishes on the fiber of the projection π.

Another geometric picture uses an idea of L_∞-homogeneous formal manifolds:

Proposition 2.8.1. *There is a one-to-one correspondence between representations,*

$$\rho : \mathcal{HS}_\infty \longrightarrow \mathcal{E}nd_{\mathfrak{g},\mathfrak{h}},$$

and the triples, $(\mathfrak{g}, \mathfrak{h}, F_\infty)$, *consisting of a* L_∞*-algebra* $\mathfrak{g}$, *a complex* $(\mathfrak{h}, d)$ *and a* L_∞*-morphism*,

$$F_\infty : \mathfrak{g} \longrightarrow \mathcal{T}_{\mathfrak{h}},$$

where $\mathcal{T}_{\mathfrak{h}}$ *is viewed as a dg Lie algebra equipped with the ordinary commutator*, $[\ ,\ ]$, *of vector fields and with the differential* ∂ *defined by*

$$\partial V := [d, V], \quad \forall V \in \mathcal{T}_{\mathfrak{h}},$$

where d is interpreted as a linear vector field on $\mathfrak{h}$.

The proof is a straightforward calculation (see Section 2.5). We omit the details.

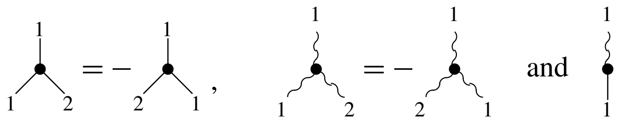
3. Operad of Lie pairs and its minimal resolution

3.1. ***Definition.*** A *Lie pair* is a collection of data $(\mathfrak{g}, \mathfrak{h}, \phi)$ consisting of

(i) Lie algebras $(\mathfrak{g}, [\ ,\ ]_{\mathfrak{g}})$ and $(\mathfrak{h}, [\ ,\ ]_{\mathfrak{h}})$, and

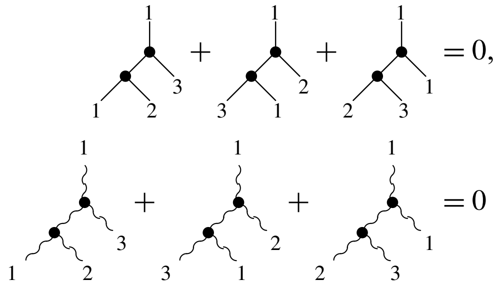
(ii) a morphism, $\phi : \mathfrak{g} \to \mathfrak{h}$ of Lie algebras.

Let $\mathcal{LP}$ be the 2-coloured operad whose representations, $\mathcal{LP} \to \mathcal{E}nd_{\mathfrak{g},\mathfrak{h}}$, are structures of Lie pairs on the vector spaces $\mathfrak{g}$ and $\mathfrak{h}$. This operad *of Lie pairs*, $\mathcal{LP}$, is, therefore, generated by the corollas



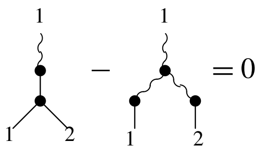
(6)

(which correspond, respectively, to the Lie brackets, $[\ ,\ ]_{\mathfrak{g}}$, Lie brackets $[\ ,\ ]_{\mathfrak{h}}$ and the morphism ϕ) modulo the relations



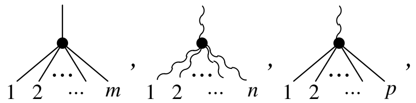
(7)

(corresponding to the Jacobi identities for $[\ ,\ ]_{\mathfrak{g}}$ and $[\ ,\ ]_{\mathfrak{h}}$), and



(corresponding to the compatibility of ϕ with Lie brackets). It is well-known [Markl et al. 2002] that the minimal resolution of $\mathcal{LP}$ is a dg free 2-coloured operad, $\mathcal{LP}_\infty$, whose representations, $\mathcal{LP}_\infty \to \mathcal{E}nd_{\mathfrak{g},\mathfrak{h}}$, describe L_∞-algebra structures in vector spaces $\mathfrak{g}$ and $\mathfrak{h}$ together with a morphism, $\phi_\infty : \mathfrak{g} \to \mathfrak{h}$, of L_∞-algebras. For completeness of the paper we show below a new short proof of this result.

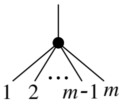
Theorem 3.1.1. *The minimal resolution, $\mathcal{LP}_\infty$, of the operad of Lie pairs is a free 2-coloured operad generated by three families of corollas with skewsymmetric input legs,*



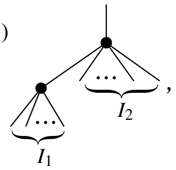
$$m \geq 2, n \geq 2, p \geq 1,$$

of degrees $2-m$, $2-n$ and $1-p$ respectively, and equipped with the differential given by

$$\delta$$

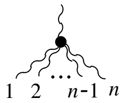


$$= \sum_{\substack{[m]=I_1\sqcup I_2\\ |I_1|\geq 2, |I_2|\geq 1}} (-1)^{I_1(I_2+1)+\sigma(I_1\sqcup I_2)}$$

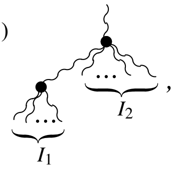


,

$$\delta$$



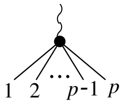
$$= \sum_{\substack{[m]=I_1\sqcup I_2\\ |I_1|\geq 2, |I_2|\geq 1}} (-1)^{I_1(I_2+1)+\sigma(I_1\sqcup I_2)}$$



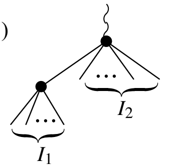
,

(8)

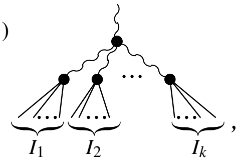
$$\delta$$



$$= \sum_{\substack{[m]=I_1\sqcup I_2\\ |I_1|\geq 2, |I_2|\geq 1}} (-1)^{I_2(I_1+1)+\sigma(I_1\sqcup I_2)}$$



$$+ \sum_{\substack{[p]=I_1\sqcup\ldots\sqcup I_k\\ |I_i|\geq 1, k\geq 2}} (-1)^{\varepsilon+\sigma(I_1\sqcup\ldots\sqcup I_k)}$$

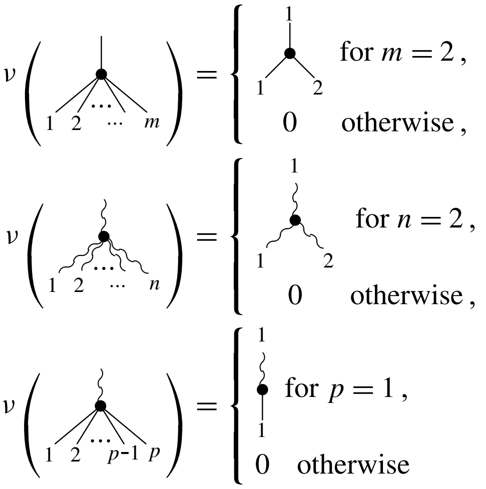


,

where

$$\varepsilon = 1 + \sum_{i=1}^{k-1} I_i(i-1+I_{i+1}+\ldots+I_k).$$

Proof. The projection $\nu : \mathcal{LP}_\infty \to \mathcal{LP}$ defined by

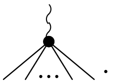


commutes with the differentials and is obviously surjective in cohomology. Thus to prove that π is a quasiisomorphism it is enough to show that $H(\mathcal{HS}_\infty) = \mathcal{HS}$ which in turn would follow if one proves that the cohomology $H(\mathcal{HS}_\infty)$ is concentrated in degree zero.

Let

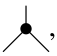
$$\ldots \subset F_{-q} \subset F_{-q+1} \subset \ldots \subset F_0 = \mathcal{HS}_\infty$$

be a filtration with F_{-q} being a subspace of $\mathcal{LP}_\infty = \{\mathcal{LP}_\infty(n)\}_{n\geq 1}$ spanned by graphs with at least q vertices of the form



This filtration is exhaustive and, as each $\mathcal{L}_\infty\mathcal{P}(n)$ is a finite-dimensional vector space, bounded, and hence the associated spectral sequence $(E_r, d_r)_{r\geq 0}$ is convergent to $H(\mathcal{HS}_\infty)$. The 0-th term of this sequence has the differential given by formulae (8) without the second sum. Hence the complex (E_0, d_0) is isomorphic, modulo actions of finite groups, to the tensor products of trivial complexes with two copies of the classical complex $\mathcal{L}_\infty$ and the complex $\mathcal{S}$ defined in the proof of Theorem 2.6.1. Hence its cohomology $E_1 = H(E_0, d_0)$ is generated by corollas (6) and is concentrated, therefore, in degree 0. This proves that $H(\mathcal{HS}_\infty)$ is concentrated in degree zero which in turn implies the required result. □

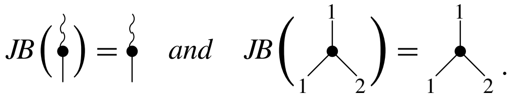
4. The Jacobi–Bernoulli morphism and its strong homotopy generalization

4.1. ***The Jacobi–Bernoulli morphism.*** The following result shows that, modulo actions of the dilation group $\mathbb{K}^*$ on the operad $\mathcal{HS}$ (see Section 2.5.2), there exists a *unique* nontrivial morphism of 2-coloured operads $\mathcal{HS} \to \mathcal{LP}$ which is identity on the generators, , with pure “straight” colour.

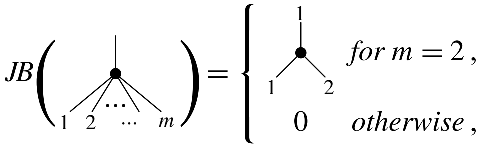
Theorem 4.1.1. *There is a unique morphism of* 2*-coloured dg operads,*

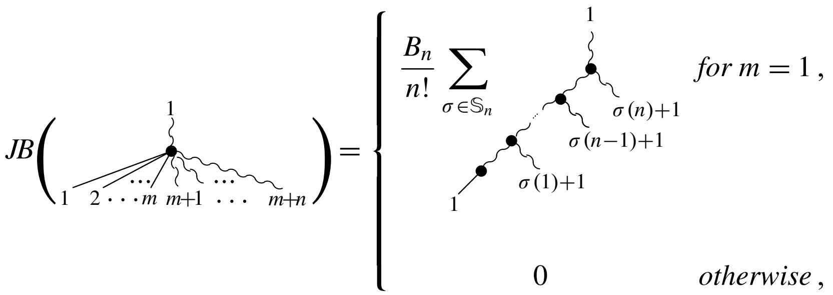
$$JB : (\mathcal{HS}_\infty, \delta) \longrightarrow (\mathcal{LP}, 0)$$

such that



It is given on the generators by





where B_n *are the Bernoulli numbers, that is,* $\sum_{n\geq 0} \frac{B_n}{n!} z^n = \frac{z}{e^z - 1}$, *in particular,* $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, *and so on.*

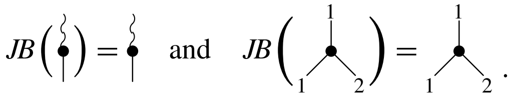
Proof. Since $\mathcal{LP}$ is concentrated in degree zero, the required morphism factors through the canonical projection,

$$JB : (\mathcal{HS}_\infty, \delta) \xrightarrow{\pi} (\mathcal{HS}, 0) \longrightarrow (\mathcal{LP}, 0),$$

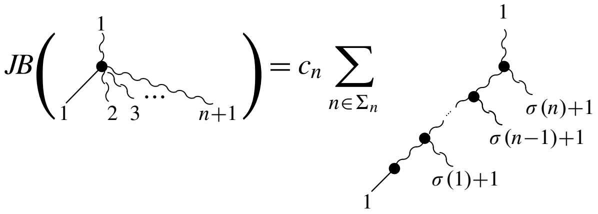
for some morphism of 2-coloured operads, $\mathcal{HS} \longrightarrow \mathcal{LP}$, which we denote by the same letter JB. Thus to prove Theorem 4.1.1 we have to show the existence of a unique morphism of operads,

$$JB : \mathcal{HS} \longrightarrow \mathcal{LP},$$

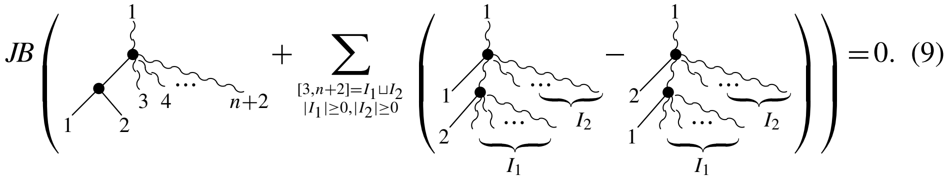
such that



For equivariance reasons it must be of the form



for some $c_n \in \mathbb{K}$ with $c_0 = 1$. Thus to prove the theorem we have to show that there exists a unique collection of numbers $\{c_n\} \in \mathbb{K}$ such that, for any $n \geq 0$,



We claim that the above equation gives an iterative procedure which uniquely specifies c_{n+1} in terms of $c_{\leq n}$ starting with $c_0 = 1$. Equation (9) is a sum of elements of the operad $\mathcal{LP}$ with all input legs of "wavy" colour being symmetrized; it is easier to control the relevant combinatorics by slightly changing the viewpoint: Equation (9) holds in $\mathcal{LP}$ if and only if it holds for an arbitrary representation $\rho_{\mathfrak{g},\mathfrak{h}} : \mathcal{LP} \to \mathcal{E}nd_{\mathfrak{g},\mathfrak{h}}$, that is, if for arbitrary pair of Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$ and a morphism $\phi : \mathfrak{g} \to \mathfrak{h}$ one has $\rho_{\mathfrak{g},\mathfrak{h}}(9) \equiv 0$, which, as it is not hard to see, is equivalent to the following system of equations (with $c_0 = 1$),

$$\sum_{\substack{0\leq k,l\leq n\\ k+l\leq n}} c_k c_{n+1-k}\big([\phi(a_1)@b^l, \phi(a_2)@b^k] - [\phi(a_2)@b^l, \phi(a_1)@b^k]\big)@b^{n-k-l}$$

$$+c_n[\phi(a_1), \phi_2(a_2)]@b^n = 0 \qquad (10)$$

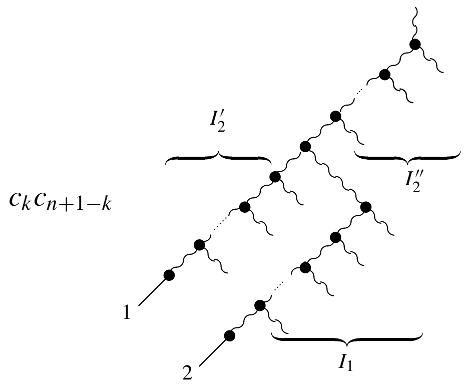
for any $a_1, a_2 \in \mathfrak{g}$ and $b \in \mathfrak{h}$. Here we used the notation of Ran [2004]

$$x@b^k := [\ldots[[x,\underbrace{b], b], \ldots, b]}_{k}, \qquad \forall\, x, b \in \mathfrak{h}.$$

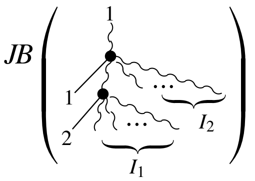
The second summand in (10) corresponds to the first summand in (9) while the summand

$$c_k c_{n+1-k}[\phi(a_1)@b^l, \phi(a_2)@b^k]@b^{n-k-l}$$

in (10) corresponds to the summand



in the image



$$, \quad |I_1| = k, \ |I_2| = n - k,$$

which is uniquely determined by a decomposition, $I_2 = I_2' \sqcup I_2''$, of the indexing set I_2 into two disjoint subsets with

$$|I_2'| = l \text{ (and hence with } |I_2''| = n - k - l).$$

Equation (10) can be rewritten as follows,

$$\begin{aligned} &c_{n+1} \sum_{k=0}^{n} \big([\phi(a_1), \phi(a_2)@b^k]@b^{n-k} - [\phi(a_2), \phi(a_1)@b^k]@b^{n-k} \big) \\ &= -c_n[\phi(a_1), \phi_2(a_2)]@b^n \\ &- \sum_{\substack{1 \le k \le n \\ 0 \le l \le n \\ k+l \le n}} c_k c_{n+1-k} \big([\phi(a_1)@b^l, \phi(a_2)@b^k] - [\phi(a_2)@b^l, \phi(a_1)@b^k] \big) @b^{n-k-l}. \end{aligned}$$

implying that if system (9) has a solution, then it is unique. For example, for $n = 0$, we have

$$2c_1 = -c_0 = -1,$$

while for $n = 1$,

$$3c_2 = -c_1 - c_1^2 = \frac{1}{4}.$$

It was proven in [Ran 2004] (see Equation 1.2.4 there) that the collection $c_n = B_n/n!$, where B_n are the Bernoulli numbers, does solve system of equations (10), completing the proof of existence and uniqueness of the morphism JB. □

Corollary 4.1.2. *For every morphism of Lie algebras $\phi : \mathfrak{g} \to \mathfrak{h}$ there is a canonically associated structure of formal $\mathfrak{g}$-homogeneous space on $\mathfrak{h}$, that is, a morphism of Lie algebras,*

$$F_\phi : \mathfrak{g} \longrightarrow \mathcal{T}_{\mathfrak{h}},$$

given in local bases $\{e_a\}$ in $\mathfrak{g}$ and $\{e_\alpha\}$ in $\mathfrak{h}$ as follows,

$$F_\phi(e_a) = \sum_{n\geq 0} \frac{B_n}{n!} \phi_a^{\gamma_1} C_{\gamma_1\beta_1}^{\gamma_2} C_{\gamma_2\beta_2}^{\gamma_3} \dots C_{\gamma_n\beta_n}^{\alpha} t^{\beta_1} t^{\beta_2} \dots t^{\beta_n} \frac{\partial}{\partial t^\alpha}, \tag{11}$$

where $C_{\alpha\beta}^{\gamma}$ are the structure constants of Lie brackets in $\mathfrak{h}$, $[e_\alpha, e_\beta] = \sum_\gamma C_{\alpha\beta}^{\gamma} e_\gamma$, ϕ_a^α are the structure constants of the morphism ϕ, $\phi(e_a) = \sum_\alpha \phi_a^\alpha e_\alpha$, and $\{t^\alpha\}$ is the dual basis in $\mathfrak{h}^*$.

Corollary 4.1.3. *For every morphism of dg Lie algebras $\phi : \mathfrak{g} \to \mathfrak{h}$ there is a canonically associated codifferential, D_ϕ, in the free coalgebra $J := \bigodot^\bullet(\mathfrak{g}[1] \oplus \mathfrak{h})$ making the data (J, D_ϕ) into the Jacobi–Bernoulli complex as defined in [Ran 2004].*

Proof. Morphism of Lie algebras $\phi : \mathfrak{g} \to \mathfrak{h}$ gives rise to an associated morphism of 2-coloured operads,

$$\rho_\phi : \mathcal{LP} \longrightarrow \mathcal{E}nd_{\mathfrak{g},\mathfrak{h}}.$$

The composition,

$$\gamma_\phi : \mathcal{HS}_\infty \xrightarrow{\mathcal{JB}} \mathcal{LP} \xrightarrow{\rho_\phi} \mathcal{E}nd_{\mathfrak{g},\mathfrak{h}},$$

gives, by Proposition 2.7.1, rise to an associated codifferential D_ϕ. The rest of the proof is just a comparison of D_ϕ with the codifferential defined in [Ran 2004]. □

Corollary 4.1.4. *For every morphism of dg Lie algebras $\phi : \mathfrak{g} \to \mathfrak{h}$ there is a canonically associated L_∞-algebra structure on the vector $\mathfrak{g} \oplus \mathfrak{h}[-1]$.*

Proof. The claimed L_∞-structure is given by the morphism of operads γ_ϕ as above and Corollary 2.7.3. A straightforward inspection shows that this structure is identical to the one constructed in [Fiorenza and Manetti 2007] with the help of the explicit homotopy transfer formulae of [Kontsevich and Soibelman 2000; Merkulov 1999]. □

4.2. ***Morphisms of L_∞-algebras.*** The following theorem generalizes all the above constructions to the case of an arbitrary morphism, $\phi_\infty : \mathfrak{g} \to \mathfrak{h}$, of L_∞-algebras. The proof given below provides us with an iterative construction of the morphism JB_∞ (and hence with the associated differential in the Jacobi–Bernoulli complex or, equivalently, a L_∞-algebra structure on the mapping cone $\mathfrak{g} \oplus \mathfrak{h}[-1]$).

Theorem 4.2.1. *There exists a morphism of 2-coloured dg operads,*

$$\mathcal{JB}_\infty : (\mathcal{HS}_\infty, \delta) \longrightarrow (\mathcal{LP}_\infty, \delta)$$

making the diagram,

$$\begin{tikzcd}
\mathcal{HS}_\infty \arrow[r, "JB_\infty"] \arrow[d, "\pi"'] & \mathcal{LP}_\infty \arrow[d, "\nu"] \\
\mathcal{HS} \arrow[r, "JB"'] & \mathcal{LP}
\end{tikzcd}$$

commutative.

Proof. We have a solid arrow diagram,

$$\begin{tikzcd}
 & \mathcal{LP}_\infty \arrow[d, "\nu"] \\
\mathcal{HS}_\infty \arrow[r, "JB"'] \arrow[ru, dotted, "JB_\infty"] & \mathcal{LP}
\end{tikzcd}$$

with morphism ν being a surjective quasiisomorphism and the operad $\mathcal{HS}_\infty$ being cofibrant. Then the existence of the dotted arrow JB_∞ making the diagram above commutative follows immediately from the model category structure on operads. In fact, one can see it directly using an analogue of the classical Whitehead lifting trick (first used in the theory of CW complexes in algebraic topology): let ν^{-1} be an arbitrary section of the surjection ν in the category of dg spaces; as a first step in the inductive procedure we set $JB_\infty(C_0) := \nu^{-1} \circ JB(C_0)$ on degree 0 generating corollas, C_0, of the operad $\mathcal{HS}_\infty$. Assume by induction that the values of a morphism JB_∞ are already defined on all generating corollas of degrees $\geq -r$, and let C_{r+1} be a generating corolla of degree $-r-1$. As $\delta(C_{r+1})$ is a linear combination of graphs built from corollas of degrees $\geq -r$, $JB_\infty(\delta C_{r+1})$ is a well-defined element of $\mathcal{LP}_\infty$. Moreover, as JB_∞ commutes, by the induction assumption, with the differentials, we have an equation in the complex $(\mathcal{LP}_\infty, \delta)$,

$$\delta JB_\infty(\delta C_{r+1}) = 0.$$

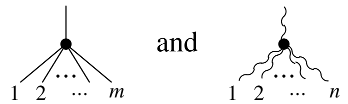
Since there are no nontrivial cohomology classes in $(\mathcal{LP}_\infty, \delta)$ of degree $-r$ for $r \geq 1$, we must have,

$$JB_\infty(\delta C_{r+1}) = \delta e_{r+1}$$

for some $e_{r+1} \in \mathcal{LP}_\infty$. We finally set $JB_\infty(C_{r+1}) := e_{r+1}$ completing thereby the inductive construction of the required morphism JB_∞. □

Corollary 4.2.2. *For every morphism of L_∞-algebras, $\phi_\infty : \mathfrak{g} \to \mathfrak{h}$, there is an associated codifferential, D_∞, in the free coalgebra $J := \bigodot^\bullet(\mathfrak{g}[1] \oplus \mathfrak{h})$ which coincides precisely with Ziv Ran's Jacobi–Bernoulli codifferential in the case of $\mathfrak{g}$, $\mathfrak{h}$ being dg Lie algebras and ϕ a morphism of dg Lie algebras.*

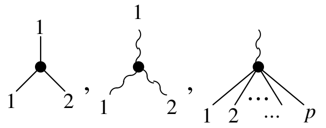
4.3. ***L_∞-morphisms of dg Lie algebras.*** Let I be the ideal in the free nondifferential operad $\mathcal{LP}_\infty$ generated by corollas



with $m \geq 3$ and $n \geq 3$, and let (I, dI) be the differential closure of I in the dg operad $(\mathcal{LP}_\infty, \delta)$. The quotient operad,

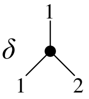
$$\mathcal{LP}_{\frac{1}{2}\infty} := \frac{\mathcal{LP}_\infty}{(I, dI)}$$

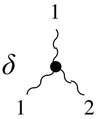
is a differential 2-coloured operad generated by corollas

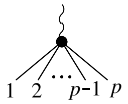


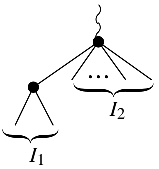
$p \geq 1,$

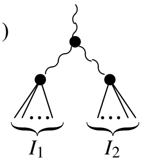
modulo relations (7); the differential is given on the generators by

δ  $= 0,$

δ  $= 0,$

δ 

$= \sum_{\substack{[m]=I_1\sqcup I_2\\ |I_1|=2,|I_2|\geq 1}} (-1)^{p-1+\sigma(I_1\sqcup I_2)}$ 

$+ \sum_{\substack{[p]=I_1\sqcup I_2\\ |I_1|,|I_2|\geq 1}} (-1)^{\sigma(I_1\sqcup I_2)}$  .

Representations,

$$\mathcal{LP}_{\frac{1}{2}\infty} \to \mathcal{E}nd_{\mathfrak{g},\mathfrak{h}},$$

of this dg operad are the same as triples, $(\mathfrak{g}, \mathfrak{h}, F_\infty)$, consisting of ordinary dg Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$ together with a L_∞-morphism, $F_\infty : \mathfrak{g} \to \mathfrak{h}$, between them. Thus this operad describes a special class of representations of the operad $\mathcal{LP}_\infty$ which is, probably, the most important one in applications. For example, for any smooth manifold M, the triple, $(\bigwedge^\bullet \mathcal{T}_M, \mathcal{D}_M^{poly}, F_K)$, consisting of a Schouten Lie algebra of polyvector fields on M, the Hochschild dg Lie algebra, $\mathcal{D}_M^{poly}$, of polydifferential operators and Kontsevich's formality morphism

$$F_K : \bigwedge^{\bullet} \mathcal{T}_M \to \mathcal{D}_M^{poly}$$

is a representation of $\mathcal{LP}_{\frac{1}{2}\infty}$.

It is not hard to describe *explicitly* the quotient part,

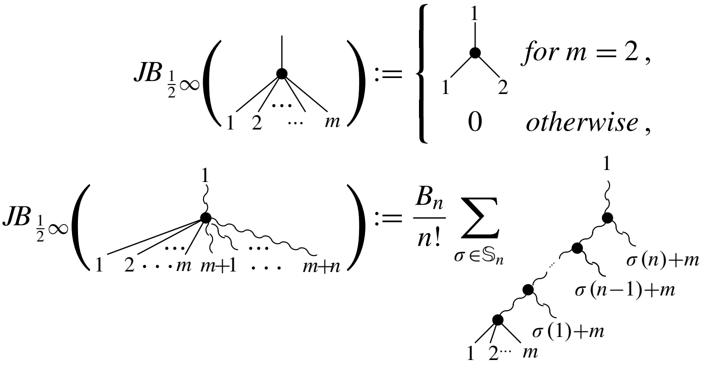
$$JB_{\frac{1}{2}\infty} : \mathcal{HS}_\infty \xrightarrow{JB_\infty} \mathcal{LP}_\infty \xrightarrow{proj} \mathcal{LP}_{\frac{1}{2}\infty},$$

of a morphism JB_∞.

Theorem 4.3.1. *The morphism of* 2*-coloured dg operads,*

$$JB_{\frac{1}{2}\infty} : (\mathcal{HS}_\infty, \delta) \longrightarrow \left(\mathcal{LP}_{\frac{1}{2}\infty}, \delta\right)$$

is given on the generators by



where B_n are the Bernoulli numbers.

The proof is similar to that of Theorem 4.1.1. We omit the details.

Acknowledgement

This paper is an expanded comment to the talk of Ziv Ran at the Mittag-Leffler Institute in Stockholm in May 2007. The author is grateful to an anonymous referee for helpful remarks.

References

[Berger and Moerdijk 2007] C. Berger and I. Moerdijk, "Resolution of coloured operads and rectification of homotopy algebras", pp. 31–58 in *Categories in algebra, geometry and mathematical physics*, Contemp. Math. **431**, Amer. Math. Soc., Providence, RI, 2007. MR 2342815 Zbl 0562.94001

[Bernšteĭn and Rosenfel′d 1973] I. N. Bernšteĭn and B. I. Rosenfel′d, "Homogeneous spaces of infinite-dimensional Lie algebras and the characteristic classes of foliations", *Uspehi Mat. Nauk* **28**:4(172) (1973), 103–138. MR 54 #3714 Zbl 0289.57011

[Fiorenza and Manetti 2007] D. Fiorenza and M. Manetti, "L_∞ structures on mapping cones", *Algebra Number Theory* **1**:3 (2007), 301–330. MR 2361936

[Kontsevich 2003] M. Kontsevich, "Deformation quantization of Poisson manifolds", *Lett. Math. Phys.* **66**:3 (2003), 157–216. MR 2005i:53122 Zbl 1058.53065

[Kontsevich and Soibelman 2000] M. Kontsevich and Y. Soibelman, "Deformations of algebras over operads and the Deligne conjecture", pp. 255–307 in *Conférence Moshé Flato 1999* (Dijon, September 5–8, 1999), vol. I, edited by G. Dito and D. Sternheimer, Math. Phys. Stud. **21**, Kluwer Acad. Publ., Dordrecht, 2000. MR 2002e:18012 Zbl 0972.18005

[van der Laan 2002] P. van der Laan, "Operads up to homotopy and deformations of operad maps", preprint, 2002. arXiv math.QA/0208041

[Longoni and Tradler 2003] R. Longoni and T. Tradler, "Homotopy inner products for cyclic operads", preprint, 2003. arXiv math.AT/0312231

[Manetti 2005] M. Manetti, "Lie description of higher obstructions to deforming submanifolds", preprint, 2005. arXiv math.AG/0507287

[Markl et al. 2002] M. Markl, S. Shnider, and J. Stasheff, *Operads in algebra, topology and physics*, Mathematical Surveys and Monographs **96**, American Mathematical Society, Providence, RI, 2002. MR 2003f:18011 Zbl 1017.18001

[Merkulov 1999] S. A. Merkulov, "Strong homotopy algebras of a Kähler manifold", *Internat. Math. Res. Notices* 3 (1999), 153–164. MR 2000h:32026 Zbl 0995.32013 arXiv math.AG/9809172

[Merkulov 2005] S. A. Merkulov, "Nijenhuis infinity and contractible differential graded manifolds", *Compos. Math.* **141**:5 (2005), 1238–1254. MR 2006g:58008 Zbl 1075.18010 math.DG/0403244

[Merkulov 2006] S. A. Merkulov, "PROP profile of Poisson geometry", *Comm. Math. Phys.* **262**:1 (2006), 117–135. MR 2006j:53122 arXiv math.DG/0401034

[Merkulov 2008a] S. A. Merkulov, "Graph complexes with loops and wheels", in *Algebra, Arithmetic and Geometry: the Manin Festschrift*, edited by Y. Tschinkel and Y. G. Zarhin, Birkhaüser, 2008.

[Merkulov 2008b] S. A. Merkulov, "Lectures on props, Poisson geometry and deformation quantization", pp. 223–258 in *Poisson Geometry in Mathematics and Physics*, edited by G. Dito et al., Contemporary Mathematics **450**, American Mathematical Society, Providence, RI, 2008. To appear.

[Merkulov and Vallette 2007] S. A. Merkulov and B. Vallette, "Deformation theory of representations of prop(erad)s", preprint, 2007. To appear in *J. Reine Angew. Math.* arXiv 0707.0889

[Ran 2004] Z. Ran, "Lie atoms and their deformations", preprint, 2004. To appear in *Geomet. Funct. Anal.* arXiv math/0412204

[Ran 2006] Z. Ran, "Jacobi cohomology, local geometry of moduli spaces, and Hitchin connections", *Proc. London Math. Soc.* (3) **92**:3 (2006), 545–580. MR 2007e:14013 Zbl 1095.14010

[Vallette 2007] B. Vallette, "A Koszul duality for PROPs", *Trans. Amer. Math. Soc.* **359**:10 (2007), 4865–4943. MR 2320654 Zbl pre05172045

Communicated by Yuri Manin
Received 2007-10-10 Revised 2008-01-17 Accepted 2008-03-09

sm@math.su.se *Department of Mathematics, Stockholm University,*
10691 Stockholm, Sweden

ALGEBRA AND NUMBER THEORY 2:4(2008)

On the algebra of some group schemes

Daniel Ferrand

The algebra of a finite group over a field k of characteristic zero is known to be a projective separable k-algebra; but these separable algebras are of a very special type, characterized by Brauer and Witt.

In contrast with that, we prove that *any* projective separable k-algebra is a quotient of the group algebra of a suitable *group scheme*, finite étale over k. In particular, any finite separable field extension $K \subset L$, even a noncyclotomic one, may be generated by a finite étale K-group scheme.

Introduction

Following Wedderburn and Brauer, the rational group algebra $\mathbb{Q}\langle\Gamma\rangle$ of a finite group Γ may be described as follows: its center is a product $K_1 \times \cdots \times K_s$ of fields, each isomorphic to a subfield of the cyclotomic extension $\mathbb{Q}(\zeta_m)$, where m is the exponent of Γ, and the group algebra itself is a product $A_1 \times \cdots \times A_s$, where A_i is a central simple K_i-algebra.

In general, the factors K_i of the center are not *equal* to cyclotomic extensions of $\mathbb{Q}$, i.e., they cannot be generated themselves by a finite group, as shown by the following example (which I owe to Vincent Beck). Let p be a prime; denote by $L = \mathbb{Q}(\zeta_p)$ the cyclotomic extension of level p. Let $S \subset \mathbb{F}_p^\times \simeq \mathrm{Gal}(L/\mathbb{Q})$ be any subgroup, and write $K = L^S$ for its invariant subfield. Then one has an isomorphism of $\mathbb{Q}$-algebras

$$\mathbb{Q}\langle\mathbb{F}_p \rtimes S\rangle \to \mathbb{Q}\langle S\rangle \times \mathrm{End}_K(L).$$

MSC2000: primary 20C05; secondary 14L15, 16S34, 16S35, 16W30.

Keywords: group algebra, finite étale group scheme, Weil restriction, separable algebra.

(The map $\mathbb{Q}\langle\mathbb{F}_p \rtimes S\rangle \to \mathrm{End}_K(L)$ is defined by $(a, s) \mapsto (\zeta_p^i \mapsto \zeta_p^{a+si})$). The center of this group algebra is thus equal to $\mathbb{Q}\langle S\rangle \times K$; for a suitable choice of S, the extension $\mathbb{Q} \to K$ is not cyclotomic.

The question of characterizing which algebras may occur as a quotient of the algebra of a finite group was already raised by Schur, but solved only around 1950, by Brauer and Witt. Even then, they got a characterization only up to Morita equivalence; see [Fontaine 1971; Yamada 1974].

In this paper, we shift this problem a little: the base ring k is now a semilocal ring, containing the field $\mathbb{Q}$, and we are dealing with projective separable k-algebras; this notion is the natural generalization of the "absolute semisimplicity" which is used when k is a field, and it is equivalent, for commutative algebras, to being étale.

We prove in Section 5 that *any* projective separable k-algebra is a quotient of the group algebra of a suitable *group scheme*, finite étale over k. In particular, we prove that any finite separable field extension $K \subset L$, even a noncyclotomic one, may be generated by a finite étale K-group scheme. Roughly speaking, a separable algebra is a finite product of matrix algebras twisted by some étale torsor; the group scheme we propose is a finite group generating the split form of the algebra, but twisted by the same torsor.

Despite a formal analogy with the Brauer–Witt theory, our result does not add much to it: even in the simplest case, that of the quaternions, our method gives a *nonconstant* group scheme for generating this $\mathbb{R}$-algebra, in fact a group which is a definitely twisted form of the dihedral group D_4.

Notation. The categories in use will be denoted by the following symbols:

Gp stands for the category of groups.

For a commutative ring k,

k-Al denotes the category of k-algebras; its objects are thus the ring morphisms $k \to A$ such that the image of k is contained in the center of A.

k-Alc denotes the category of *commutative* k-algebras.

We say that a commutative ring k is connected if its spectrum $\mathrm{Spec}(k)$ is connected; that is, if k is not isomorphic to a proper finite product of rings.

Local rank. In this paper, most of the k-modules are locally free, but the base rings are seldom connected, and the rank of these modules seldom constant. Moreover, the constructions we have in mind, because they use the Weil restriction relative to a finite flat morphism $X \to S$, cannot be done locally on X. Thus we can't avoid introducing and using the *local* rank of a locally free k-module M of finite type, which is the map

$$n : \mathrm{Spec}(k) \to \mathbb{N}, \qquad \mathfrak{p} \mapsto \mathrm{rank}_{k_{\mathfrak{p}}}(M_{\mathfrak{p}}).$$

This map is constant on each connected component of $\mathrm{Spec}(k)$. We need words to refer to these things; we propose the terms

- *k-integer* for a locally constant map $\mathrm{Spec}(k) \to \mathbb{N}$, and
- *k-rank* (of a locally free k-module M of finite type) for the local rank alluded to above.

For a k-integer n, we can define the k-algebra $\mathbf{M}_n(k)$, the k-group scheme $\mu_{n,k}$, and any other object which may be defined locally on $\mathrm{Spec}(k)$ for the Zariski topology. We have to be careful with the connected components where the k-integer vanishes: $\mathbf{M}_0(k) = 0$ (endomorphisms of the null space), but $\mu_{0,k} = \mathbf{G}_{m,k}$, since for every invertible element x, one has $x^0 = 1$.

1. The algebra of a group scheme

1.1. *The algebra of a constant group.* At first, let us recall, in the case of a *constant* group scheme, the well known constructions of its ring of functions (also called its representing algebra), and the construction of the algebra of such a group. Compare [Waterhouse 1979, Chapter 2].

1.1.1. Let k be a commutative ring. For a finite group Γ, we let $\prod_\Gamma k$ denote the ring of the maps from the set Γ to k (we reserve the notation k^Γ for the ring of invariants when is given an action of Γ on k); it is contravariant in Γ. The product in Γ induces a morphism of commutative k-algebras

$$\prod_\Gamma k \to \prod_{\Gamma\times\Gamma} k \simeq \prod_\Gamma k \otimes_k \prod_\Gamma k.$$

More explicitly, let $(\delta_\rho)_{\rho\in\Gamma}$ be the basis made up with the usual Kronecker maps $\delta_\rho : \Gamma \to k$; then the morphism above is given by

$$\delta_\rho \mapsto \sum_{\sigma\tau=\rho} \delta_\sigma \otimes \delta_\tau .$$

We thus get what is sometimes called a k-Hopf-algebra, but we prefer to emphasize the scheme point of view: $\mathrm{Spec}\big(\prod_\Gamma k\big)$ is a k-group scheme; it is called the constant k-group Γ, and it is denoted by Γ_k.

1.1.2. The group algebra of Γ over k will be denoted by $k\langle\Gamma\rangle$, instead of $k[\Gamma]$, because the symbol with brackets $k[V]$ often denotes also the commutative ring of algebraic, or regular, functions on the scheme V; see [Waterhouse 1979, 4.5], for example.

Recall that the group algebra $k\langle\Gamma\rangle$ is the free k-module based on the set Γ, with multiplication induced by that of Γ. It is equipped with a commutative coproduct given by the map

$$k\langle\Gamma\rangle \to k\langle\Gamma\rangle \otimes_k k\langle\Gamma\rangle, \qquad \sum_\sigma a_\sigma \sigma \mapsto \sum_\sigma a_\sigma \sigma \otimes \sigma$$

The dual of this ring is isomorphic to the ring of functions on Γ; namely, consider the k-linear isomorphism

$$\prod_\Gamma k \to \operatorname{Hom}_k(k\langle\Gamma\rangle, k), \qquad \delta_\rho \mapsto \Big(\sum_\sigma a_\sigma \sigma \mapsto a_\rho\Big). \tag{1-1}$$

The right-hand side (the dual as a k-module) may be endowed with the multiplication coming from dualizing the coproduct mentioned above; then this k-linear map is an isomorphism of k-algebras, as one can check immediately.

By dualizing the preceding morphism, we get the isomorphism

$$\operatorname{Hom}_k\Big(\prod_\Gamma k,\ k\Big) \to k\langle\Gamma\rangle, \qquad \xi \mapsto \sum_{\sigma\in\Gamma} \xi(\delta_\sigma)\sigma.$$

In Section 1.3, we will proceed along the same lines to define the algebra of a k-group scheme, and to get, in Proposition 1.3.2, an analogue of this well-known result:

Lemma 1.1.1. *Let Γ be a finite group, and let $k \to A$ be a k-algebra, whose multiplicative group is denoted by $A^\times$. Then one has an isomorphism of bifunctors*

$$\operatorname{Hom}_{k\text{-}\mathsf{Al}}(k\langle\Gamma\rangle, A) \xrightarrow{\sim} \operatorname{Hom}_{\mathsf{Gp}}(\Gamma, A^\times).$$

1.2. ***The multiplicative group functor.*** Let $k \to A$ be a k-algebra; recall that the ring A is not assumed to be commutative, but the morphism is required to send k into the center of A.

We will denote by $\mathbf{G}_{m,A/k}$ the multiplicative group functor of A, namely the functor

$$\mathbf{G}_{m,A/k} : k\text{-}\mathsf{Alc} \to \mathsf{Gp}, \qquad k' \mapsto \mathbf{G}_{m,A/k}(k') = (k' \otimes_k A)^\times.$$

It is also written $\mathrm{GL}_1(A)$ by Borel, and μ^A by Demazure and Gabriel.

Lemma 1.2.1 [Waterhouse 1979, 7.5; Demazure and Gabriel 1970, p. 149]. *Suppose that the k-algebra A is a projective (i.e., locally free) k-module of finite type. Then the functor $\mathbf{G}_{m,A/k}$ is representable by an affine k-group scheme of finite type.*

Sketch of proof. Let $A^D = \operatorname{Hom}_k(A, k)$ be the linear dual of A, and let

$$S = \operatorname{Sym}_k(A^D)$$

be the symmetric algebra of that module. Let $\xi \in A^D \otimes_k A$ be the element that corresponds to the identity of A under the canonical isomorphism $A^D \otimes_k A \xrightarrow{\sim} \operatorname{End}_k(A)$.

(If you prefer more explicit things, you can choose a basis (e_i) of A, and the dual basis (X_i) of A^D; this allows you to write $\xi = \sum X_i \otimes e_i$.) We must consider this element

$$\xi \in A^D \otimes_k A \subset S \otimes_k A$$

as the *generic element* of A, since each specification $S \to k'$ of the parameters towards a commutative k-algebra k', gives rise to an element in $k' \otimes_k A$, namely the image of ξ.

Since $S \otimes_k A$ is a finite and locally free S-module, we dispose of the usual norm $N : S \otimes_k A \to S$, namely, $N(x) = \det(y \mapsto xy)$. Then we can check easily that the algebra of fractions $S_{N(\xi)}$ represents $\mathbf{G}_{m,A/k}$ as a functor from k-Alc to the category of sets.

The group structure is induced by the algebra morphism $S_{N(\xi)} \to S_{N(\xi)} \otimes_k S_{N(\xi)}$ given by extending to symmetric algebra, and localizing, the linear map

$$A^D \xrightarrow{(\text{mult.})^D} (A \otimes_k A)^D \xleftarrow{\sim} A^D \otimes_k A^D \subset \operatorname{Sym}_k(A^D) \otimes_k \operatorname{Sym}_k(A^D). \qquad \square$$

1.3. ***The group-algebra.*** We now deal with group schemes over k, instead of constant groups; their category will be denoted by k-Gp. We are looking for something like a left adjoint to the multiplicative group functor, that is, a functor which, to a k-group scheme G, would associate a k-algebra $k\langle G\rangle$, endowed with an isomorphism of functors

$$\operatorname{Hom}_{k\text{-Al}}(k\langle G\rangle,\ A) \quad \xrightarrow{\sim} \quad \operatorname{Hom}_{k\text{-Gp}}(G, \mathbf{G}_{m,A}).$$

Fortunately, in what follows, we have available strong enough finiteness assumptions to guarantee that these objects exist.

1.3.1. We will try to stick to the notations and terminology used in [Waterhouse 1979]. We recall some of them:

Let $G = \operatorname{Spec}(R)$ be an affine k-group scheme.

- $u : k \to R$ stands for the canonical map,
- $m : R \otimes_k R \to R$ stands for the multiplication,
- $\Delta : R \to R \otimes_k R$ denotes the coproduct,
- $\varepsilon : R \to k$ denotes the counit,
- S indicates the coinverse.

Suppose that R is finite and locally free as a k-module; let $R^D = \operatorname{Hom}_k(R, k)$ be the linear dual of R; then the k-module R^D may be endowed with a structure of a (usually noncommutative) k-algebra: the product is defined as the map

$$R^D \otimes_k R^D \simeq (R \otimes_k R)^D \xrightarrow{\Delta^D} R^D;$$

the associativity of this multiplication comes from the associativity of the product in the group G, and the map $\varepsilon^D : k \to R^D$ actually defines a morphism of algebras since it corresponds to the unity of G.

Definition 1.3.1. Let $G = \mathrm{Spec}(R)$ be an affine k-group scheme with R finite and locally free as a k-module. We define the *k-algebra of the group G*, and we note $k\langle G\rangle$ the linear dual R^D endowed with the algebra structure given above.

Let $k \to k'$ be a commutative k-algebra. We denote by $G_{k'} = \mathrm{Spec}(k' \otimes_k R)$ the group scheme over k' obtained by base change. For G finite and locally free, there is an isomorphism

$$k\langle G\rangle \otimes_k k' \xrightarrow{\sim} k'\langle G_{k'}\rangle$$

since one has the following sequence of standard isomorphisms, the first one coming from the local freeness of R over k:

$$k\langle G\rangle \otimes_k k' = \mathrm{Hom}_k(R, k) \otimes_k k' \simeq \mathrm{Hom}_k(R, k') \simeq \mathrm{Hom}_{k'}(k' \otimes_k R, k') = k'\langle G_{k'}\rangle.$$

Proposition 1.3.2. *Let $G = \mathrm{Spec}(R)$ be an affine k-group scheme with R finite and locally free as a k-module.Then, for any finite and locally free k-algebra $k \to A$, there is a bijection of functors in G*

$$\mathrm{Hom}_{k\text{-}\mathsf{Al}}(k\langle G\rangle,\ A) \xrightarrow{\sim} \mathrm{Hom}_{k\text{-}\mathsf{Gp}}(G, \mathbf{G}_{m,A/k}).$$

Proof. For every k-algebra $k' \in k\text{-}\mathsf{Alc}$, consider the multiplications in the group $G(k')$ and in the ring $k\langle G\rangle \otimes_k k'$, that is the multiplications in $\mathrm{Hom}_{k\text{-}\mathsf{Alc}}(R, k')$ and in $\mathrm{Hom}_k(R, k')$; they are both given by dualizing the same map $\Delta : R \to R \otimes_k R$; therefore, from the mere inclusion

$$\mathrm{Hom}_{k\text{-}\mathsf{Alc}}(R, k') \subset \mathrm{Hom}_k(R, k')$$

we deduce a morphism of multiplicative monoids

$$G(k') \to k' \otimes_k k\langle G\rangle.$$

Since every element of $G(k')$ has an inverse, its image is invertible in the ring $k' \otimes_k k\langle G\rangle$. We have thus defined a morphism of (ordinary) groups, which is functorial in k',

$$G(k') = \mathrm{Hom}_{k\text{-}\mathsf{Alc}}(R, k') \ \to\ (\mathrm{Hom}_k(R, k'))^\times = \mathbf{G}_{m,k\langle G\rangle/k}(k'),$$

that is a morphism of group functors on k-Alc

$$G \to \mathbf{G}_{m,k\langle G\rangle/k}. \tag{1-2}$$

A morphism of k-algebras $k\langle G\rangle \to A$ clearly induces a morphism of group functors

$$\mathbf{G}_{m,k\langle G\rangle/k} \to \mathbf{G}_{m,A/k}.$$

By composition with (1-2), we get a map which is functorial in G

$$\mathrm{Hom}_{k\text{-}\mathsf{Al}}(k\langle G\rangle,\ A) \to \mathrm{Hom}_{k\text{-}\mathsf{Gp}}(G, \mathbf{G}_{m,A/k}). \tag{1-3}$$

Conversely, let $G \to \mathbf{G}_{m,A/k}$ be a morphism of k-group schemes. We want to produce from it a morphism of k-algebras $k\langle G\rangle \to A$. Since the k-group $\mathbf{G}_{m,A/k}$ is not finite over k (except if $k = A$), the above elementary construction does not allow to define something like $k\langle \mathbf{G}_{m,A/k}\rangle$, nor, of course, a morphism $k\langle \mathbf{G}_{m,A/k}\rangle \to A$. At first sight, we are given, for each commutative k-algebra k', the two solid arrows in the following diagram, and we need to complete it with the dotted one:

$$\begin{tikzcd}
\mathrm{Hom}_{k\text{-}\mathsf{Alc}}(R, k') \arrow[rr] \arrow[dr] & & k' \otimes_k A \\
& \mathrm{Hom}_k(R, k') \arrow[ur, dotted] &
\end{tikzcd}$$

To achieve this, we must use the representability of $\mathbf{G}_{m,A/k}$ (Lemma 1.2.1): since the groups G and $\mathbf{G}_{m,A/k}$ are affine, the given morphism $G \to \mathbf{G}_{m,A/k}$ is associated to a morphism of k-algebras

$$\mathrm{Sym}_k(A^D)_{N(\xi)} \to R.$$

The compatibility with the group laws implies the commutativity of the squares

$$\begin{tikzcd}
A^D \arrow[r] \arrow[d, "(\mathrm{mult.})^D"'] & \mathrm{Sym}_k(A^D)_{N(\xi)} \arrow[r] \arrow[d] & R \arrow[d, "\Delta"] \\
A^D \otimes_k A^D \arrow[r] & \mathrm{Sym}_k(A^D)_{N(\xi)} \otimes_k \mathrm{Sym}_k(A^D)_{N(\xi)} \arrow[r] & R \otimes_k R
\end{tikzcd}$$

By dualizing, one gets a k-linear map

$$R^D \to A$$

(Recall that both R and A are locally free k-modules of finite rank). Now the above diagram shows that this map is compatible with Δ^D and with the multiplication in A. We have thus defined a map

$$\mathrm{Hom}_{k\text{-}\mathsf{Al}}(k\langle G\rangle,\ A) \leftarrow \mathrm{Hom}_{k\text{-}\mathsf{Gp}}(G, \mathbf{G}_{m,A/k}).$$

which we can easily check to be the inverse of (1-3). □

1.4. ***Another approach to the group algebra.*** We now sketch a very general definition of an algebra that looks like a "group algebra", and which may appear to be more natural than the previous one, if less explicit; but, this new algebra can be proven to satisfy the required left adjoint property only when the group is finite étale; and, for these groups, this algebra coincides with the previous one.

1.4.1. Let k be a ring, and let G be a group functor on k-Alc; let $F : k\text{-Alc} \to k\text{-Al}$ be the functor defined by

$$F(k') = k'\langle G(k')\rangle.$$

Thus, $F(k')$ is the usual k'-algebra of the discrete group $G(k')$.

Let $\tilde{F}$ be the sheaf associated to F for the étale topology. The algebra $\tilde{F}(k)$ of global sections of this sheaf is equipped with the map

$$\mathrm{Hom}_{k\text{-Gp}}(G, \mathbf{G}_{m,A/k}) \to \mathrm{Hom}_{k\text{-Al}}(\tilde{F}(k),\ A), \tag{1-4}$$

defined as follows: a morphism of functors $G \to \mathbf{G}_{m,A}$ gives, for each $k' \in k$-Alc, a group homomorphism

$$G(k') \to \mathbf{G}_{m,A}(k') = (k' \otimes_k A)^\times$$

which gives rise to a morphism of k'-algebras

$$F(k') = k'\langle G(k')\rangle \to k' \otimes_k A.$$

We thus get a morphism of sheaves from $\tilde{F}$ to the sheaf $k' \mapsto k' \otimes_k A$, and, finally, taking their global sections, we get a morphism of k-algebras $\tilde{F}(k) \to A$. It is not clear if the map (1-4) should be bijective without strong hypothesis.

Proposition 1.4.1. *For a finite étale k-group G, the group algebra $k\langle G\rangle$, defined in Definition 1.3.1, is canonically isomorphic to the ring of global sections of the étale sheaf associated to the functor $k' \mapsto k'\langle G(k')\rangle$, considered above.*

For the proof, we need the following variant of the Dedekind independence result.

Lemma 1.4.2. *Let $G = \mathrm{Spec}(R)$ be a finite étale k-group, and let $k\langle G\rangle$ be its group algebra in the sense of Definition 1.3.1. Then, for $k' \in k$-Alc, the morphism*

$$k'\langle G(k')\rangle \to k\langle G\rangle \otimes_k k' = \mathrm{Hom}_k(R, k')$$

is injective. In other words, the elements of $G(k') = \mathrm{Hom}_{k\text{-Alc}}(R, k')$ are linearly independent in $\mathrm{Hom}_k(R, k')$.

Moreover, there exists a finite étale k-algebra k' for which this morphism is an isomorphism.

We may suppose that $\mathrm{Spec}(k')$ is connected, and we rewrite k' as k for simplicity. Let $g_1, \dots, g_s \in G(k)$ be distinct elements, seen as k-morphisms $R \to k$; since R is étale over k, each morphism $g_i : R \to k$ gives a projective R-module structure on k, in other words, each kernel $J_i = \mathrm{Ker}(g_i) \subset R$ is generated by an idempotent $e_i \in R$. These ideals are pairwise comaximal: in fact, the ring $R/J_i \simeq k$ being assumed to be connected, the image of an idempotent e_j is either 0, and then $J_i = J_j$ and $i = j$, or this image is 1, implying that $J_i + J_j = R$.

The Chinese remainder theorem then implies that the morphism induced by the s morphisms g_i,

$$R \to k^s,$$

is surjective. This, in turn, clearly implies that the g_i are linearly independent.

Since R is finite and étale over k, it is split by a finite étale morphism $k \to k'$, i.e one has an isomorphism of k'-algebras

$$k' \otimes_k R \xrightarrow{\sim} \prod_{G(k')} k'.$$

It is now clear that any linear form $R \to k'$ is a linear combination, with coefficients in k', of the projections $k' \otimes_k R \to k'$, which indeed correspond to elements in $G(k')$.

Proof of the proposition. Denote by H the functor given by $H(k') = k\langle G\rangle \otimes_k k' = \mathrm{Hom}_k(R, k')$; it is clearly a sheaf in the étale topology. We have to show that the functor map $F \to H$ induces an isomorphism

$$\tilde{F} \xrightarrow{\sim} H.$$

According to the previous lemma, for any k' étale over k, the map $F(k') \to H(k')$ is injective, and it is even bijective if $k \to k'$ factors trough a k_0 which splits R.

Then, following [Artin 1962, chapter II], we use the construction $F \rightsquigarrow F^+$ to get the associated sheaf $\tilde{F}$; roughly speaking, a section of $F^+(U)$ "is" a coherent family of sections of F given locally on U, that is, an element of the kernel

$$F(U') \rightrightarrows F(U' \times_U U') \ ,$$

where $U' \to U$ is an étale covering. Since F is a subfunctor of the sheaf H, it is a "separated" presheaf, or, with Artin's notations, F satisfy the property $(+)$; therefore, by [Artin 1962, II.1.4], F^+ is already the associated sheaf $\tilde{F}$. But the injectivity of $F \to H$, and the definition of F^+, alluded to above, imply that the map $\tilde{F} \to H$ is still injective. Now, over the "covering" $\mathrm{Spec}(k_0) \to \mathrm{Spec}(k)$, the morphism $F \to H$ becomes an isomorphism, thus also the morphism $\tilde{F} \to H$; as $\tilde{F}$ and H are sheaves, the map $\tilde{F} \to H$ is an isomorphism everywhere. □

1.5. ***Galois description.*** We now translate essentially the same considerations to the more concrete situation of Galois extensions. Let $k \to K$ be a finite Galois extension of fields, with Galois group $\pi = \mathrm{Gal}(K/k)$; suppose the k-group scheme G be split by K, i.e., that G_K is isomorphic to the constant (finite) group Γ_K; this group G is thus associated to an action of π on Γ, that is to a morphism

$$\pi \to \mathrm{Aut}_{\mathsf{Gp}}(\Gamma).$$

(See [Waterhouse 1979, 6.3] or [Demazure and Gabriel 1970, II.5.1.7, p. 237].) The ring of polynomial maps on G is then given by

$$R = \Big(\prod_{\Gamma} K\Big)^{\pi},$$

where the action of $\sigma \in \pi$ on an element $x : \Gamma \to K \in \prod_{\Gamma} K$ is

$${}^{\sigma}x = (\gamma \mapsto \sigma(x(\sigma^{-1}\gamma))).$$

Proposition 1.5.1. *The k-group-algebra of G is the ring*

$$k\langle G\rangle = (K\langle\Gamma\rangle)^{\pi},$$

where both the coefficients in K and the basis Γ *are acted on by the Galois group* π.

To prove this we go back to the isomorphism (1-1)

$$\varphi : \prod_{\Gamma} K \xrightarrow{\sim} \operatorname{Hom}_K(K\langle\Gamma\rangle, K), \quad \delta_\gamma \mapsto \Big(\sum_{\gamma'} a_{\gamma'}\gamma' \mapsto a_\gamma\Big),$$

and we must see that it induces an isomorphism

$$\Big(\prod_{\Gamma} K\Big)^{\pi} \xrightarrow{\sim} \operatorname{Hom}_k(K\langle\Gamma\rangle^{\pi}, k).$$

The morphism φ may be characterized as follows: Given $(x : \Gamma \to K) \in \prod_{\Gamma} K$, the K-linear map $\varphi(x)$ is defined on the basis Γ, by $\varphi(x)(\gamma) = x(\gamma)$. It is clear that φ is π-equivariant (if $\operatorname{Hom}_K(K\langle\Gamma\rangle, K)$ is acted on by π, both on $K\langle\Gamma\rangle$ and on K); taking the invariants, we thus get an isomorphism

$$\Big(\prod_{\Gamma} K\Big)^{\pi} \xrightarrow{\sim} \operatorname{Hom}_K(K\langle\Gamma\rangle, K)^{\pi}.$$

Since $k \to K$ is a Galois extension, one has $k = K^{\pi}$. It remains to produce an isomorphism

$$\operatorname{Hom}_K(K\langle\Gamma\rangle, K)^{\pi} \xrightarrow{\sim} \operatorname{Hom}_{K^{\pi}}((K\langle\Gamma\rangle)^{\pi}, K^{\pi}).$$

We will apply to $V = K\langle\Gamma\rangle$ the following general result: let V be a K-vector space endowed with a *semilinear* action of π; that means that the group V is equipped with a morphism $\pi \to \operatorname{Aut}_{\mathbb{Z}}(V)$ such that, for $\sigma \in \pi$, $x \in V$ and $\lambda \in K$, one has $\sigma(\lambda x) = \sigma(\lambda)\sigma(x)$. The group V^{π} is then a vector space over K^{π}, and we have an isomorphism

$$K \otimes_{K^{\pi}} V^{\pi} \xrightarrow{\sim} V$$

(See [Bourbaki 1981, A V, §10, Prop. 7, p. 61], for example.) From this we deduce the sequence of isomorphisms

$$\operatorname{Hom}_K(V, K)^{\pi} \simeq \operatorname{Hom}_K(K \otimes_{K^{\pi}} V^{\pi}, K)^{\pi} \simeq \operatorname{Hom}_{K^{\pi}}(V^{\pi}, K)^{\pi} \simeq \operatorname{Hom}_{K^{\pi}}(V^{\pi}, K^{\pi}).$$

Remark 1.5.2. It is easy to show an example where $k\langle G\rangle \not\subseteq k\langle\Gamma\rangle$: with notations as above, suppose there exist an element $\gamma \in \Gamma$, and an element $a \in K$, having both a trivial stabilizer for the action of π. Let

$$x = \sum_{\sigma\in\pi} \sigma(a)\sigma(\gamma) \quad \in K\langle\Gamma\rangle.$$

It is clear that x is π-invariant and does not lie in $k\langle\Gamma\rangle$. Thus, in this case, $(K\langle\Gamma\rangle)^\pi \not\subseteq K^\pi\langle\Gamma^\pi\rangle$.

2. Group generation of finite étale algebras

2.1. ***The Weil restriction.*** Let $k \to K$ be a finite étale morphism of (commutative) rings. The direct image, or Weil restriction, or norm, is the functor

$$\mathsf{R}_{K/k} : K\text{-}\mathsf{Alc} \to k\text{-}\mathsf{Alc}$$

which is left adjoint to the base change functor; for any (commutative) k-algebra A, and any (commutative) K-algebra A', we thus have a bijection

$$\mathrm{Hom}_{k\text{-}\mathsf{Alc}}(\mathsf{R}_{K/k}(A'), A) \quad \xrightarrow{\sim} \quad \mathrm{Hom}_{K\text{-}\mathsf{Alc}}(A', K \otimes_k A),$$

which is functorial in A and in A'. The existence and the main properties of this functor are explained in [Demazure and Gabriel 1970, I.1.6.6, p. 30] and in [Bosch et al. 1990, 7.6].

Suppose that K is a product $K = K_1 \times K_2$; then a K-algebra A' also decomposes as a product $A' = A'_1 \times A'_2$, where A'_i is a K_i-algebra, and one has an isomorphism

$$\mathsf{R}_{K/k}(A') \simeq \mathsf{R}_{K_1/k}(A'_1) \otimes_k \mathsf{R}_{K_2/k}(A'_2).$$

In particular, in the split case $K = k^d$, where $A' = \prod_{i=1}^d A_i$, we have

$$\mathsf{R}_{k^d/k}(A_1 \times \cdots \times A_d) = A_1 \otimes_k \cdots \otimes_k A_d.$$

(From a scheme-theoretic viewpoint, the Weil restriction transforms disjoint unions into products.)

We will use this functor only for K-algebras coming from k, that is, for algebras of the form $A' = K \otimes_k B$ for a k-algebra B. The bijection above then reads as

$$\mathrm{Hom}_{k\text{-}\mathsf{Alc}}(\mathsf{R}_{K/k}(K \otimes_k B), A) \xrightarrow{\sim} \mathrm{Hom}_{k\text{-}\mathsf{Alc}}(B, K \otimes_k A).$$

We may regard the ring $\mathsf{R}_{K/k}(K \otimes_k B)$ as the form of the tensor product $B^{\otimes d}$ twisted by the $\mathfrak{S}_d$-torsor P associated to K; this torsor is the functor $P : k\text{-}\mathsf{Alc} \to \mathsf{Ens}$ defined by

$$P(k') = \mathrm{Isom}_{k'\text{-}\mathsf{Alc}}(k' \otimes_k K, k'^d)$$

This point of view, if easy to conceive, is a little hard writing down (but see [Ferrand 1998, 6.2.2 and 7.3.2], and Section 2.2 below). Anyway, it is clear that for the trivial étale algebra $K = k^d$, the k-algebra $\mathsf{R}_{K/k}(K \otimes_k B)$ is indeed isomorphic to $B^{\otimes d}$, due to the above isomorphism, or to the explicit bijections

$$\begin{aligned}\mathrm{Hom}_{k\text{-}\mathsf{Alc}}(B, K \otimes_k A) \simeq \mathrm{Hom}_{k\text{-}\mathsf{Alc}}(B, A^d) \simeq \mathrm{Hom}_{k\text{-}\mathsf{Alc}}(B, A)^d \\ \simeq \mathrm{Hom}_{k\text{-}\mathsf{Alc}}(B^{\otimes d}, A).\end{aligned}$$

We will use the same symbol $\mathsf{R}_{K/k}$ for the Weil restriction of schemes; in particular, if $G' = \mathrm{Spec}(A')$ is an affine K-group, we write $\mathsf{R}_{K/k}(G')$ for the scheme $\mathrm{Spec}(\mathsf{R}_{K/k}(A'))$; letting $G = \mathrm{Spec}(\mathsf{R}_{K/k}(A'))$, one has, for any $k' \in k\text{-}\mathsf{Alc}$,

$$G(k') = \mathrm{Hom}_{k\text{-}\mathsf{Alc}}(\mathsf{R}_{K/k}(A'), k') = \mathrm{Hom}_{K\text{-}\mathsf{Alc}}(A', K \otimes_k k') = G'(K \otimes_k k').$$

(This isomorphism shows, among other properties, that $G = \mathsf{R}_{K/k}(G')$ is a k-group).

The Weil restriction of a constant K-group is usually *not* a constant k-group.

2.2. ***The twisted Klein group*** $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\boldsymbol{\mu}_{2,\mathbb{C}})$**.** As an example which anticipates the next result, and which is also used later, we now compute the Weil restriction from $\mathbb{C}$ to $\mathbb{R}$, of the group $\mu_{2,\mathbb{C}} = \mathrm{Spec}(\mathbb{C}[T]/(T^2 - 1))$; this Weil restriction will also appear as a twisted form of the Klein group $\mu_2 \times \mu_2$. Let A be the $\mathbb{R}$-algebra of regular functions on this Weil restriction; so we have

$$\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}}) = \mathrm{Spec}(A).$$

We find that

$$A = \mathbb{R}[X, Y]/(X^2 - Y^2 - 1, XY).$$

(To see this, the usual trick is to construct the Weil restriction in order for the canonical morphism

$$\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})_{\mathbb{C}} \longrightarrow \mu_{2,\mathbb{C}} \tag{2-1}$$

to exist. So, we start with the map $\mathbb{C}[T] \longrightarrow \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[X, Y]$ given by

$$T \mapsto 1 \otimes X + i \otimes Y,$$

and we impose the conditions on X and Y for the image of $T^2 - 1$ to be zero; that immediately gives the required relations.)

Let x and y be the classes in A, of X and Y respectively. We will then show that A is an $\mathbb{R}$-vector space of rank 4, and that the set $\{x, y\}$ may be included in a basis; the simplest way for doing so is to introduce the element $s = x + y \in A$, whose powers are $s^2 = x^2 + y^2$, $s^3 = x - y$ and $s^4 = 1$; it is then clear that one gets a morphism

$$\mathbb{R}[S]/(S^4 - 1) \longrightarrow A$$

which is easily checked to be an isomorphism. Despite this isomorphism, the group $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})$ is obviously not isomorphic to $\mu_{4,\mathbb{R}}$. In fact, the group law on $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})$ is associated to the morphism $\Delta : A \to A \otimes_{\mathbb{R}} A$ given by

$$\Delta(x) = x \otimes x - y \otimes y, \quad \Delta(y) = x \otimes y + y \otimes x.$$

The conjugation in $\mathbb{C}$ induces an involution of the functor $\mathsf{R}_{\mathbb{C}/\mathbb{R}}$, and thus an involution u on A, compatible with Δ; it is given by $u(x) = x, u(y) = -y$. By composing with (2-1), we thus get another morphism $\mathbb{C}[T]/(T^2 - 1) \to \mathbb{C} \otimes_{\mathbb{R}} A$; putting both together, we get

$$\mathbb{C}[T_1, T_2]/(T_1^2 - 1, T_2^2 - 1) \longrightarrow \mathbb{C} \otimes_{\mathbb{R}} A, \quad t_1 \mapsto 1 \otimes x + i \otimes y, t_2 \mapsto 1 \otimes x - i \otimes y$$

It is clearly an isomorphism; moreover, the conjugation in $\mathbb{C}$ induces on $\mathbb{C} \otimes_{\mathbb{R}} A$ an automorphism which corresponds, in the left hand algebra, to the transposition of T_1 and T_2: this is the algebraic meaning of the statement that the Weil restriction $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})$ is a twisted form of the Klein group $\mu_2 \times \mu_2$.

We now define a *surjective* morphism from the $\mathbb{R}$-algebra of the Weil restriction, to $\mathbb{C}$

$$\mathbb{R}\langle \mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})\rangle \longrightarrow \mathbb{C}.$$

(This is the simplest example for Theorem 2.3 below.) Actually, since $\{x, y\}$ is part of a basis of A, the map

$$\mathbb{R}\langle \mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})\rangle = A^D = \mathrm{Hom}_{\mathbb{R}}(A, \mathbb{R}) \to \mathbb{C}, \quad \alpha \mapsto \alpha(x) + i\alpha(y),$$

is surjective; it is also a morphism of algebras, as one can check from the definition of Δ given above.

But, if, instead of the nonconstant group $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})$, you prefer to generate $\mathbb{C}$ with a constant one, you can, as everybody does, use the cyclic group of order four $\{\pm 1, \pm i\}$.

Theorem 2.3. *Let $k \to K$ be a finite étale morphism. Let $n : \mathrm{Spec}(K) \to \mathbb{N}$ be an K-integer which is invertible in k. Then the Weil restriction*

$$G = \mathsf{R}_{K/k}(\mu_{n,K}) = \mathrm{Ker}(\mathbf{G}_{m,K/k} \xrightarrow{n} \mathbf{G}_{m,K/k})$$

is a finite étale group scheme over $\mathrm{Spec}(k)$. *According to Proposition 1.3.2, the inclusion $G \subset \mathbf{G}_{m,K/k}$ induces a morphism of k-algebras*

$$k\langle G\rangle \to K. \tag{2-2}$$

This morphism is surjective.

Recall form Section 1.2 that $\mathbf{G}_{m,K/k}$ denotes the group scheme over $\operatorname{Spec}(k)$ given by the multiplicative group of K; since K is commutative one has, here, $\mathbf{G}_{m,K/k} = \mathsf{R}_{K/k}(\mathbf{G}_{m,K})$.

Proof. The hypothesis on n means that we are given a decomposition as a product $K = K_1 \times \cdots \times K_s$, and a family $(n_1, \ldots, n_s)$ of integers, each of which is invertible in k; the K-group $\mu_{n,K}$ is equal, over the open-closed set $\operatorname{Spec}(K_i)$, to μ_{n_i,K_i}.

The properties of the Weil restriction do not allow to reduce to the case where n is constant, but we may suppose $\operatorname{Spec}(k)$ to be connected; then there exists a faithfully flat étale morphism $k \to k'$, with $\operatorname{Spec}(k')$ connected, a finite set I and an isomorphism of k'-algebras

$$k' \otimes_k K \simeq \prod_I k'.$$

The decomposition of K as the product associated to n gives the surjective map

$$\alpha : I \to \{1, 2, \ldots, s\}$$

such that, for $j = 1, \ldots, s$, one has

$$k' \otimes_k K_j = \prod_{\alpha^{-1}(j)} k'.$$

The definition of the direct image now gives

$$G(k') = \mu_n(k' \otimes_k K) = \prod_{i \in I} \mu_{n_{\alpha(i)}}(k').$$

This last group will be noted as $\prod_I \mu_{n\alpha}(k')$. Since n is supposed to be invertible in k, the group schemes μ_{n_j} are étale and finite; this shows that G is finite and étale over k.

Now the surjectivity of the morphism (2-2) can be checked after any faithfully flat base change $k \to k'$; so we may suppose that the ring k', connected as above, is big enough so that it contains, for all $i \in I$, an $n_{\alpha(i)}$-th root of unity ζ_i different from 1; by connectedness, $1 - \zeta_i$ is invertible.[1]

We have to show that every idempotent of $\prod_I k'$ is in the image of the morphism

$$k'\langle \prod_I \mu_{n\alpha}(k') \rangle \to \prod_I k'.$$

[1] A quick proof I learned from Pascal Autissier: Let R be a connected ring containing two roots u an v of a separable polynomial $P(T)$; then either $u - v$ is zero, or it is invertible in R. In fact, letting $P(T) = (T - u)Q(T)$, one has $P' = (T - u)Q' + Q$, so $(T - u)P' = (T - u)^2 Q' + P$, and then $(v - u)P'(v) = (v - u)^2 Q'(v)$; since P is separable, $P'(v)$ is invertible in R, and thus, the ideal $(v - u)R$ is equal to its square; it is therefore generated by an idempotent. But, by assumption, R doesn't contain any nontrivial idempotent.

Fix $i_0 \in I$, and let $e = (e_i) \in \prod_I k' = k' \otimes_k K$, be the idempotent given by $e_{i_0} = 1$, and $e_i = 0$ for $i \neq i_0$. Consider the element $f = (f_i) \in \prod_I \mu_{n\alpha}(k')$, with $f_{i_0} = \zeta_{i_0}$, and for $i \neq i_0$, $f_i = 1$. One has

$$(1 - \zeta_{i_0})e = 1 - f.$$

But $1 - \zeta_{i_0}$ is invertible in the base ring k'. So we are done. □

2.4. ***The case of a Galois field extension.*** By using the Galois descent machinery, we now generalize Section 2.2 to a Galois extension of fields $k \to K$, with Galois group π, and where 2 is invertible in k; we take $n = 2$.

One has the inclusion

$$\mu_2 = \{\pm 1\} \to K^\times \subset K$$

Extend it as

$$\prod_\pi \mu_2 \to \prod_\pi K.$$

The elements of these sets will be seen as maps from π to μ_2, and to K respectively. We define a left action of π on these maps: for $\sigma, \tau \in \pi$,

$$({}^\sigma u)(\tau) = u(\tau\sigma).$$

(Note that, for this action, π acts on the source ($= \pi$), but not the target ($= K$).)

We consider the ring $\prod_\pi K$ as a K-algebra via the morphism $K \to \prod_\pi K$ given by $x \mapsto (\sigma \mapsto \sigma(x))$; this morphism is π-equivariant, and taking the invariants gives back the initial morphism

$$k = K^\pi \to K \simeq \big(\prod_\pi K\big)^\pi.$$

The group scheme G is now defined by the abstract group $G(K) = \prod_\pi \mu_2$, equipped with the given above action of π. We thus have a π-equivariant map

$$G(K) \to \big(\prod_\pi K\big)^\times \subset \prod_\pi K.$$

It induces a morphism of K-algebras

$$K\langle G(K)\rangle \;\to\; \prod_\pi K.$$

To be explicit: for $x \in K$, and $g \in G(K)$, the image of $xg \in K\langle G(K)\rangle$ is the map $\pi \to K$ given by $\sigma \mapsto \sigma(x)g(\sigma)$; this morphism is π-equivariant for π acting on $K\langle G(K)\rangle$ by the rule ${}^\tau(xg) = \tau(x)^\tau g$; it is also surjective since the Kronecker idempotent $\delta_\sigma \in \prod_\pi K$ is the image of $\frac{1}{2}(1 + g)$, where $g(\tau) = -1$ if $\tau \neq \sigma$, and

$g(\sigma)=1$. Taking the invariants, one gets the surjective morphism

$$k\langle G\rangle \overset{1.5.1}{=} \big(K\langle G(K)\rangle\big)^{\pi} \;\to\; K=\big(\prod_{\pi} K\big)^{\pi}.$$

3. Some properties of separable algebras

Let k be a commutative ring. A k-algebra $k\to A$ is said to be *separable* if A is a projective $A\otimes_k A^{\mathrm{opp}}$-module, for the module structure given by

$$A\otimes_k A^{\mathrm{opp}}\times A\to A,\quad (x\otimes y,a)\mapsto xay.$$

This notion was introduced and studied by Auslander and Goldman [Auslander and Goldman 1960] (or see [Knus and Ojanguren 1974]); it generalizes what is called *absolutely semisimplicity* when k is a field. Nowadays, separable algebras are as ubiquitous as their commutative counterparts, the étale algebras.

The definition above is equivalent to the more explicit following one:

Definition 3.1. Let $p: A\otimes_k A\to A$ be the product map, given by $p(a\otimes b)=ab$; this map is $A\otimes_k A^{\mathrm{opp}}$-linear. The separability is equivalent to the existence of an element $e\in A\otimes_k A$ such that $p(e)=1$, and, for all $c\in A$, $c\otimes 1\cdot e=e\cdot 1\otimes c$. To avoid any doubt on which product is used in this equality, we write $e=\sum_i a_i\otimes b_i$; then one must have $\sum a_ib_i=1$, and for any $c\in A$, $\sum ca_i\otimes b_i=\sum a_i\otimes b_ic$.

Such an element e is called a *separability idempotent* for A.

Lemma 3.2. *Let $k\to A$ be a separable algebra, and let M be a left A-module. If M is k-projective, then it is A-projective as well.*

We give the proof from [Orzech and Small 1975, p. 13], because it shows how the product by e acts as taking the mean value, which is usual when dealing with finite groups. So let $u: P\to M$ be a surjective map of left A-modules, and let $v: M\to P$ be a k-linear right inverse ($uv=1$). Look at $\mathrm{Hom}_k(M,P)$ as a left $A\otimes_k A^{\mathrm{opp}}$-module, by letting

$$(x\otimes y\cdot v)(m)=xv(ym).$$

Then it makes sense to consider the map ev; we check that it is an A-linear right inverse of u. It is A-linear since, for $c\in A$, one has

$$c(ev)=(c\otimes 1\cdot e)v=(e\cdot 1\otimes c)v,$$

and then

$$c(ev)(m)=\big(\sum a_iv(b_icm)\big)=(ev)(cm)$$

Moreover, it is easy to check that $u(ev)=1$. Therefore, M is A-projective.

3.3. In the following, we only consider separable algebras which in addition are projective k-modules of finite type; since a projective separable algebra must be a finitely generated k-module (see [Knus and Ojanguren 1974, p. 82] or [Orzech and Small 1975, p. 13]), we call such algebras simply *projective separable*. The main examples of projective separable algebras are

- finite étale (commutative) k-algebras;
- k-algebras $\mathrm{End}_k(P)$ of endomorphisms of a projective k-module of finite type; if P is free, and denoting by (e_{ij}) the usual basis of the ring of matrices, the element $\sum_{i,j} e_{ij} \otimes e_{ji}$ is a separability idempotent;
- the algebra $k\langle\Gamma\rangle$ of a finite group Γ whose order n is invertible in k; for a separability idempotent one may then take $\frac{1}{n}\sum_{\sigma\in\Gamma}\sigma\otimes\sigma^{-1}$.

3.4. Let A be a k-algebra. Then A is projective separable if and only if there exists a faithfully flat morphism $k \to k'$ (even an étale one), a finite family $(n_i)_{i\in I}$ of k'-integers n_i, and an isomorphism of k'-algebras

$$k' \otimes_k A \simeq \prod_{i\in I} \mathrm{M}_{n_i}(k')$$

This characterization, or a direct proof, shows:

Proposition. *Let A be a projective separable k-algebra. Then the center K of A is finite étale over k and A is projective separable over K* [Knus and Ojanguren 1974, III, 5.5].

A K-algebra that is projective separable and *central* is called an Azumaya K-algebra.

In this paper, we shall not consider the Morita equivalence between Azumaya algebra, nor the Brauer group.

3.5. ***Existence of a maximal étale subalgebra.*** A careful reading of the proof given in [Auslander and Goldman 1960, p. 384] or in [Knus and Ojanguren 1974, III,6.4], which both concern a local base ring, leads to the following very slight generalization:

Proposition. *Let k be a semilocal ring and $k \to A$ a projective separable algebra, with center K. Then there exists a maximal commutative subalgebra $L \subset A$, which is finite étale over the center K, and then also finite étale over k. Moreover, if the rank of A as a K-module is constant, equal to n^2, then the rank of L over K is n.*

3.6. Let L be a maximal étale subalgebra of A. From the inclusion $L \subset A$ come two structures of L-module on A: we note respectively by ${}_LA$ and A_L the L-modules given by multiplication of “scalars” in L on the left, and on the right. Since L is étale over K, both these L-modules are projective (Lemma 3.2).

Proposition 3.7 [Knus and Ojanguren 1974, III.6.1]. *The morphism from $A \otimes_K L$ to* $\mathrm{End}_L(A_L)$ *given by* $a \otimes \lambda \mapsto (a' \mapsto aa'\lambda)$, *is an isomorphism.*

4. Construction of the group G

For this section, we fix the following notations:

- $k \to A$ is a projective separable k-algebra;
- K denotes the center of A;
- L denotes a chosen maximal étale subalgebra $L \subset A$;
- ${}_LA$ is the L-module for the law given by the multiplication on the left; it is a locally free L-module.

We thus have the algebra inclusions

$$k \subset K \subset L \subset A.$$

4.1. ***Introducing the "normalizer" of L in A.*** The inclusion of k-algebras $L \subset A$ gives rise to a closed immersion of multiplicative group functors

$$\mathbf{G}_{m,L/k} \subset \mathbf{G}_{m,A/k}.$$

Denote the normalizer of this subgroup by

$$\mathsf{N} = \mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k})$$

Let us be more explicit. For $k' \in k$-Alc, one has

$$\mathsf{N}(k') = \{a \in (k' \otimes_k A)^\times \mid a(k' \otimes_k L)^\times a^{-1} = (k' \otimes_k L)^\times\}.$$

We show, by the standard Lie-type argument, that $\mathsf{N}(k')$ acts, in fact, on the whole algebra $k' \otimes_k L$, and not only on its invertible elements. Let, as usual, $k'[\varepsilon]$ be the ring of dual numbers over k' ($\varepsilon^2 = 0$); one has an exact sequence of groups

$$0 \longrightarrow k' \otimes_k L \xrightarrow{x \mapsto 1+\varepsilon x} \mathbf{G}_{m,L/k}(k'[\epsilon]) \longrightarrow \mathbf{G}_{m,L/k}(k'),$$

where the first term $k' \otimes_k L$ stands for the additive underlying group of that ring. As the group functor $\mathbf{G}_{m,L/k}$ is acted upon by N, one sees that N also acts on the above kernel, that is on the functor in additive groups $k' \mapsto k' \otimes_k L$; to be precise, a section $a \in \mathsf{N}(k')$ induces the inner automorphism $x \mapsto axa^{-1}$ of the group $(k' \otimes_k L)^\times$, and thus it defines an automorphism w of the k'-algebra $k' \otimes_k L$, characterized by

$$ax = w(x)a \quad \text{for all } x \in k' \otimes_k L. \tag{4-1}$$

By its very definition, this automorphism w is the identity on the subalgebra $k' \otimes_k K$.

Therefore we get a morphism of group functors

$$\mathsf{N} = \mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k}) \to \mathsf{Aut}(L/K),$$

where $\mathsf{Aut}(L/K)$ is the functor on the category of commutative k-algebras given by

$$\mathsf{Aut}(L/K)(k') \;=\; \mathrm{Aut}_{(k'\otimes_k K)\text{-}\mathsf{Alc}}(k'\otimes_k L)$$

(Technically, the base ring k should appear in the symbol $\mathsf{Aut}(L/K)$, but it is clear from the context that this functor, like most of the others under consideration, is defined on the category of commutative k-algebras.)

Let us introduce the local rank of A as a K-module; since A is locally a matrix algebra, this rank is a square; so, let $n : \mathrm{Spec}(K) \to \mathbb{N}$ be the map defined by

$$\mathrm{rank}_{K_\mathfrak{q}}(A_\mathfrak{q}) = n(\mathfrak{q})^2.$$

Since L is étale over K the L-module ${}_LA$ is locally free by Lemma 3.2. As the K-rank of L is n, the L-rank of ${}_LA$ is also n — with a slight abuse of notation, this last n being the composite map

$$\mathrm{Spec}(L) \to \mathrm{Spec}(K) \xrightarrow{n} \mathbb{N}.$$

Denote by $\mathscr{L}$ the determinant of the L-module ${}_LA$, that is the invertible L-module defined by

$$\mathscr{L} = \det_L({}_LA) = \bigwedge\nolimits^n {}_LA$$

Fix $k' \in k\text{-}\mathsf{Alc}$, and consider a section $a \in \mathsf{N}(k')$; as above, we write ϖ for the inner automorphism of $k'\otimes_k L$ defined by a — see (4-1). The product by a on the left in $k'\otimes_k A$ is thus a ϖ-semilinear map, that we may write as a $k'\otimes_k L$-linear map

$$k'\otimes_k A \to \varpi_\star(k'\otimes_k A), \quad a' \mapsto aa'$$

The n-th exterior power of this map gives a $k'\otimes_k L$-linear map

$$\det(a) : k'\otimes_k \mathscr{L} \to \varpi_\star(k'\otimes_k \mathscr{L})$$

(The notation $\det(a)$, usually reserved for endomorphisms, is a bit improper here; but it cannot cause any confusion.)

4.2. ***Constructing the group functor* G.** Because k is supposed to be semilocal, the ring L is also semilocal since it is finite over k; hence, the invertible L-module $\mathscr{L}$ is isomorphic to L; we *choose* a basis $e \in \mathscr{L}$, i.e., an isomorphism

$$L \xrightarrow{\sim} \mathscr{L}, \qquad x \mapsto xe.$$

We now define the group functor G as the stabilizer of the basis e of $\mathscr{L}$, for its action through det; more precisely,

$$\mathsf{G}(k') = \left\{a \in \mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k})(k') \mid \det(a)(1\otimes e) = 1\otimes e\right\}.$$

(Although the map det is not a morphism, G is indeed a group.)

Proposition 4.3. *We maintain the assumptions and notation at the beginning of Section 4, and we suppose in addition that the ring k is semilocal and that the K-integer n is invertible in k. Then the group functor* G, *defined above, fits into the following commutative diagram, whose rows are exact sequences of sheaves on* $\mathrm{Spec}(k)$ *for the étale topology*:

$$\begin{tikzcd}
1 \arrow[r] & \mathsf{R}_{L/k}(\mu_{n,L}) \arrow[r] \arrow[d] & \mathsf{G} \arrow[r] \arrow[d] & \mathsf{Aut}(L/K) \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \mathbf{G}_{m,L/k} \arrow[r] \arrow[d, "n"] & \mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k}) \arrow[r] & \mathsf{Aut}(L/K) \arrow[r] & 1 \\
 & \mathbf{G}_{m,L/k} & & &
\end{tikzcd}$$

In particular, G *is finite étale over k.*

The proof occupies Sections 4.4–4.5.

4.4. ***The sequence*** $\mathbf{1} \to \mathbf{G}_{m,L/k} \to \mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L}) \to \mathsf{Aut}(L/K) \to \mathbf{1}$ ***is exact.***

(a) *Exactness at* $\mathsf{N} = \mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k})$. The property of L being a "maximal commutative" subalgebra may be interpreted as the exactness of the following sequence of K-modules

$$0 \to L \to A \to \mathrm{Hom}_K(L, A),$$

where the map on the right associates to $a \in A$ the K-linear map $x \mapsto ax - xa$. Such exactness is preserved by any flat base change.

Now, consider a section $a \in \mathsf{N}(k')$, where k' is flat over k; suppose that the conjugation by a gives the identity in $\mathsf{Aut}(L/K)(k')$; this means that $axa^{-1} = x$ for all $x \in k' \otimes_k L$; thus a commutes with all the elements of the *maximal commutative* subalgebra $k' \otimes_k L$; therefore, one has $a \in \mathbf{G}_{m,L/k}(k')$.

(b) The proof of the (local) *surjectivity of* $\mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k}) \to \mathsf{Aut}(L/K)$ needs several steps.

4.4.1. We begin with the "split" case where $A = \mathrm{End}_K(L)$, the inclusion $L \subset A$ being isomorphic to the map $m : L \to \mathrm{End}_K(L)$ given by the multiplication. Then each automorphism of K-algebras $w : L \to L$ is the restriction to L of the conjugation by w in $\mathrm{End}_K(L)$, as the formula $wm(x)w^{-1} = m(w(x))$ shows. That implies the surjectivity in this case.

We will now show that the general case is "locally" isomorphic to this split one.

4.4.2. There is an isomorphism of algebras $\omega\colon A\otimes_K L \xrightarrow{\sim} \mathrm{End}_K(L)\otimes_K L$ making the following diagram commutative (it is an isomorphism of L-algebras for the product *on the right* by elements of L).

$$\begin{tikzcd}
L \otimes_K L \arrow[r, "\imath\otimes 1"] \arrow[d, equal] & A \otimes_K L \arrow[d, "\omega"] \\
L \otimes_K L \arrow[r, "m\otimes 1"'] & \mathrm{End}_K(L) \otimes_K L
\end{tikzcd}$$

Proof. Look at A as an $L \otimes_K L$-module via the law $(x \otimes y, a) \mapsto xay$; since $L \otimes_K L$ is étale over K, and since A is locally free over K, A is locally free as a $L \otimes_K L$-module (Lemma 3.2); as both A and $L \otimes_K L$ have the same rank n^2 over K, the module A is of rank 1 over $L \otimes_K L$. But the ring $L \otimes_K L$ is finite over the semilocal ring k; therefore it is also semilocal, and then any rank one projective module over $L \otimes_K L$ is isomorphic to $L \otimes_K L$. Thus we can find $\varepsilon \in A$ such that the map

$$L \otimes_K L \to A, \quad x \otimes y \mapsto x\varepsilon y,$$

is an isomorphism. On considering both $L \otimes_K L$ and A as L-modules for the product on the right, we get an isomorphism of L-algebras

$$\mathrm{End}_L(A_L) \xrightarrow{\sim} \mathrm{End}_L(L \otimes_K L).$$

We obtain the isomorphism ω by composing the above one with the isomorphism indicated in Proposition 3.7:

$$A \otimes_K L \xrightarrow{3.7} \mathrm{End}_L(A_L) \xrightarrow{\sim} \mathrm{End}_L(L \otimes_K L) \xrightarrow{\sim} \mathrm{End}_K(L) \otimes_K L.$$

The required commutativity of the square is easy to check. □

4.4.3. There exist a finite injective étale morphism $k \to k'$ and an isomorphism of k'-algebras

$$\omega' : A \otimes_k k' \xrightarrow{\sim} \mathrm{End}_K(L) \otimes_k k'$$

making commutative the diagram

$$\begin{tikzcd}
L \otimes_k k' \arrow[r, "\imath\otimes 1"] \arrow[d, equal] & A \otimes_k k' \arrow[d, "\omega'"] \\
L \otimes_k k' \arrow[r, "m\otimes 1"'] & \mathrm{End}_K(L) \otimes_k k'
\end{tikzcd}$$

(The difference with the previous diagram is that the tensor products are now taken over k.)

Proof. Let $k' = \mathsf{R}_{K/k}(L)$ be the Weil restriction of L from Section 2.1; it is a finite étale k-algebra, and by its very definition, it is equipped with a morphism of K-algebras

$$L \;\to\; K \otimes_k k'.$$

Now, for any K-module V, we have the isomorphisms

$$(V \otimes_K L) \otimes_L (K \otimes_k k') \simeq V \otimes_K (K \otimes_k k') \simeq V \otimes_k k'.$$

It is now clear that the required square is obtained from the square of the step 4.4.2 by the base change $L \to K \otimes_k k'$.

One can interpret this step by saying that the inclusion $\iota : L \to A$ is a twisted form, for the finite étale topology on k, of the map $m : L \to \mathrm{End}_K(L)$, given by the product in L.

That ends the proof that the map $\mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k}) \to \mathsf{Aut}(L/K)$ is locally surjective. □

4.5. *The sequence* $1 \to \mathsf{R}_{L/k}(\mu_{n,L}) \to \mathsf{G} \to \mathsf{Aut}(L/K) \to 1$ *is exact.*

(a) *Exactness at* G. Due to the exactness of the bottom row of the diagram of Proposition 4.3, we have to check the equality

$$\mathsf{G} \cap \mathbf{G}_{m,L/k} \;=\; \mathsf{R}_{L/k}(\mu_{n,L}).$$

But, for k' over k, a section $a \in \mathbf{G}_{m,L/k}(k') = (k' \otimes_k L)^\times$ has to be seen as a scalar for the $k' \otimes_k L$-module $k' \otimes_k A$, which is of rank n; therefore, one has $\det(a) = a^n$; since $e \in \mathscr{L}$ is a basis over L, the equality $\det(a)(1 \otimes e) = 1 \otimes e$ is equivalent to $a^n = 1$.

(b) We now check that the morphism $\mathsf{G} \longrightarrow \mathsf{Aut}(L/K)$ is "locally" surjective: given k' finite étale over k, and given an automorphism $w \in \mathsf{Aut}(L/K)(k')$, we have to find a finite étale morphism $k' \to k''$, and a section $a \in \mathsf{G}(k'')$ such that w induces on $k'' \otimes_k L$ the conjugation by a. We already know this to be true for the bottom morphism $\mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k}) \to \mathsf{Aut}(L/K)$; we have thus to show the following: given k' finite étale over k and $a \in \mathsf{N}(k')$, there exists a finite étale morphism $k' \to k''$, and a section $y \in \mathbf{G}_{m,L/k}(k'')$ such that $y^{-1}a \in \mathsf{G}(k'')$. But, in any case, since $e \in \mathscr{L}$ is a basis over L, there exists $x \in (k' \otimes_k L)^\times$ such that

$$\det(a)(1 \otimes e) \;= x \cdot 1 \otimes e.$$

Let $k' \to k'_1$ be finite étale morphism which "splits" $k' \otimes_k L$. Thus, there exists a finite set I and an isomorphism

$$k'_1 \otimes_k L \;\xrightarrow{\sim}\; \prod_I k'_1.$$

To the element $x \in (k' \otimes_k L)^\times$ there corresponds a family $(x_i)_{i\in I}$ of invertible elements of k'_1; since the integer n is supposed invertible in k, each of the polynomials $Y^n - x_i \in k'_1[Y]$ is separable; therefore, there exists a finite étale morphism $k'_1 \to k''$, and a family $(y_i) \in \prod_I k''$ such that $y_i^n = x_i$. Going back to $k'' \otimes_k L$ via its isomorphism with $\prod_I k''$, we get an element $y \in k'' \otimes_k L$ such that $y^n = x$; therefore $y^{-1}a \in \mathsf{G}(k'')$.

5. Group generation of separable algebras

Recall the result we want to prove.

Theorem 5.0. *Let k be a semilocal ring containing the field $\mathbb{Q}$. Let $k \to A$ be a projective separable algebra. Then, there exists a finite étale k-group G and a surjective morphism of k-algebras*

$$k\langle \mathsf{G}\rangle \to A.$$

5.1. ***Fixed points.*** We begin by recalling the few facts we need about the fixed points under the action of a group functor.

Let $k \subset K \subset L$ be two finite injective étale morphisms of rings. Let $W \subset \mathsf{Aut}(L/K)$ be a subgroup functor (it is a functor on k-Alc). We will denote by $L^W \subset L$ the subring of the elements which are *absolutely* invariant under W, that is the set of those $x \in L$ such that for all k-algebra k', the image of x in $k' \otimes_k L$ is invariant under the group $W(k')$. Suppose that W is affine and flat over k; let $u : k \to R$ be its (commutative) algebra of functions, so that $W = \mathrm{Spec}(R)$; then the action of W on L is given by a morphism of k-algebras

$$\delta : L \longrightarrow L \otimes_k R$$

The ring of invariants L^W is then characterized by the exactness of the sequence

$$\begin{tikzcd} L^W \arrow[r] & L \arrow[r, shift left, "1\otimes u"] \arrow[r, shift right, "\delta"'] & L \otimes_k R \end{tikzcd} .$$

In fact, fix $k' \in k$-Alc; an automorphism $w \in W(k')$ may be seen as a morphism of k-algebras $w : R \to k'$; it leads to the commutative diagram

$$\begin{tikzcd} L \arrow[r, shift left, "1\otimes u"] \arrow[r, shift right, "\delta"'] \arrow[d] & L \otimes_k R \arrow[d, "1\otimes w"] \\ L \otimes_k k' \arrow[r, shift left, "\mathrm{Id}"] \arrow[r, shift right, "w'"'] & L \otimes_k k' \end{tikzcd}$$

where w' is induced from $(1 \otimes w) \circ \delta$; this is nothing but the automorphism given by w, acting on $L \otimes_k k'$. That shows the claim.

The relevance of using group functors (instead of constant groups) appears again in the following result: in a weak sense, any finite étale morphism is "galoisian".

Lemma 5.1.1. *Let $k \subset K \subset L$ be two finite injective étale morphisms of rings. Then*

$$L^{\mathsf{Aut}(L/K)} = K.$$

To make notations lighter, let $W = \mathsf{Aut}(L/K)$. The inclusion $K \subset L^W$ comes from the definition.

For the converse, it is enough to show the inclusion $k' \otimes_k L^W \subset k' \otimes_k K$ for a faithfully flat morphism $k \to k'$. Remark first that for any such morphism, the canonical morphism

$$k' \otimes_k (L^W) \longrightarrow (k' \otimes_k L)^{W(k')}$$

is clearly injective. Let us now take for $k \to k'$ a finite étale morphism which splits the finite étale algebras K and L; the inclusion $k' \otimes_k K \subset k' \otimes_k L$ is then isomorphic to the inclusion $\prod_I k' \subset \prod_J k'$ associated to some surjective map $\alpha : J \to I$ of finite sets; in this situation, the group $W(k')$ is isomorphic to the subgroup $\Gamma \subset \mathfrak{S}_J$ of all the bijections σ of J such that $\alpha \circ \sigma = \alpha$; precisely, one has $\Gamma = \prod_{i \in I} \mathfrak{S}_{\alpha^{-1}(i)}$. As the map α clearly induces a bijection $J/\Gamma \simeq I$, the elements of $k' \otimes_k L = \prod_J k'$ which are invariants under the automorphisms in Γ are those of $\prod_I k' = k' \otimes_k K$.

5.2. ***Proof of the theorem.*** As in Section 4, we denote by K the center of A, and by n^2 the K-rank of A as a locally free K-module. We again choose an étale maximal subalgebra $L \subset A$, and a generator of the invertible L-module $\mathscr{L} = \det_L({}_L A) = \bigwedge^n{}_L A$.

According to Proposition 4.3 we can define a sequence of morphisms between finite étale groups

$$\begin{tikzcd} 1 \arrow[r] & \mathsf{R}_{L/k}(\mu_{n,L}) \arrow[r] & \mathsf{G}_0 \arrow[r] & \mathsf{Aut}(L/K) \arrow[r] & 1 \end{tikzcd}$$

which is exact as a sequence of sheaves for the étale topology.

5.2.1. Now suppose given a k-subgroup $W \subset \mathsf{Aut}(L/K)$, which is finite étale over k, and such that $L^W = K$ (according to Lemma 5.1.1, W may be the whole $\mathsf{Aut}(L/K)$, but it may also be the (constant) Galois group of L/K in case this morphism is galoisian).

We then define the group G for the theorem as the pull-back of G_0, as shown in the diagram

$$\begin{tikzcd} 1 \arrow[r] & \mathsf{R}_{L/k}(\mu_{n,L}) \arrow[r] \arrow[d, equal] & \mathsf{G} \arrow[r] \arrow[d] & W \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & \mathsf{R}_{L/k}(\mu_{n,L}) \arrow[r] & \mathsf{G}_0 \arrow[r] & \mathsf{Aut}(L/K) \arrow[r] & 1 \end{tikzcd}$$

Consider the canonical morphism

$$f : k\langle \mathsf{G}\rangle \to A$$

associated, via Proposition 1.3.2, to the inclusion $\mathsf{G} \subset \mathsf{G}_0 \subset \mathsf{N} \subset \mathbf{G}_{m,A/k}$. We will prove it to be surjective.

5.2.2. The first step is to prove that an element $a \in A$ which commutes with any "local" section of G is in fact in the center K of A.

Let a be such an element; the hypothesis means that for each commutative algebra $k \to k'$, the image of a in $k' \otimes_k A$ commutes with the elements of $\mathsf{G}(k') \subset k' \otimes_k A$.

First, we show that $a \in L$. By assumption, $af(b) = f(b)a$ for all $b \in k\langle \mathsf{G}\rangle$. By Theorem 2.3, the k-algebra L is generated by the subgroup $\mathsf{R}_{L/k}(\mu_{n,L}) \subset \mathsf{G}$; thus, the element a must commute with all the elements of L; but L is a *maximal* commutative subalgebra; therefore, $a \in L$.

Next we show that $a \in K = L^W$. Let $w \in W(k')$; since the morphism of sheaves $\mathsf{G} \to W$ is surjective, we may find a faithfully flat extension k'' of k' and a section $g \in \mathsf{G}(k'')$, such that

$$w(1 \otimes a) = g(1 \otimes a)g^{-1}$$

The hypothesis on a then implies that $w(1 \otimes a) = 1 \otimes a$.

5.2.3. Let C be the center of the group algebra $k\langle \mathsf{G}\rangle$. We prove that

$$f(C) = K.$$

Take $c \in C$; since the image $f(c)$ commutes with the local sections of G, the previous step shows that $f(c) \in K$. Conversely, let us check the inclusion $K \subset f(C)$. The group $\mathsf{R}_{K/k}(\mu_{n,K})$ is clearly a subfunctor of G, and we have, by Theorem 2.3,

$$f(k\langle \mathsf{R}_{K/k}(\mu_{n,K})\rangle) = K.$$

Moreover, since $\mathsf{R}_{K/k}(\mu_{n,K})$ is a subgroup of $\mathbf{G}_{m,K/k}$, it is included in the center of $\mathsf{G} \subset \mathbf{G}_{m,A/k}$; therefore $k\langle \mathsf{R}_{K/k}(\mu_{n,K})\rangle \subset C$, and we are done.

5.2.4. We now conclude the proof of the surjectivity of f. The k-algebra $B = k\langle \mathsf{G}\rangle$ is separable since the order of the étale group G is invertible in k (recall that $\mathbb{Q} \subset k$); it is thus an Azumaya C-algebra. Since $f(C)$ is contained in the center K of A, the K-algebra A can be seen as a C-algebra, and f as a morphism of C-algebras from the Azumaya C-algebra B to A. According to [Knus and Ojanguren 1974, III.5.3, p. 95], f induces an isomorphism

$$B \otimes_C A^B \quad \xrightarrow{\sim} \quad A,$$

where $A^B = \{a \in A \mid af(b) = f(b)a \text{ for all } b \in B\}$; but this ring is equal to K, as seen in 5.2.2, and the map $C \to K$ is surjective, by 5.2.3. Therefore the morphism $f : B \to A$ is surjective.

6. Examples

Let K be a field of characteristic zero.

6.1. ***Some finite groups generating a matrix algebra.*** We begin with the "standard" representation of the symmetric group

$$K\langle\mathfrak{S}_{n+1}\rangle \longrightarrow \mathbf{M}_n(K) \tag{6-1}$$

More generally, let Γ be a group acting transitively on the set $I = \{0, 1, \dots, n\}$; consider the $K\langle\Gamma\rangle$-module $U = \mathsf{M}(I, K) \simeq K^{n+1}$ whose elements are the maps $u : I \to K$; it is the direct sum $U = U_0 \oplus U_1$, of the submodules $U_0 = \{u \mid \sum_i u(i) = 0\}$, and $U_1 = U^\Gamma$; this last module is a K-vector space of rank one, generated by the constant map with value 1. The algebra $\mathrm{End}_{K\langle\Gamma\rangle}(U)$ decomposes as the product $\mathrm{End}_{K\langle\Gamma\rangle}(U_0) \times \mathrm{End}_{K\langle\Gamma\rangle}(U_1)$, and the second factor is isomorphic to K. On the other hand, by expressing the elements of $\mathrm{End}_K(U)$ as matrices indexed by $I \times I$, one can check that the K-vector space $\mathrm{End}_{K\langle\Gamma\rangle}(U) \subset \mathrm{End}_K(U)$ has a basis indexed by the quotient set $(I \times I)/\Gamma$; the factor $\mathrm{End}_{K\langle\Gamma\rangle}(U_1)$ is generated by the class of the diagonal which is one orbit in $I \times I$; therefore, the morphism $K \to \mathrm{End}_{K\langle\Gamma\rangle}(U_0)$ is an isomorphism if and only if Γ has just one more orbit on the product, that is if Γ is 2-transitive on I; by the Wedderburn double centralizer theorem we finally get the following well-known characterization (for a proof using character theory, see [Serre 1977, §2.3, exercise 2]):

Proposition 6.1.1. *The morphism $K\langle\Gamma\rangle \to \mathrm{End}_K(U_0)$ is surjective if and only if the action of Γ is 2-transitive on I.*

We return to (6-1). The matrix algebra $\mathbf{M}_n(K) \simeq \mathrm{End}_K(U_0)$ is thus shown to be generated by the symmetric group $\mathfrak{S}_{n+1}$, but this group is far from being of the type we introduced in Section 4. Let us try to get close to these constructions.

We define a commutative étale maximal subalgebra of $\mathrm{End}_K(U_0)$ coming from a commutative subgroup of $\mathfrak{S}_{n+1}$: namely, let $H \subset \mathfrak{S}_{n+1}$ be the subgroup generated by the cyclic permutation $\rho = (0, 1, 2, \dots, n)$, and let $L \subset \mathrm{End}_K(U_0)$ be the subalgebra it generates; since the composite map

$$K\langle H\rangle \to \mathrm{End}_K(U_0) \times \mathrm{End}_K(U_1) \to \mathrm{End}_K(U)$$

is injective, we readily get an isomorphism

$$K[X]/(X^n + X^{n-1} + \dots + 1) \xrightarrow{\sim} L$$

showing that L is étale of rank n (recall that $\mathbb{Q} \subset K$). Let $N \subset \mathfrak{S}_{n+1}$ be the normalizer of ρ; this group is isomorphic to the semidirect product

$$\Gamma = \mathbb{Z}/(n+1)\mathbb{Z} \rtimes (\mathbb{Z}/(n+1)\mathbb{Z})^\times;$$

consider the morphism

$$K\langle\Gamma\rangle \to \mathrm{End}_K(U_0);$$

according to Proposition 6.1.1, this morphism is surjective if and only if the integer $n+1$ is prime. If it is not, we may follow the method of Section 4; it leads to a nonconstant group scheme (see also Section 6.3).

In any case, it is easy — and this is certainly well known — to get smaller finite (constant) subgroups of $\mathrm{GL}_n(K)$ which generate $\mathbf{M}_n(K)$; for example, choose a transitive group W of permutations of the canonical basis of K^n, say the group generated by a cycle of length n, and let $D \subset \mathrm{GL}_n(K)$ be the group of diagonal matrices with coefficients ± 1; then the morphism

$$K\langle D \rtimes W\rangle \to \mathbf{M}_n(K)$$

is easily seen to be surjective.

6.2. ***Back to quaternions.*** For the following remarks, it is useful to define the $\mathbb{R}$-algebra of quaternions as a subring of the ring of complex 2×2 matrices

$$\mathbb{H} = \left\{ \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} \,\middle|\, a, b \in \mathbb{C} \right\}.$$

We choose the maximal étale subalgebra $L \subset \mathbb{H}$ consisting of the matrices of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & \bar{a} \end{smallmatrix}\right)$; we denote by $\delta : \mathbb{C} \to L$ the isomorphism given by $\delta(a) = \left(\begin{smallmatrix} a & 0 \\ 0 & \bar{a} \end{smallmatrix}\right)$.

Recall that the choice of a generator $i \in \mathbb{C}$ leads to an isomorphism of $\mathbb{R}$-group functors

$$\mu_{2,\mathbb{R}} \xrightarrow{\sim} \mathsf{Aut}(\mathbb{C}/\mathbb{R}).$$

Namely, to an $\mathbb{R}$-algebra K and an element $u \in K$ such that $u^2 = 1$, one associates the K-automorphism of $K \otimes_{\mathbb{R}} \mathbb{C}$, given by $1 \otimes i \mapsto u \otimes i$. For the sequel, it is better to describe $\mathsf{Aut}(\mathbb{C}/\mathbb{R})$ without any choice, as follows: let $\epsilon = \frac{1}{2}(1+u)$; this is an idempotent of K, and the automorphism associated to u may be rewritten as $z \mapsto \epsilon z + (1-\epsilon)\bar{z}$; that only involves the automorphism $z \mapsto \bar{z}$ induced by the conjugation on the factor $\mathbb{C}$. Similarly, we denote by $W = \mathsf{Aut}(L/\mathbb{R})$ the constant Galois group functor of $L/\mathbb{R}$; the group $W(K)$ contains the involution $c : K \otimes_{\mathbb{R}} L \to K \otimes_{\mathbb{R}} L$ given by $\left(\begin{smallmatrix} a & 0 \\ 0 & \bar{a} \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} \bar{a} & 0 \\ 0 & a \end{smallmatrix}\right)$, and one has

$$W(K) = \mathrm{Gal}(K \otimes_{\mathbb{R}} L/K) = \{\epsilon \mathrm{Id} + (1-\epsilon)c \mid \epsilon^2 = \epsilon \in K\}.$$

Set $j = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$; then, $\{1, j\}$ is a basis of the L-module ${}_L\mathbb{H}$ associated to the multiplication on the left. Let K be a commutative $\mathbb{R}$-algebra. For $x \in K \otimes_{\mathbb{R}} L$, we have $jxj^{-1} = c(x)$. Any element of $K \otimes_{\mathbb{R}} \mathbb{H}$ may be written as

$$\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & \bar{a} \end{pmatrix} + \begin{pmatrix} \bar{b} & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \delta(a) + \delta(\bar{b}) \cdot j,$$

with $a, b \in K \otimes_{\mathbb{R}} \mathbb{C}$; an expression which we simplify in $x + yj$, with $x, y \in K \otimes_{\mathbb{R}} L$.

Note that $\det x = a\bar{a} \in K$ for $x = \delta(a)$. One checks that $\det(x + yj) = \det x + \det y$. For $x, y \in K \otimes_{\mathbb{R}} L$, the next formula gives the condition of invertibility, and the inverse.

$$(x + yj)(c(x) - yj) = (\det x + \det y)\, 1.$$

Let $\mathsf{N} = \mathrm{Norm}_{\mathbf{G}_{m,\mathbb{H}/\mathbb{R}}}(\mathbf{G}_{m,L/\mathbb{R}})$ be the normalizer. An invertible element $x + yj$ is in $\mathsf{N}(K)$ if and only if, for any $z \in (K \otimes_{\mathbb{R}} L)^{\times}$, one has

$$(x + yj)z(c(x) - yj) \in K \otimes_{\mathbb{R}} L.$$

By looking at the coefficient of j, we see that this condition means that, for any $z \in (K \otimes_{\mathbb{R}} L)^{\times}$, one has

$$xy(z - c(z)) = 0.$$

But, if $z = \left(\begin{smallmatrix} 1\otimes i & 0 \\ 0 & -1\otimes i \end{smallmatrix}\right)$, the element $z - c(z)$ is invertible; therefore the conditions on $x + yj$ for being in $\mathsf{N}(K)$ are $\det x + \det y \in K^{\times}$ and $xy = 0$.

We now follow Section 4.2 for constructing a group G which will generate $\mathbb{H}$: we take $e = 1 \wedge j$ as a basis of $\mathscr{L} = \bigwedge^2{}_L\mathbb{H}$. Let us compute the "wedge two" of the left product by $x + yj$ (written as $x \cdot 1 + y \cdot j$ for clarity): one finds, since $j^2 = -1$,

$$(x \cdot 1 + y \cdot j) \wedge (x \cdot j - y \cdot 1) = x^2 \cdot 1 \wedge j - (y \cdot j) \wedge (y \cdot 1) = (x^2 + y^2) \cdot 1 \wedge j.$$

Thus, using the isomorphism $\delta : \mathbb{C} \to L$, one has

$$\mathsf{G}(K) \simeq \{(a, b) \in (K \otimes_{\mathbb{R}} \mathbb{C})^2 \mid ab = 0, a^2 + b^2 = 1, a\bar{a} + b\bar{b} \in K^{\times}\}. \tag{6-2}$$

The group law takes j into account:

$$(a, b).(a', b') = (aa' - b\bar{b}', ab' + b\bar{a}'). \tag{6-3}$$

Now consider the map $\mathsf{G} \to W$ that sends $x + yj$ to the automorphism

$$z \mapsto (x + yj)\, z\, (x + yj)^{-1}.$$

We check that, with the notation of (6-2), the map $\mathsf{G}(K) \to W(K)$ can be written as

$$(a, b) \;\mapsto\; \Big(\frac{a\bar{a}}{a\bar{a} + b\bar{b}}\Big)\mathrm{Id} + \Big(\frac{b\bar{b}}{a\bar{a} + b\bar{b}}\Big)c.$$

The conditions given in (6-2) imply that the coefficient $\dfrac{a\bar{a}}{a\bar{a} + b\bar{b}}$ is indeed an idempotent of K.

Finally, the group functor G comes within an exact sequence

$$1 \longrightarrow \mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}}) \longrightarrow \mathsf{G} \longrightarrow W \longrightarrow 1,$$

where $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})$ denotes the Weil restriction already considered in Section 2.2, and where the left hand map is defined as follows: an element in $a \in \mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})(K)$ is an element in $K \otimes_{\mathbb{R}} \mathbb{C}$ such that $a^2 = 1$; it is mapped to $(a, 0) \in \mathsf{G}(K)$.

This sequence splits locally but not globally. In fact, a splitting of $\mathsf{G}(K) \to W(K)$ must map $c \in W(K)$ to an involution $(a, b) \in \mathsf{G}(K)$, whose image back to $W(K)$ must be c; the last condition implies $a = 0$ and then $b^2 = 1$, and, according to (6-3), the first condition implies $b\bar{b} = -1$. In $\mathbb{R} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}$, such an element b cannot exist; but in $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ you can take $b = i \otimes i$. Thus the sequence is split over $\mathbb{C}$, and it is not split over $\mathbb{R}$.

As seen in the Section 2.2, the group scheme $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})$ is a twisted form of the Klein four group; therefore, the group G constructed above is a twisted form of the dihedral group D_4; it has nothing to do with the (constant) quaternion group Q_8 which, of course, also generates $\mathbb{H}$.

6.3. ***A split case.*** Let $K \to L$ be a finite Galois extension of fields, of degree n, with galois group $W = \mathrm{Gal}(L/K)$. We consider the (Azumaya) algebra $A = \mathrm{End}_K(L)$ equipped with its maximal étale subalgebra L.

In this situation, we will see that different choices for a basis of the invertible sheave $\mathscr{L}$ may lead, following Section 4.2, to nonisomorphic groups G.

6.3.1. The normalizer of $L^\times$ is known to be isomorphic to a semidirect product:

$$\mathrm{Norm}_{A^\times}(L^\times) \xrightarrow{\sim} L^\times \rtimes W, \quad a \mapsto (a(1), a(1)^{-1}a). \tag{6-4}$$

In fact, if an element $a \in A^\times$, seen as a K-*linear* automorphism of L, is assumed to normalize $L^\times$, then for any $x \in L^\times$ there exists $x' \in L^\times$ such that for all $y \in L^\times$,

$$a(xa^{-1}(y)) = x'y;$$

Letting $y = a(1)$, we see that $x' = a(1)^{-1}a(x)$; the above equality then gives

$$a(1)^{-1}a(xy) = a(1)^{-1}a(x)a(1)^{-1}a(y).$$

Therefore,the map $z \mapsto a(1)^{-1}a(z)$ is a K-*algebra* automorphism of L; the map (6-4) is thus well defined. Consider now an element $(x, w) \in L^\times \rtimes W$; the map a defined by $a(y) = xw(y)$ normalizes the (left product by an) element $z \in L^\times$, since $a(za^{-1}(y)) = xw(za^{-1}(y)) = w(z)y$; therefore, (6-4) is an isomorphism.

6.3.2. We now choose a first basis of $\mathscr{L}$, by using the isomorphism

$$L \otimes_K L^D \xrightarrow{\sim} \mathrm{End}_K(L) = A, \qquad x \otimes y^* \mapsto (z \mapsto y^*(z)x)$$

(As before, L^D stands for the K-linear dual $\mathrm{Hom}_K(L, K)$). The structure of L-module on ${}_LA$ corresponds to the structure of L-module on $L \otimes_K L^D$ coming from the first factor. For the sheaf $\mathcal{L} = \bigwedge_L^n A$ introduced in Section 4.1, we thus have the isomorphism

$$\mathcal{L} = \bigwedge\nolimits_L^n (L \otimes_K L^D) = L \otimes_K \bigwedge\nolimits_K^n (L^D).$$

Let $e' \in \bigwedge_K^n (L^D)$ be any basis of this K-vector space of rank one; take $e = 1 \otimes e' \in L \otimes_K \bigwedge_K^n (L^D)$ as an L-basis of $\mathcal{L}$.

The isomorphism of $L \otimes_K L^D$ corresponding to the left product by $a = xw \in \mathrm{Norm}_{A^\times}(L^\times)$, is given by $y \otimes z^* \mapsto xw(y) \otimes z^*$. Therefore, the "wedge" of this map is

$$\det{}_L(a) : \mathcal{L} \longrightarrow w_\star(\mathcal{L}), \quad y \otimes e' \mapsto x^n w(y) \otimes e'$$

The group scheme G_1 we are looking for, along the lines of Section 4.2, is "locally" given by the set of sections a of N such that $\det_L(a)(e) = e$; thus, for a connected (commutative) K-algebra K', one has

$$\mathsf{G}_1(K') = \{(x, w) \in (K' \otimes_K L)^\times \rtimes W \mid x^n = 1\}$$

That is,

$$\mathsf{G}_1 = \mathsf{R}_{L/K}(\mu_{n,L}) \rtimes W_K,$$

where W_K denotes the constant group scheme on $\mathrm{Spec}(K)$ defined by W.

6.3.3. We choose another basis for $\mathcal{L}$ by using the following consequence from Galois theory: every endomorphism $a \in \mathrm{End}_K(L)$ is writable in a unique way as

$$a = \sum_{w \in W} x_w w,$$

with the x_w in L.

Choose a total ordering $\{w_1, \ldots, w_n\}$ on the set W, and let $e = w_1 \wedge \cdots \wedge w_n$; it is an L-basis of $\mathcal{L}$.

Consider, as above, the product in A by the element $a = xw \in \mathrm{Norm}_{A^\times}(L^\times)$; the determinant of the matrix, relative to the basis W, of the multiplication on the left by w is nothing but the *sign*, noted $\mathrm{sgn}_W(w)$, of the permutation of the finite set W, given by $w' \mapsto ww'$. We thus have, for $ye \in \mathcal{L}$,

$$\det{}_L(a)(ye) = x^n w(y) \mathrm{sgn}_W(w) e.$$

The group G_2 associated to this new basis is thus given (for K' connected) by

$$\mathsf{G}_2(K') = \{(x, w), x \in (K' \otimes_K L)^\times \mid w \in W, x^n \mathrm{sgn}_W(w) = 1\}.$$

This is a subgroup of the semidirect product $(K' \otimes_K L)^\times \rtimes W$, but it is not isomorphic to $\mathsf{G}_1(K')$.

In fact, for $(x, w) \in \mathsf{G}_2(K')$, if $\mathrm{sgn}_W(w) = -1$, then x may be of order $2n$ (Recall that $\mathrm{sgn}_W(w) = 1$ except if W is of even order, and the subgroup generated by w contains a 2-Sylow subgroup of W).

6.4. ***Crossed products.*** Keeping the hypotheses and the notation of Section 6.3, we now consider the Azumaya K-algebra associated to a 2-cocycle θ, that is, a map

$$\theta : W \times W \longrightarrow L^\times$$

satisfying, for $s, t, u \in W$, the relation

$$s(\theta(t, u))\theta(st, u)^{-1}\theta(s, tu)\theta(s, t)^{-1} = 1.$$

We suppose that the cocycle is normalized, in the sense that, for any $s \in W$, one has

$$\theta(s, 1) = \theta(1, s) = 1.$$

The algebra $A = (L/K, \theta)$ associated to θ is the free L-module with basis $(e_s)_{s \in W}$, endowed with the product extending linearly the following relations, for $s, t \in W$ and $\lambda \in L$,

$$e_s e_t = \theta(s, t) e_{st} \tag{6-5}$$

and

$$e_s \lambda = s(\lambda) e_s.$$

The identity of A is e_1, and $Le_1 \subset A$ is a maximal étale K-subalgebra of A; the normalizer of its multiplicative group is the set $\{\lambda e_s \mid \lambda \in L^\times, s \in W\}$. According to Equation (6-5), the determinant of the matrix of the map $a \mapsto \lambda e_s a$, relative to the basis (e_t) is

$$\det(a \mapsto \lambda e_s a) = \lambda^n . \big(\prod_{t \in W} \theta(s, t) \big) . \mathrm{sgn}_W(s).$$

Letting

$$\gamma(s) = \big(\prod_{t \in W} \theta(s, t) \big) . \mathrm{sgn}_W(s),$$

we find for the group functor $\mathsf{G} \subset \mathbf{G}_{m, L/K} \rtimes W$,

$$\mathsf{G}(K') = \{(\lambda, s) \mid \lambda \in (K' \otimes_K L)^\times, s \in W, \lambda^n \gamma(s) = 1\}.$$

References

[Artin 1962] M. Artin, "Grothendieck topologies", mimeographed notes, Harvard University, 1962. Zbl 0208.48701

[Auslander and Goldman 1960] M. Auslander and O. Goldman, "The Brauer group of a commutative ring", *Trans. Amer. Math. Soc.* **97** (1960), 367–409. MR 22 #12130 Zbl 0100.26304

[Bosch et al. 1990] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik (3) **21**, Springer, Berlin, 1990. MR 91i:14034 Zbl 0705.14001

[Bourbaki 1981] N. Bourbaki, *Éléments de mathématique*, Masson, Paris, 1981. Algèbre, chapitres IV à VII. MR 84d:00002 Zbl 0498.12001

[Demazure and Gabriel 1970] M. Demazure and P. Gabriel, *Groupes algébriques, I: Géométrie algébrique, généralités, groupes commutatifs*, Masson, Paris, 1970. MR 46 #1800 Zbl 0203.23401

[Ferrand 1998] D. Ferrand, "Un foncteur norme", *Bull. Soc. Math. France* **126**:1 (1998), 1–49. MR 2000a:13018 Zbl 1017.13005

[Fontaine 1971] J.-M. Fontaine, "Sur la décomposition des algèbres de groupes", *Ann. Sci. École Norm. Sup.* (4) **4** (1971), 121–180. MR 47 #1925 Zbl 0215.10003

[Knus and Ojanguren 1974] M.-A. Knus and M. Ojanguren, *Théorie de la descente et algèbres d'Azumaya*, Lecture Notes in Math. **389**, Springer, Berlin, 1974. MR 54 #5209 Zbl 0284.13002

[Orzech and Small 1975] M. Orzech and C. Small, *The Brauer group of commutative rings*, Lecture Notes Pure Appl. Math. **11**, Dekker, New York, 1975. MR 56 #15627 Zbl 0302.13001

[Serre 1977] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics **42**, Springer, New York, 1977. MR 56 #8675 Zbl 0355.20006

[Waterhouse 1979] W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Math. **66**, Springer, New York, 1979. MR 82e:14003 Zbl 0442.14017

[Yamada 1974] T. Yamada, *The Schur subgroup of the Brauer group*, Lecture Notes in Math. **397**, Springer, Berlin, 1974. MR 50 #456 Zbl 0321.20004

Communicated by Jean-Louis Colliot-Thélène
Received 2007-12-12 Revised 2008-03-31 Accepted 2008-05-06

daniel.ferrand@univ-rennes1.fr *IRMAR, Université de Rennes 1, Campus de Beaulieu,*
35042 Rennes, France

Group actions and rational ideals

Martin Lorenz

We develop the theory of rational ideals for arbitrary associative algebras R without assuming the standard finiteness conditions, noetherianness or the Goldie property. The Amitsur–Martindale ring of quotients replaces the classical ring of quotients which underlies the previous definition of rational ideals but is not available in a general setting.

Our main result concerns rational actions of an affine algebraic group G on R. Working over an algebraically closed base field, we prove an existence and uniqueness result for generic rational ideals in the sense of Dixmier: for every G-rational ideal I of R, the closed subset of the rational spectrum Rat R that is defined by I is the closure of a unique G-orbit in Rat R. Under additional Goldie hypotheses, this was established earlier by Mœglin and Rentschler (in characteristic 0) and by Vonessen (in arbitrary characteristic), answering a question of Dixmier.

Introduction

0.1. Rational ideals have been rather thoroughly explored in various settings. In the simplest case, that of an affine commutative algebra R over an algebraically closed base field $\Bbbk$, rational ideals of R are the same as maximal ideals. More generally, this holds for any affine $\Bbbk$-algebra satisfying a polynomial identity [Procesi 1973]. For other classes of noncommutative algebras R, rational ideals are identical with primitive ideals, that is, annihilators of irreducible R-modules. Examples of such algebras include group algebras of polycyclic-by-finite groups over an algebraically closed base field $\Bbbk$ containing a nonroot of unity [Lorenz and Passman 1979] and enveloping algebras of finite-dimensional Lie algebras over an algebraically closed field $\Bbbk$ of characteristic 0 [Mœglin 1980; Irving and Small 1980]. Rational ideals of enveloping algebras have been the object of intense investigation by Dixmier, Joseph and many others from the late 1960s through the 80s; see Section 0.6 below. The fundamental results concerning algebraic group actions on rational

MSC2000: primary 16W22; secondary 16W35, 17B35.

Keywords: algebraic group, rational action, prime ideal, rational ideal, primitive ideal, generic ideal, extended centroid, Amitsur–Martindale ring of quotient.

Research of the author supported in part by NSA Grant H98230-07-1-0008.

ideal spectra, originally developed in the context of enveloping algebras, were later extended to general noetherian (or Goldie) algebras by Mœglin and Rentschler [1981, 1984, 1986b, 1986a] (for characteristic 0) and by Vonessen [1996, 1998] (for arbitrary characteristic). Currently, the description of rational ideal spectra in algebraic quantum groups is a thriving research topic; see the monograph [Brown and Goodearl 2002] for an introduction. Again, rational ideals turn out to coincide with primitive ideals for numerous examples of quantum groups [Brown and Goodearl 2002, II.8.5].

0.2. The aim of the present article is to liberate the theory of rational ideals of the standard finiteness conditions, noetherianness or the Goldie property, that are traditionally assumed in the literature. Thus, rational ideals are defined and explored here for an arbitrary associative algebra R (with 1) over some base field $\Bbbk$. The Amitsur–Martindale ring of quotients will play the role of the classical ring of quotients which underlies the usual definition of rational ideals but need not exist in general.

Specifically, for any prime ideal P of R, the center of the Amitsur–Martindale ring of quotients of R/P, denoted by $\mathscr{C}(R/P)$ and called the *extended centroid* of R/P, is an extension field of $\Bbbk$. The prime P will be called *rational* if

$$\mathscr{C}(R/P) = \Bbbk.$$

In the special case where R/P is right Goldie, $\mathscr{C}(R/P)$ coincides with the center of the classical ring of quotients of R/P; so our notion of rationality reduces to the familiar one in this case. Following common practice, we will denote the collection of all rational ideals of R by $\operatorname{Rat} R$; so

$$\operatorname{Rat} R \subseteq \operatorname{Spec} R,$$

where $\operatorname{Spec} R$ is the collection of all prime ideals of R, as usual.

0.3. Besides always being available, the extended centroid turns out to lend itself rather nicely to our investigations. In fact, some of our arguments appear to be more straightforward than earlier proofs in more restrictive settings which were occasionally encumbered by the fractional calculus in classical rings of quotients and by the necessity to ensure the transfer of the Goldie property under various constructions. Section 1 is preliminary in nature and serves to deploy the definition and basic properties of extended centroids in a form suitable for our purposes. In particular, we show that all primitive ideals are rational under fairly general circumstances; see Proposition 6.

After sending out the first version of this article, we learned that much of the material in this section was previously known, partly even for nonassociative rings.

For the convenience of the reader, we have opted to leave our proofs intact while also indicating, to the best of our knowledge, the original source of each result.

0.4. In Section 2, we consider actions of a group G by $\Bbbk$-algebra automorphisms on R. Such an action induces G-actions on the extended centroid $\mathscr{C}(R)$ and on the set of ideals of R. Recall that a proper G-stable ideal I of R is said to be *G-prime* if $AB \subseteq I$ for G-stable ideals A and B of R implies that $A \subseteq I$ or $B \subseteq I$. In this case, the subring $\mathscr{C}(R/I)^G$ of G-invariants in $\mathscr{C}(R/I)$ is an extension field of $\Bbbk$. The G-prime I is called *G-rational* if

$$\mathscr{C}(R/I)^G = \Bbbk.$$

We will denote the collections of all G-primes and all G-rational ideals of R by G-Spec R and G-Rat R, respectively; so

$$G\text{-Rat}\, R \subseteq G\text{-Spec}\, R.$$

The action of G on the set of ideals of R preserves both Spec R and Rat R. Writing the corresponding sets of G-orbits as $G\backslash$ Spec R and $G\backslash$ Rat R, the assignment

$$P \mapsto \bigcap_{g\in G} g.P$$

always yields a map

$$G\backslash\, \text{Spec}\, R \longrightarrow G\text{-Spec}\, R. \tag{0-1}$$

Under fairly mild hypotheses, (0-1) is surjective: this certainly holds whenever every G-orbit in R generates a finitely generated ideal of R; see Proposition 8(b). In Proposition 12 we show that (0-1) always restricts to a map

$$G\backslash\, \text{Rat}\, R \longrightarrow G\text{-Rat}\, R. \tag{0-2}$$

More stringent conditions are required for (0-2) to be surjective. If the group G is finite then (0-1) is easily seen to be a bijection, and it follows from Lemma 10 that (0-2) is bijective as well.

0.5. Section 3 focuses on rational actions of an affine algebraic $\Bbbk$-group G on R; the basic definitions will be recalled at the beginning of the section. Working over an algebraically closed base field $\Bbbk$, we show that (0-2) is then a bijection:

Theorem 1. *Let R be an associative algebra over the algebraically closed field $\Bbbk$ and let G be an affine algebraic group over $\Bbbk$ acting rationally by $\Bbbk$-algebra automorphisms on R. Then the map*

$$P \mapsto \bigcap_{g\in G} g.P$$

yields a surjection Rat $R \twoheadrightarrow G$-Rat R *whose fibres are the G-orbits in* Rat R.

The theorem quickly reduces to the situation where G is connected. Theorem 22 below gives a description of the fibre of the map $\operatorname{Rat} R \to G\text{-}\operatorname{Rat} R$ over any given G-rational ideal of R for connected G. This description allows us to prove transitivity of the G-action on the fibres by simply invoking an earlier result of Vonessen [1998, Theorem 4.7] on subfields of the rational function field $\Bbbk(G)$ that are stable under the regular G-action. Under suitable Goldie hypotheses, Theorem 1 is due to Mœglin and Rentschler [1986a, Théorème 2] in characteristic 0 and to Vonessen [1998, Theorem 2.10] in arbitrary characteristic. The basic outline of our proof of Theorem 1 via the description of the fibres as in Theorem 22 is adapted from the groundbreaking work of Mœglin, Rentschler and Vonessen. However, the generality of our setting necessitates a complete reworking of the material and our presentation contains numerous simplifications over the original arguments.

0.6. The systematic investigation of rational ideals in the enveloping algebra $U(\mathfrak{g})$ of a finite-dimensional Lie algebra $\mathfrak{g}$ over an algebraically closed field $\Bbbk$ of characteristic 0 was initiated in [Nouazé and Gabriel 1967; Gabriel 1971]. As mentioned in Section 0.1, it was eventually established that "rational" is tantamount to "primitive" for ideals of $U(\mathfrak{g})$; over an uncountable base field $\Bbbk$, this is due to Dixmier [1977]. The reader is referred to the standard reference [Dixmier 1996] for a detailed account of the theory of primitive ideals in enveloping algebras; for an updated survey, see [Rentschler 1987]. Here we just mention that the original motivation behind Theorem 1 and its predecessors was a question of Dixmier [1972] (see also [Dixmier 1996, Problem 11]) concerning primitive ideals of $U(\mathfrak{g})$. Specifically, if G is the adjoint algebraic group of $\mathfrak{g}$ then, for any ideal $\mathfrak{k}$ of $\mathfrak{g}$ and any primitive ideal Q of $U(\mathfrak{g})$, the ideal $I = Q \cap U(\mathfrak{k})$ of $U(\mathfrak{k})$ is G-rational [Dixmier 1977]. Dixmier asked if the following are true for I:

(a) $I = \bigcap_{g \in G} g.P$ for some primitive ideal P of $U(\mathfrak{k})$, and

(b) any two such primitive ideals belong to the same G-orbit.

The earlier version of Theorem 1, due to Mœglin and Rentschler, settled both (a) and (b) in the affirmative. Letting $\operatorname{Prim} U(\mathfrak{k})$ denote the collection of all primitive ideals of $U(\mathfrak{k})$ endowed with the Jacobson–Zariski topology, (a) says that the set

$$\{J \in \operatorname{Prim} U(\mathfrak{k}) \mid J \supseteq I\}$$

is the closure of the orbit $G.P$ in $\operatorname{Prim} U(\mathfrak{k})$. Following Dixmier [1972] such P are called *generic* for I. The uniqueness of generic orbits as in (b) was proved for solvable $\mathfrak{g}$ in [Borho et al. 1973] and generally (over uncountable $\Bbbk$) in [Rentschler 1979]; this fact was instrumental for the proof that the Dixmier and Duflo maps are injective in the solvable and algebraic case, respectively [Rentschler 1974; Duflo 1982].

0.7. In future work, we hope to address some topological aspects of Rat R endowed with the Jacobson–Zariski topology from Spec R. Finally, it remains to bring the machinery developed herein to bear on new classes of algebras that lack the traditional finiteness conditions.

1. The extended centroid

Throughout this section, R will denote an associative ring. It is understood that all rings have a 1 which is inherited by subrings and preserved under homomorphisms.

1.1. ***The Amitsur–Martindale ring of quotients.*** Let $\mathscr{E} = \mathscr{E}(R)$ denote the filter consisting of all (two-sided) ideals I of R such that

$$\text{l.}\,\text{ann}_R\, I = \{r \in R \mid rI = 0\} = 0.$$

The right Amitsur–Martindale ring of quotients, introduced for prime rings R by Martindale [1969b] and in general by Amitsur [1972], is defined by

$$\mathrm{Q_r}(R) = \varinjlim_{I \in \mathscr{E}} \mathrm{Hom}(I_R, R_R).$$

Explicitly, the elements of $\mathrm{Q_r}(R)$ are equivalence classes of right R-module maps $f : I_R \to R_R$ with $I \in \mathscr{E}$; the map f is defined to be equivalent to $f' : I'_R \to R_R$ ($I' \in \mathscr{E}$) if f and f' agree on some ideal $J \subseteq I \cap I'$, $J \in \mathscr{E}$. In this case, f and f' actually agree on $I \cap I'$; see [Amitsur 1972, Lemma 1]. The sum of two elements $q, q' \in \mathrm{Q_r}(R)$, represented by

$$f : I_R \to R_R \ (I \in \mathscr{E}) \quad \text{and} \quad f' : I'_R \to R_R \ (I' \in \mathscr{E}),$$

respectively, is defined to be the class of

$$f + f' : I \cap I' \to R.$$

Similarly, the product $qq' \in \mathrm{Q_r}(R)$ is the class of the composite

$$f \circ f' : I'I \to R.$$

This makes $\mathrm{Q_r}(R)$ into a ring; the identity element is the class of the identity map Id_R on R. Sending an element $r \in R$ to the equivalence class of the map

$$\lambda_r : R \to R, \ x \mapsto rx$$

yields an embedding of R as a subring of $\mathrm{Q_r}(R)$. Suppose the element $q \in \mathrm{Q_r}(R)$ is represented by $f : I_R \to R_R$ ($I \in \mathscr{E}$). Then the equality $f \circ \lambda_r = \lambda_{f(r)}$ ($r \in I$) shows that $qI \subseteq R$.

We summarize the foregoing and some easy consequences thereof in the following proposition. Complete details can be found in [Amitsur 1972] and in [Passman 1989, Proposition 10.2], for example.

Proposition 2. *The ring* $\mathrm{Q_r}(R)$ *has the following properties*:

(i) *There is a ring embedding* $R \hookrightarrow \mathrm{Q_r}(R)$;

(ii) *for each* $q \in \mathrm{Q_r}(R)$, *there exits* $I \in \mathscr{E}$ *with* $qI \subseteq R$;

(iii) *if* $qI = 0$ *for* $q \in \mathrm{Q_r}(R)$ *and* $I \in \mathscr{E}$ *then* $q = 0$;

(iv) *given* $f : I_R \to R_R$ *with* $I \in \mathscr{E}$, *there exists* $q \in \mathrm{Q_r}(R)$ *with* $qr = f(r)$ *for all* $r \in I$.

Moreover, $\mathrm{Q_r}(R)$ *is characterized by these properties*: *any other ring satisfying* (i)–(iv) *is* R*-isomorphic to* $\mathrm{Q_r}(R)$.

1.2. *The extended centroid.* The extended centroid of R is defined to be the center of $\mathrm{Q_r}(R)$; it will be denoted by $\mathscr{C}(R)$:

$$\mathscr{C}(R) = \mathscr{Z}(\mathrm{Q_r}(R)).$$

It is easy to see from Proposition 2 that $\mathscr{C}(R)$ coincides with the centralizer of R in $\mathrm{Q_r}(R)$:

$$\mathscr{C}(R) = C_{\mathrm{Q_r}(R)}(R) = \{\, q \in \mathrm{Q_r}(R) \mid qr = rq \text{ for all } r \in R \,\}.$$

In particular, the center $\mathscr{Z}(R)$ of R is contained in $\mathscr{C}(R)$. Moreover, an element $q \in \mathrm{Q_r}(R)$ belongs to $\mathscr{C}(R)$ if and only if q is represented by an (R, R)-*bimodule* map $f : I \to R$ with $I \in \mathscr{E}$; in this case, every representative

$$f' : I'_R \to R_R \quad (I' \in \mathscr{E})$$

of q is an (R, R)-bimodule map; see [Amitsur 1972, Theorem 3].

1.2.1. By reversing sides, one can define the left ring of quotients $\mathrm{Q}_\ell(R)$ and its center $\mathscr{C}_\ell(R) = \mathscr{Z}(\mathrm{Q}_\ell(R))$ as above. However, we will mainly be concerned with semiprime rings, that is, rings R having no nonzero ideals of square 0. In that case,

$$\mathrm{l.ann}_R\, I = \mathrm{r.ann}_R\, I$$

holds for every ideal I of R; so the definition of $\mathscr{E}(R)$ is symmetric. Moreover, any $q \in \mathscr{C}(R)$ is represented by an (R, R)-bimodule map $f : I \to R$ with $I \in \mathscr{E}$. The class of f in $\mathrm{Q}_\ell(R)$ is an element $q' \in \mathscr{C}_\ell(R)$, and the map $q \mapsto q'$ yields an isomorphism $\mathscr{C}(R) \xrightarrow{\sim} \mathscr{C}_\ell(R)$. In the following, we shall always work with $\mathrm{Q_r}(R)$ and $\mathscr{C}(R)$.

1.2.2. Let R be semiprime. Then one knows that $\mathscr{C}(R)$ is a von Neumann regular ring. Moreover, R is prime if and only if $\mathscr{C}(R)$ is a field; see [Amitsur 1972, Theorem 5].

1.3. ***Central closure.*** Rings R such that $\mathscr{C}(R) \subseteq R$ are called *centrally closed*. In this case, $\mathscr{C}(R) = \mathscr{Z}(R)$. For every semiprime ring R, the subring $R\mathscr{C}(R)$ of $\mathrm{Q_r}(R)$ is a semiprime centrally closed ring called the *central closure* of R; see [Baxter and Martindale 1979, Theorem 3.2]. If R is prime then so is the central closure $R\mathscr{C}(R)$ by Proposition 2(ii).

Lemma 3 [Martindale 1969b]. *Let R be a prime centrally closed ring and let S be an algebra over the field $C = \mathscr{C}(R)$. Then*:

(a) *Every nonzero ideal I of $R \otimes_C S$ contains an element $0 \neq r \otimes s$ with $r \in R$, $s \in S$.*

(b) *If S is simple then every nonzero ideal I of $R \otimes_C S$ intersects R nontrivially. Consequently, $R \otimes_C S$ is prime.*

(c) *If I is a prime ideal of $R \otimes_C S$ such that $I \cap R = 0$ then $I = R \otimes_C (I \cap S)$.*

Proof. (a) Fix a C-basis $\{s_i\}$ of S. Consider an element $0 \neq t = \sum_i r_i \otimes s_i \in I$ with a minimal number of nonzero R-coefficients r_i among all nonzero elements of I and choose i_0 with $r = r_{i_0} \neq 0$. Then the element

$$rxt - txr = \sum_{i \neq i_0} (rxr_i - r_i xr) \otimes s_i$$

must be zero for all $x \in R$. Hence $rxr_i = r_i xr$ holds for all i, and by [Martindale 1969b, Theorem 1], there are $c_i \in C$ such that $r_i = rc_i$. Therefore, $t = r \otimes s$ with $s = \sum_i c_i s_i \in S$.

(b) If S is simple then we can make $s = 1$ in (a), and so $0 \neq r \in I \cap R$. Since R is prime, it follows that $R \otimes_C S$ is prime as well.

(c) Suppose for a contradiction that $I \supsetneqq R \otimes_C (I \cap S)$. Replacing S by $S/(I \cap S)$, we may assume that $I \neq 0$ but $I \cap R = 0$ and $I \cap S = 0$. Choosing $r \otimes s \in I$ as in (a), we obtain that

$$I \supseteq S(r \otimes s)R = rR \otimes_C Ss.$$

Since I is prime, we must have $r \in I$ or $s \in I$, whence the desired contradiction. □

1.4. ***Examples.***

1.4.1. If R is a simple ring, or a finite product of simple rings, then $\mathscr{E}(R) = \{R\}$, and hence $\mathrm{Q_r}(R) = R$ by Proposition 2(i)(ii). Thus, R is certainly centrally closed in this case. Less trivial examples of centrally closed rings include crossed products $R * F$ with R a simple ring and F a free semigroup on at least two generators [Passman

1989, Theorem 13.4] and Laurent power series rings $R((x))$ over centrally closed rings R [Martindale et al. 1990].

1.4.2. If R is semiprime right Goldie then $\mathscr{C}(R) = \mathscr{Z}(\mathrm{Q}_{\mathrm{cl}}(R))$, the center of the classical ring of quotients of R. Indeed, $\mathrm{Q}_{\mathrm{cl}}(R)$ coincides with the maximal ring of quotients $\mathrm{Q}_{\max}(R)$ in this case; see, for example, [Lambek 1976, Proposition 4.6.2]. Furthermore, the Amitsur–Martindale ring of quotients $\mathrm{Q}_{\mathrm{r}}(R)$ is R-isomorphic to the subring of $\mathrm{Q}_{\max}(R)$ consisting of all $q \in \mathrm{Q}_{\max}(R)$ such that $qI \subseteq R$ for some $I \in \mathscr{E}(R)$; see [Passman 1991, Chapter 24] or [Montgomery 1980, Chapter 3]. This isomorphism yields an isomorphism $\mathscr{C}(R) \cong \mathscr{Z}(\mathrm{Q}_{\max}(R))$.

1.4.3. Let R be a semiprime homomorphic image of the enveloping algebra $U(\mathfrak{g})$ of a finite-dimensional Lie algebra $\mathfrak{g}$ over some base field $\Bbbk$. Answering a question of Rentschler, we show here that

$$\mathrm{Q}_{\mathrm{r}}(R) \textit{ consists of all } \operatorname{ad}\mathfrak{g}\textit{-finite elements of } \mathrm{Q}_{\mathrm{cl}}(R).$$

Here

$$\operatorname{ad}\colon U(\mathfrak{g}) \to \operatorname{End}_{\Bbbk} \mathrm{Q}_{\mathrm{cl}}(R)$$

is the standard adjoint action, given by $\operatorname{ad} x(q) = xq - qx$ for $x \in \mathfrak{g}$ and $q \in \mathrm{Q}_{\mathrm{cl}}(R)$, and q is called $\operatorname{ad}(\mathfrak{g})$-*finite* if the $\Bbbk$-subspace $\operatorname{ad} U(\mathfrak{g})(q)$ of $\mathrm{Q}_{\mathrm{cl}}(R)$ is finite-dimensional.

Proof. Recall from Section 1.4.2 that

$$\mathrm{Q}_{\mathrm{r}}(R) = \{\, q \in \mathrm{Q}_{\mathrm{cl}}(R) \mid qI \subseteq R \text{ for some } I \in \mathscr{E}(R) \,\}.$$

First consider $q \in \mathrm{Q}_{\mathrm{r}}(R)$. Letting R_n and $I_n = I \cap R_n$ $(n \geq 0)$ denote the filtrations of R and I, respectively, that are induced by the canonical filtration of $U(\mathfrak{g})$ [Dixmier 1996, 2.3.1], we have $I = I_s R$ and $qI_s \subseteq R_t$ for suitable $s, t \geq 0$. Since both I_s and R_t are $\operatorname{ad}(\mathfrak{g})$-stable, it follows that $\operatorname{ad} U(\mathfrak{g})(q) I_s \subseteq R_t$. Furthermore,

$$\mathrm{l.\,ann}_{\mathrm{Q}_{\mathrm{cl}}(R)} I_s = \mathrm{l.\,ann}_{\mathrm{Q}_{\mathrm{cl}}(R)} I = 0;$$

so $\operatorname{ad} U(\mathfrak{g})(q)$ embeds into $\operatorname{Hom}_{\Bbbk}(I_s, R_t)$ proving that q is $\operatorname{ad}(\mathfrak{g})$-finite. Conversely, suppose that $q \in \mathrm{Q}_{\mathrm{cl}}(R)$ is $\operatorname{ad}(\mathfrak{g})$-finite and let $\{q_i\}_1^m$ be a $\Bbbk$-basis of $\operatorname{ad} U(\mathfrak{g})(q)$. Each $D_i = \{r \in R \mid q_i r \in R\}$ is an essential right ideal of R, and hence

$$I = \bigcap_{i=1}^{m} D_i = \{\, r \in R \mid \operatorname{ad} U(\mathfrak{g})(q) r \subseteq R \,\}$$

is an essential right ideal of R which is also $\operatorname{ad}(\mathfrak{g})$-stable, since this holds for $\operatorname{ad} U(\mathfrak{g})(q)$ and R. Therefore, $I \in \mathscr{E}(R)$ which shows that $q \in \mathrm{Q}_{\mathrm{r}}(R)$. □

1.5. ***Centralizing homomorphisms.*** A ring homomorphism $\varphi\colon R \to S$ is called *centralizing* if the ring S is generated by $\varphi(R)$ and the centralizer

$$C_S(\varphi(R)) = \{s \in S \mid s\varphi(r) = \varphi(r)s \text{ for all } r \in R\}.$$

Surjective ring homomorphisms are clearly centralizing, and composites of centralizing homomorphisms are again centralizing. Note also that any centralizing homomorphism $\varphi\colon R \to S$ sends the center $\mathscr{Z}(R)$ of R to $\mathscr{Z}(S)$. Finally, φ induces a map

$$\operatorname{Spec} S \to \operatorname{Spec} R, \quad P \mapsto \varphi^{-1}(P).$$

For any $q \in \mathrm{Q_r}(R)$, we define the ideal D_q of R by

$$D_q = \{r \in R \mid qRr \subseteq R\}. \tag{1-1}$$

By Proposition 2(ii), $D_q \in \mathscr{E}(R)$. If $q \in \mathscr{C}(R)$ then the description of the ideal D_q simplifies to

$$D_q = \{r \in R \mid qr \subseteq R\}.$$

Lemma 4. *Let $\varphi\colon R \to S$ be a centralizing homomorphism of rings. Put*

$$\mathscr{C}_\varphi = \left\{ q \in \mathscr{C}(R) \;\middle|\; \mathrm{l.ann}_S\, \varphi(D_q) = 0 \right\}.$$

Then $R\mathscr{C}_\varphi$ is a subring of $\mathrm{Q_r}(R)$ containing R. The map φ extends uniquely to a centralizing ring homomorphism $\widetilde{\varphi}\colon R\mathscr{C}_\varphi \to S\mathscr{C}(S)$. In particular, $\widetilde{\varphi}(\mathscr{C}_\varphi) \subseteq \mathscr{C}(S)$.

Proof. Put

$$R_\varphi = \left\{ q \in \mathrm{Q_r}(R) \;\middle|\; \mathrm{l.ann}_S\, \varphi(D_q) = 0 \right\}.$$

Since $R = \{q \in \mathrm{Q_r}(R) \mid 1 \in D_q\}$, we certainly have $R \subseteq R_\varphi$. For $q, q' \in \mathrm{Q_r}(R)$, one easily checks that $D_{q'}D_q \subseteq D_q \cap D_{q'} \subseteq D_{q+q'}$ and $D_{q'}D_q \subseteq D_{qq'}$. Moreover, if $\varphi(D_q)$ and $\varphi(D_{q'})$ both have zero left annihilator in S then so does $\varphi(D_{q'}D_q) = \varphi(D_{q'})\varphi(D_q)$. This shows that $q + q' \in R_\varphi$ and $qq' \in R_\varphi$ for $q, q' \in R_\varphi$; so R_φ is a subring of $\mathrm{Q_r}(R)$ containing R. Since $\mathscr{C}_\varphi = \mathscr{Z}(R_\varphi)$, it follows that $R\mathscr{C}_\varphi$ is also a subring of $\mathrm{Q_r}(R)$ containing R.

Now let $q \in \mathscr{C}_\varphi$ be given. Then $\varphi(D_q)S = \varphi(D_q)C_S(\varphi(R)) \in \mathscr{E}(S)$. Define $\bar{q}\colon \varphi(D_q)S \to S$ by

$$\bar{q}\left(\sum_i \varphi(x_i)c_i\right) = \sum_i \varphi(qx_i)c_i$$

for $x_i \in D_q$, $c_i \in C_S(\varphi(R))$. To see that $\bar{q}$ is well-defined, note that, for each $d \in D_q$, we have

$$\begin{aligned}\sum_i \varphi(x_i)c_i\varphi(qd) &= \sum_i \varphi(x_i)\varphi(qd)c_i = \sum_i \varphi(x_iqd)c_i \\ &= \sum_i \varphi(qx_id)c_i = \sum_i \varphi(qx_i)\varphi(d)c_i \\ &= \sum_i \varphi(qx_i)c_i\varphi(d).\end{aligned}$$

Thus, if $\sum_i \varphi(x_i)c_i = \sum_j \varphi(y_j)e_j$ with $x_i, y_j \in D_q$ and $c_i, e_j \in C_S(\varphi(R))$ then the above computation gives

$$0=\Bigl(\sum_i \varphi(x_i)c_i-\sum_j \varphi(y_j)e_j\Bigr)\varphi(qD_q)=\Bigl(\sum_i \varphi(qx_i)c_i-\sum_j \varphi(qy_j)e_j\Bigr)\varphi(D_q),$$

and so $0 = \sum_i \varphi(qx_i)c_i - \sum_j \varphi(qy_j)e_j$. Therefore, $\bar{q}$ is well-defined.

It is straightforward to check that $\bar{q}$ is an (S, S)-bimodule map. Hence, the class of $\bar{q}$ in $\mathrm{Q_r}(R)$ is an element $\widetilde{\varphi}(q) \in \mathscr{C}(S)$. The map $q \mapsto \widetilde{\varphi}(q)$ is a ring homomorphism $\mathscr{C}_\varphi \to \mathscr{C}(S)$ which yields the desired extension

$$\begin{aligned}&\widetilde{\varphi}\colon R\mathscr{C}_\varphi \to S\mathscr{C}(S),\\ &\widetilde{\varphi}(\sum_i r_iq_i) = \sum_i \varphi(r_i)\widetilde{\varphi}(q_i),\end{aligned}$$

for $r_i \in R$, $q_i \in \mathscr{C}_\varphi$. Well-definedness and uniqueness of $\widetilde{\varphi}$ follow easily from the fact that, given finitely many $x_i \in R_\varphi$, there is an ideal D of R with $\mathrm{l.\,ann}_S\, \varphi(D) = 0$ and $x_iD \subseteq R$ for all i. □

In the special case where both R and S are commutative domains in Lemma 4 above, we have $\mathrm{Q_r}(R) = \mathscr{C}(R) = \operatorname{Fract} R$, the classical field of fractions of R, and similarly for S. Moreover, $R\mathscr{C}_\varphi = R_P$ is the localization of R at the prime $P = \operatorname{Ker}\varphi$ and the map $R\mathscr{C}_\varphi \to S\mathscr{C}(S)$ is the usual map $R_P \to \operatorname{Fract} S$.

1.6. ***Extended centroids and primitive ideals.*** By Schur's Lemma, the endomorphism ring $\mathrm{End}_R\, V$ of any simple R-module V_R is a division ring. The following lemma is well-known in the special case of noetherian (or Goldie) rings (see, for example, [Dixmier 1996, 4.1.6]); for general rings, the lemma was apparently first observed by Martindale [1969a, Theorem 12]. Since the latter result is stated in terms of the so-called complete ring of quotients, we include the proof for the reader's convenience.

Lemma 5. *Let V_R be a simple R-module, and let $P = \mathrm{ann}_R\, V$ be its annihilator. Then the canonical embedding $\mathscr{Z}(R/P) \hookrightarrow \mathscr{Z}(\mathrm{End}_R\, V)$ extends to an embedding* *of fields*

$$\mathscr{C}(R/P) \hookrightarrow \mathscr{Z}(\mathrm{End}_R V).$$

Proof. We may assume that $P = 0$. For a given $q \in \mathscr{C}(R)$, we wish to define an endomorphism $\delta_q \in \mathscr{Z}(\mathrm{End}_R V)$. To this end, note that every $x \in V$ can be written as $x = vd$ for suitable $d \in D_q$, $v \in V$. Define

$$\delta_q(x) = v(dq) \in V.$$

To see that this is well-defined, assume that $vd = v'd'$ holds for $v, v' \in V$ and $d, d' \in D_q$. Then

$$\big(v(dq) - v'(d'q)\big)D_q = (vd - v'd')(qD_q) = 0$$

and so $v(dq) - v'(d'q) = 0$. It is straightforward to check that $\delta_q \in \mathrm{End}_R V$. Moreover, for any $\delta \in \mathrm{End}_R V$ and $vd \in V$, one computes

$$\delta\delta_q(vd) = \delta(v(dq)) = \delta(v)(dq) = \delta_q(\delta(v)d) = \delta_q\delta(vd).$$

Thus, $\delta_q \in \mathscr{Z}(\mathrm{End}_R V)$. The map $\mathscr{C}(R) \to \mathscr{Z}(\mathrm{End}_R V)$, $q \mapsto \delta_q$, is easily seen to be additive. Furthermore, for $q, q' \in \mathscr{C}(R)$, $d \in D_q$, $d' \in D_{q'}$ and $v \in V$, one has

$$\delta_{qq'}(vd'd) = v(d'dqq') = v(d'q')(dq) = \delta_q(\delta_{q'}(vd')d) = \delta_q(\delta_{q'}(vd'd)).$$

Thus, the map is a ring homomorphism; it is injective because $\mathscr{C}(R)$ is a field. □

1.7. *Rational algebras and ideals.* An algebra R over some field $\Bbbk$ will be called *rational* (or $\Bbbk$-*rational*) if R is prime and $\mathscr{C}(R) = \Bbbk$. A prime ideal P of R will be called *rational* if R/P is a rational $\Bbbk$-algebra. In view of Section 1.2.1, the notion of rationality is left-right symmetric.

We remark that rational $\Bbbk$-algebras are called *closed over* $\Bbbk$ in [Erickson et al. 1975] where such algebras are investigated in a nonassociative context. Alternatively, one could define a prime $\Bbbk$-algebra R to be rational if the field extension $\mathscr{C}(R)/\Bbbk$ is algebraic; for noetherian (or Goldie) algebras, this version of rationality is adopted in many places in the literature (for example, [Brown and Goodearl 2002]). However, we will work with the above definition throughout.

1.7.1. By Section 1.3 the central closure $R\mathscr{C}(R)$ of any prime ring R is $\mathscr{C}(R)$-rational.

1.7.2. The Schur division rings $\mathrm{End}_R V$ considered in Section 1.6 are division algebras over $\Bbbk$, and their centers are extension fields of $\Bbbk$. We will say that the algebra R satisfies the *weak Nullstellensatz* if $\mathscr{Z}(\mathrm{End}_R V)$ is algebraic over $\Bbbk$ for every simple R-module V_R.

Proposition 6. *If R is a $\Bbbk$-algebra satisfying the weak Nullstellensatz and $\Bbbk$ is algebraically closed then all primitive ideals of R are rational.*

Proof. By hypothesis, $\mathscr{Z}(\operatorname{End}_R V) = \Bbbk$ holds for every simple R-module V_R. It follows from Lemma 5 that $P = \operatorname{ann}_R V$ satisfies $\mathscr{C}(R/P) = \Bbbk$. □

For an affine commutative $\Bbbk$-algebra R, the Schur division algebras in question are just the quotients R/P, where P is a maximal ideal of R. The classical weak Nullstellensatz is equivalent to the statement that R/P is always algebraic over $\Bbbk$; see [Lang 2002, Theorem IX.1.4]. Thus affine commutative algebras do satisfy the weak Nullstellensatz.

Many noncommutative algebras satisfying the weak Nullstellensatz are known; see [McConnell and Robson 2001, Chapter 9] for an overview. In fact, as long as the cardinality of the base field $\Bbbk$ is larger than $\dim_{\Bbbk} R$, the weak Nullstellensatz is guaranteed to hold; see [McConnell and Robson 2001, Corollary 9.1.8] or [Brown and Goodearl 2002, II.7.16]. This applies, for example, to any countably generated algebra over an uncountable field $\Bbbk$.

1.8. ***Scalar extensions.*** We continue to let R denote an algebra over some field $\Bbbk$. For any given $\Bbbk$-algebra A, we have an embedding

$$\mathrm{Q_r}(R) \otimes_{\Bbbk} A \hookrightarrow \mathrm{Q_r}(R \otimes_{\Bbbk} A)$$

which extends the canonical embedding $R \otimes_{\Bbbk} A \hookrightarrow \mathrm{Q_r}(R \otimes_{\Bbbk} A)$. For, let $q \in \mathrm{Q_r}(R)$ be represented by the map $f : I_R \to R_R$ with $I \in \mathscr{E}(R)$. Then $I \otimes_{\Bbbk} A \in \mathscr{E}(R \otimes_{\Bbbk} A)$. Sending q to the class of the map $f \otimes \mathrm{Id}_A$ we obtain a ring homomorphism

$$\mathrm{Q_r}(R) \to \mathrm{Q_r}(R \otimes_{\Bbbk} A)$$

extending the canonical embedding

$$R \hookrightarrow R \otimes_{\Bbbk} A \hookrightarrow \mathrm{Q_r}(R \otimes_{\Bbbk} A).$$

By Proposition 2(ii)(iii), the image of $\mathrm{Q_r}(R)$ in $\mathrm{Q_r}(R \otimes_{\Bbbk} A)$ commutes with A and the resulting map

$$\mathrm{Q_r}(R) \otimes_{\Bbbk} A \to \mathrm{Q_r}(R \otimes_{\Bbbk} A)$$

is injective. Moreover, since $f \otimes \mathrm{Id}_A$ is an $(R \otimes_{\Bbbk} A, R \otimes_{\Bbbk} A)$-bimodule map if f is an (R, R)-bimodule map, the embedding of $\mathrm{Q_r}(R)$ into $\mathrm{Q_r}(R \otimes_{\Bbbk} A)$ sends $\mathscr{C}(R)$ to $\mathscr{C}(R \otimes_{\Bbbk} A)$. Thus, if A is commutative, this yields an embedding

$$\mathscr{C}(R) \otimes_{\Bbbk} A \hookrightarrow \mathscr{C}(R \otimes_{\Bbbk} A). \tag{1-2}$$

The following lemma is the associative case of [Erickson et al. 1975, Theorem 3.5].

Lemma 7. *Assume that R is rational. Then, for every field extension $K/\Bbbk$, the K-algebra $R_K = R \otimes_{\Bbbk} K$ is rational.*

Proof. By Lemma 3(b), we know that R_K is prime. Moreover, for any given $q \in \mathscr{C}(R_K)$, we may choose an element $0 \neq x \in D_q \cap R$. Fix a $\Bbbk$-basis $\{k_i\}$ for K. The map

$$q_i \colon I = RxR \xrightarrow{q\cdot} R_K \overset{\text{proj}}{\twoheadrightarrow} R \otimes k_i \xrightarrow{\sim} R$$

is an (R, R)-bimodule map. Hence q_i is multiplication with some $c_i \in \Bbbk$, by hypothesis on R, and all but finitely many c_i are zero. Therefore, the map $I \xrightarrow{q\cdot} R_K$ is multiplication with $k = \sum_i c_i k_i \in K$. Consequently, $q = k \in K$. □

2. Group actions

In this section, we assume that a group G acts by automorphisms on the ring R; the action will be written as $G \times R \to R$, $(g, r) \mapsto g.r$.

2.1. Let M be a set with a left G-action $G \times M \to M$, $(g, m) \mapsto g.m$. For any subset X of M,

$$G_X = \operatorname{stab}_G X = \{g \in G \mid g.X = X\}$$

will denote the isotropy group of X. Furthermore, we put

$$(X : G) = \bigcap_{g \in G} g.X \ ;$$

this is the largest G-stable subset of M that is contained in X. We will be primarily concerned with the situation where $M = R$ and X is an ideal of R in which case $(X : G)$ is also an ideal of R.

2.2. ***G-primes.*** The ring R is said to be *G-prime* if $R \neq 0$ and the product of any two nonzero G-stable ideals of R is again nonzero. A G-stable ideal I of R is called *G-prime* if R/I is a G-prime ring for the G-action on R/I coming from the given action of G on R. In the special case where the G-action on R is trivial, G-primes of R are just the prime ideals of R in the usual sense. Recall that the collection of all G-prime ideals of R is denoted by G-Spec R while Spec R is the collection of all ordinary primes of R.

Proposition 8. (a) *There is a well-defined map*

$$\operatorname{Spec} R \longrightarrow G\text{-}\operatorname{Spec} R\,, \qquad P \mapsto (P : G).$$

(b) *Assume that, for each $r \in R$, the G-orbit $G.r$ generates a finitely generated ideal of R. Then the map in* (a) *is surjective. In particular, all G-primes of R are semiprime in this case.*

Proof. It is straightforward to check that $(P : G)$ is G-prime for any prime ideal P of R; so (a) is clear.

For (b), consider a G-prime ideal I of R. We will show that there is an ideal P of R which is maximal subject to the condition $(P : G) = I$; the ideal P is then easily seen to be prime. In order to prove the existence of P, we use Zorn's Lemma. So let $\{I_j\}$ be a chain of ideals of R such that $(I_j : G) = I$ holds for all j. We need to show that the ideal $I_* = \bigcup_j I_j$ satisfies $(I_* : G) = I$. For this, let $r \in (I_* : G)$ be given. Then the ideal $(G.r)$ that is generated by $G.r$ is contained in $(I_* : G)$ and $(G.r)$ is a finitely generated G-stable ideal of R. Therefore, $(G.r) \subseteq (I_j : G)$ for some j and so $r \in I$, as desired. □

For brevity, we will call G-actions satisfying the finiteness hypothesis in (b) above *locally ideal finite*. Clearly, all actions of finite groups as well as all group actions on noetherian rings are locally ideal finite. Another important class of examples are the *locally finite* actions in the usual sense: by definition, these are G-actions on some $\Bbbk$-algebra R such that the G-orbit of each $r \in R$ generates a finite-dimensional $\Bbbk$-subspace of R. This includes the rational actions of algebraic groups to be considered in Section 3. In all these cases, Proposition 8 is a standard result; the argument given above is merely a variant of earlier proofs.

2.3. ***G-primes and the extended centroid.*** The G-action on R extends uniquely to an action of G on $\mathrm{Q_r}(R)$: if $q \in \mathrm{Q_r}(R)$ is represented by $f : I_R \to R_R$ $(I \in \mathscr{E})$ then $g.q \in \mathrm{Q_r}(R)$ is defined to be the class of the map $g.f : g.I \to R$ that is given by

$$(g.f)(g.x) = g.f(x)$$

for $x \in I$. Therefore, G also acts on the extended centroid $\mathscr{C}(R)$ of R. As usual, the ring of G-invariants in $\mathscr{C}(R)$ will denoted by $\mathscr{C}(R)^G$.

Proposition 9. *If R is G-prime then $\mathscr{C}(R)^G$ is a field. Conversely, if R is semiprime and $\mathscr{C}(R)^G$ is a field then R is G-prime.*

Proof. We follow the outline of the proof of [Amitsur 1972, Theorem 5].

First assume that R is G-prime and let $0 \neq q \in \mathscr{C}(R)^G$ be given. Then qD_q is a nonzero G-stable ideal of R, and hence $\mathrm{l.ann}_R(qD_q) = 0$ because R is G-prime. So $qD_q \in \mathscr{E}(R)$. Moreover,

$$\mathrm{ann}_R(q) = \{r \in R \mid rq = 0\} \subseteq \mathrm{l.ann}_R(qD_q)$$

and so $\mathrm{ann}_R(q) = 0$. Therefore, the map $D_q \to qD_q$, $r \mapsto qr = rq$, is an (R, R)-bimodule isomorphism which is G-equivariant. The class of the inverse map belongs to $\mathscr{C}(R)^G$ and is the desired inverse for q.

Next, assume that R is semiprime but not G-prime. Then there exists a nonzero G-stable ideal I of R such that $J = \mathrm{l.ann}_R(I) \neq 0$. Since R is semiprime, the sum $I + J$ is direct and $I + J \in \mathscr{E}(R)$. Define maps $f, f' : I + J \to R$ by

$$f(i + j) = i \quad \text{and} \quad f'(i + j) = j.$$

Letting q and q' denote the classes of f and f', respectively, in $\mathrm{Q_r}(R)$ we have $f, f' \in \mathscr{C}(R)^G$ and $ff' = 0$. Therefore, $\mathscr{C}(R)^G$ is not a field. □

The following technical lemma will be crucial. Recall that G_I denotes the isotropy group of I.

Lemma 10. *Let P be a prime ideal of R.*

(a) *For every subgroup of $H \leq G$, the canonical map $R/(P : G) \twoheadrightarrow R/(P : H)$ induces an embedding of fields*

$$\mathscr{C}(R/(P : G))^G \hookrightarrow \mathscr{C}(R/(P : H))^{G_{(P:H)}}.$$

The degree of the field extension is at most $[G : G_{(P:H)}]$.

(b) *If P has a finite G-orbit then we obtain an isomorphism of fields*

$$\mathscr{C}(R/(P : G))^G \xrightarrow{\sim} \mathscr{C}(R/P)^{G_P}.$$

Proof. (a) After factoring out the ideal $(P : G)$ we may assume that $(P : G) = 0$, R is G-prime, and $\mathscr{C}(R)^G$ is a field; see Propositions 8 and 9. Consider the canonical map

$$\varphi\colon R \twoheadrightarrow S := R/(P : H).$$

Using the notation of Lemma 4, we have $\mathscr{C}(R)^G \subseteq \mathscr{C}_\varphi$. Indeed, for each $q \in \mathscr{C}(R)^G$, the ideal D_q is nonzero and G-stable, and hence $D_q \nsubseteq P$. Therefore, $\varphi(D_q)$ is a nonzero H-stable ideal of the H-prime ring S, and so $\varphi(D_q) \in \mathscr{E}(S)$. The map $\mathscr{C}_\varphi \to \mathscr{C}(S)$ constructed in Lemma 4 yields an embedding $\mathscr{C}(R)^G \hookrightarrow \mathscr{C}(S)$: the image of $q \in \mathscr{C}(R)^G$ is the class of the map $f\colon \varphi(D_q) \to S$ that is defined by $f(\varphi(x)) = \varphi(qx)$ for $x \in D_q$. Since φ is $G_{(P:H)}$-equivariant, one computes, for $x \in D_q$ and $g \in G_{(P:H)}$,

$$\begin{aligned}(g.f)(g.\varphi(x)) &= g.f(\varphi(x)) = g.\varphi(qx) = \varphi(g.(qx))\\ &= \varphi(q(g.x)) = f(\varphi(g.x)) = f(g.\varphi(x));\end{aligned}$$

so $g.f = f$. Therefore the image of $\mathscr{C}(R)^G$ is contained in $\mathscr{C}(S)^{G_{(P:H)}}$.

It remains to show that

$$\left[\mathscr{C}(S)^{G_{(P:H)}} : \mathscr{C}(R)^G\right] \leq [G : G_{(P:H)}]$$

if the latter number is finite. To this end, put

$$N = \bigcap_{g\in G} g^{-1} G_{(P:H)} g;$$

this is a normal subgroup of G which has finite index in G and is contained in $G_{(P:H)}$. Since $(P : H) = (P : G_{(P:H)})$, the foregoing yields embeddings of fields

$$\mathscr{C}(R)^G \hookrightarrow \mathscr{C}(S)^{G_{(P:H)}} = \mathscr{C}\big(R/(P : G_{(P:H)})\big)^{G_{(P:H)}} \hookrightarrow \mathscr{C}(R/(P : N))^{N'},$$

where $N' := G_{(P:H)} \cap G_{(P:N)}$. The image of $\mathscr{C}(R)^G$ under the composite embedding is contained in $\mathscr{C}(R/(P:N))^{G_{(P:N)}}$ and, by Galois theory,

$$\big[\mathscr{C}(R/(P:N))^{N'} : \mathscr{C}(R/(P:N))^{G_{(P:N)}}\big] \leq [G_{(P:N)} : N'] \leq [G : G_{(P:H)}].$$

It suffices to show that the image of $\mathscr{C}(R)^G$ is actually equal to $\mathscr{C}(R/(P:N))^{G_{(P:N)}}$. Therefore, replacing H by N, it suffices to show that

$$\text{If } H \trianglelefteq G \text{ and } [G : G_{(P:H)}] < \infty \text{ then } \mathscr{C}(R)^G \text{ maps onto } \mathscr{C}(S)^{G_{(P:H)}}. \tag{2-1}$$

To this end, we will prove the following:

Claim 11. *Let $t \in \mathscr{C}(S)^{G_{(P:H)}}$ be given. There exists a G-stable ideal I of R such that $0 \neq \varphi(I) \subseteq D_t$ and such that, for every $x \in I$, there exists an $x' \in R$ satisfying*

$$\varphi(g.x') = t\varphi(g.x) \quad \textit{for all } g \in G. \tag{2-2}$$

Note that G-stability of I and the condition $\varphi(I) \subseteq D_t$ ensure that $t\varphi(g.x) \in S$ holds for all $g \in G$, $x \in I$. Moreover, any G-stable ideal I satisfying $0 \neq \varphi(I)$ belongs to $\mathscr{C}(R)$. Indeed, $\operatorname{l.ann}_S \varphi(I) = 0$ since S is H-prime, and hence $\operatorname{l.ann}_R I$ is contained in $(P:G) = 0$. Finally, the element x' is uniquely determined by (2-2) for any given x, because, if $x'' \in R$ also satisfies (2-2) then $\varphi(g.x') = \varphi(g.x'')$ holds for all $g \in G$ and so $x' - x'' \in (P:G) = 0$. Therefore, assuming Claim 11 for now, we can define a map

$$f : I \to R\,, \quad x \mapsto x'.$$

It is easy to check that f is G-equivariant. Furthermore, for $r_1, r_2 \in R$,

$$\begin{aligned}\varphi(g.(r_1x'r_2)) &= \varphi(g.r_1)\varphi(g.x')\varphi(g.r_2) = \varphi(g.r_1)t\varphi(g.x)\varphi(g.r_2)\\ &= t\varphi(g.r_1)\varphi(g.x)\varphi(g.r_2) = t\varphi(g.(r_1xr_2)).\end{aligned}$$

This shows that f is (R, R)-bilinear. Hence, defining q to be the class of f, we obtain the desired element $q \in \mathscr{C}(R)^G$ mapping to our given $t \in \mathscr{C}(S)^{G_{(P:H)}}$, thereby proving (2-1).

It remains to construct I as in the claim. Put

$$D = \Bigg(\bigcap_{\substack{x,y \in G \\ x^{-1}y \notin G_{(P:H)}}} x.(P:H) + y.(P:H) \Bigg)^{[G:G_{(P:H)}]-1}.$$

Then D is a G-stable ideal of R satisfying $0 \neq \varphi(D)$. For the latter note that the finitely many ideals $x.(P:H) + y.(P:H)$ are H-stable, since H is normal, and none of them is contained in $(P:H)$. By the Chinese remainder theorem [Brown and Lorenz 1996, 1.3], the image of the map

$$\begin{tikzcd}
\mu : R \arrow[r, hook] & \prod_{g\in G/G_{(P:H)}} R/g.(P:H) \arrow[r, "\sim"] & \prod_{g\in G/G_{(P:H)}} S \\
r \arrow[u, phantom, sloped, "\in"] \arrow[r, mapsto] & (r+g.(P:H))_{g\in G/G_{(P:H)}} \arrow[u, phantom, sloped, "\in"] \arrow[r, mapsto] & \big(\varphi(g^{-1}.r)\big)_{g\in G/G_{(P:H)}} \arrow[u, phantom, sloped, "\in"]
\end{tikzcd}$$

contains the ideal $\prod_{g\in G/G_{(P:H)}} \varphi(D)$. Now put

$$I = \big(\varphi^{-1}(D_t) : G\big)\, D.$$

This is certainly a G-stable ideal of R satisfying $\varphi(I) \subseteq D_t$. Suppose that $\varphi(I) = 0$. Since $\varphi(D)$ is a nonzero H-stable ideal of the H-prime ring S, we must have

$$\big(\varphi^{-1}(D_t) : G\big) = \bigcap_{g\in G/G_{(P:H)}} g.\varphi^{-1}(D_t) \subseteq (P : H)$$

and so $g.\varphi^{-1}(D_t) \subseteq (P : H)$ for some $g \in G$. But then

$$g.\varphi^{-1}(D_t) \subsetneqq \varphi^{-1}(D_t)$$

which is impossible because $\varphi^{-1}(D_t)$ is $G_{(P:H)}$-stable and $G_{(P:H)}$ has finite index in G. Therefore, $\varphi(I) \neq 0$. Finally, if $x \in I$ then $\varphi(g.x) \in D_t\varphi(D)$ for all $g \in G$, and hence $t\varphi(g.x) \in \varphi(D)$. Therefore,

$$\big(t\varphi(g^{-1}.x)\big)_{g\in G/G_{(P:H)}} = \mu(x')$$

for some $x' \in R$, that is,

$$\varphi(g^{-1}.x') = \big(t\varphi(g^{-1}.x)\big)$$

holds for all $g \in G/G_{(P:H)}$. Since φ and t are $G_{(P:H)}$-invariant, it follows that

$$\varphi\big((gh)^{-1}.x'\big) = \big(t\varphi((gh)^{-1}.x)\big)$$

holds for all $g \in G/G_{(P:H)}$, $h \in G_{(P:H)}$. Therefore, $\varphi(g.x') = t\varphi(g.x)$ for all $g \in G$, as desired.

(b) This is just (2-1) with $H = 1$. □

2.4. *G-rational ideals.* Assume now that R is an algebra over some field $\Bbbk$, as in Section 1.7, and that G acts on R by $\Bbbk$-algebra automorphisms. A G-prime ideal I of R will be called *G-rational* if $\mathscr{C}(R/I)^G = \Bbbk$. One can check as in Section 1.2.1 that the notion of G-rationality is left-right symmetric.

Lemma 10 (a) with $H = 1$ immediately implies the following:

Proposition 12. *The map* Spec $R \to G$-Spec R, $P \mapsto (P : G)$, *in* Proposition 8 *restricts to a map* Rat $R \to G$-Rat R.

Unfortunately, the map $\operatorname{Rat} R \to G\text{-}\operatorname{Rat} R$ above need not be surjective, even when the G-action on R is locally ideal finite in the sense of Proposition 8 (b).

Example 13. Let $F \supset \Bbbk$ be any nonalgebraic field extension satisfying $F^G = \Bbbk$ for some subgroup G of $\operatorname{Gal}(F/\Bbbk)$. For example, F could be chosen to be the rational function field $\Bbbk(t)$ over an infinite field $\Bbbk$ and $G = \Bbbk^*$ acting via $\lambda.f(t) = f(\lambda^{-1}t)$ for $\lambda \in \Bbbk^*$. The G-action on F is clearly locally ideal finite and $\mathrm{Q_r}(F) = \mathscr{C}(F) = F$. Therefore, the zero ideal of F is G-rational, but F has no rational ideals.

2.5. *Algebras over a large algebraically closed base field.* We continue to assume that R is an algebra over some field $\Bbbk$ and that G acts on R by $\Bbbk$-algebra automorphisms. The following lemma is a version of [Mœglin and Rentschler 1981, Lemme 3.3].

Lemma 14. *Let $I \in \operatorname{Spec} R$ be given. Put $C = \mathscr{C}(R/I)$ and consider the natural map of C-algebras*

$$\psi\colon R_C = R \otimes_{\Bbbk} C \twoheadrightarrow (R/I) \otimes_{\Bbbk} C \twoheadrightarrow (R/I)C$$

where $(R/I)C \subseteq \mathrm{Q_r}(R/I)$ is the central closure of R/I. Then:

(a) *$\widetilde{I} = \operatorname{Ker} \psi$ is a C-rational ideal of R_C.*

(b) *If $I \in G\text{-}\operatorname{Rat} R$ then, letting G act on R_C by C-linear extension of the action on R, we have*
$$\big(\widetilde{I} : G\big) = I \otimes_{\Bbbk} C.$$

Proof. Part (a) is clear, since $R_C/\widetilde{I} \cong (R/I)C$ is C-rational; see Section 1.7.1.

For (b), note that the map ψ is G-equivariant for the diagonal G-action on $R_C = R \otimes_{\Bbbk} C$ and the usual G-action on $(R/I)C \subseteq \mathrm{Q_r}(R/I)$. Therefore, $\widetilde{I}$ is stable under all automorphisms $g \otimes g$ with $g \in G$, and hence we have

$$(g \otimes 1)\big(\widetilde{I}\big) = (1 \otimes g^{-1})\big(\widetilde{I}\big).$$

We conclude that

$$\big(\widetilde{I} : G\big) = \bigcap_{g \in G} (1 \otimes g)\big(\widetilde{I}\big) = I \otimes_{\Bbbk} C,$$

where the last equality uses the fact that $\widetilde{I} \cap R = I$ and our hypothesis $C^G = \Bbbk$; see [Bourbaki 1981, Corollary to Proposition V.10.6]. □

As an application of the lemma, we offer the following "quick and dirty" existence result for generic rational ideals.

Proposition 15. *Let R be a countably generated algebra over an algebraically closed base field $\Bbbk$ of infinite transcendence degree over its prime subfield and assume that the group G is countably generated. Then every prime ideal $I \in G\text{-}\operatorname{Rat} R$ has the form $I = (P : G)$ for some $P \in \operatorname{Rat} R$.*

Proof. Let a prime $I \in G\text{-Rat}\, R$ be given and let $\Bbbk_0$ denote the prime subfield of $\Bbbk$. By hypothesis on R, we have

$$\dim_{\Bbbk} R \leq \aleph_0.$$

Choosing a $\Bbbk$-basis $\mathcal{B}$ of R which contains a $\Bbbk$-basis for I and adjoining the structure constants of R with respect to $\mathcal{B}$ to $\Bbbk_0$, we obtain a countable field K with $\Bbbk_0 \subseteq K \subseteq \Bbbk$. Putting $R_0 = \sum_{b \in \mathcal{B}} Kb$ we obtain a K-subalgebra of R such that $R = R_0 \otimes_K \Bbbk$ and $I = I_0 \otimes_K \Bbbk$, where $I_0 = I \cap R_0$. At the cost of adjoining at most countably many further elements to K, we can also make sure that R_0 is stable under the action of G. Thus, R_0/I_0 is a G-stable K-subalgebra of R/I and $R/I = (R_0/I_0) \otimes_K \Bbbk$. Put $C = \mathscr{C}(R_0/I_0)$ and note that (1-2) implies that $C^G = K$, because $\mathscr{C}(R/I)^G = \Bbbk$. Thus, $I_0 \in G\text{-Rat}\, R_0$ and Lemma 14 yields an ideal

$$\widetilde{I_0} \in \text{Rat}(R_0 \otimes_K C)$$

such that

$$\big(\widetilde{I_0} : G\big) = I_0 \otimes_K C.$$

Furthermore, since R_0/I_0 is countable, the field C is countable as well; this follows from Proposition 2. By hypothesis on $\Bbbk$, there is a $\Bbbk_0$-embedding of C into $\Bbbk$; see [Bourbaki 1981, Corollary 1 to Théorème V.14.5]. Finally, Lemma 7 implies that $P = \widetilde{I_0} \otimes_C \Bbbk$ is a rational ideal of $(R_0 \otimes_K C) \otimes_C \Bbbk = R$ satisfying

$$(P : G) = (I_0 \otimes_K C) \otimes_C \Bbbk = I,$$

as desired. □

3. Rational actions of algebraic groups

In this section, we work over an algebraically closed base field $\Bbbk$. Throughout, the group G will be an affine algebraic group over $\Bbbk$ and R will be a $\Bbbk$-algebra on which G acts by $\Bbbk$-algebra automorphisms. The Hopf algebra of regular functions on G will be denoted by $\Bbbk[G]$. The notations introduced in Section 2 remain in effect. In addition, $\otimes$ will stand for $\otimes_{\Bbbk}$.

3.1. ***G-modules.*** A $\Bbbk$-vector space M is called a *G-module* if there is a linear representation

$$\rho_M : G \longrightarrow \text{GL}(M)$$

satisfying

(a) local finiteness, that is, all G-orbits in M generate finite-dimensional subspaces of M, and

(b) for every finite-dimensional G-stable subspace $V \subseteq M$, the induced group homomorphism $G \to \text{GL}(V)$ is a homomorphism of algebraic groups.

As is well-known, these requirements are equivalent to the existence of a $\Bbbk$-linear map

$$\Delta_M\colon M \longrightarrow M \otimes \Bbbk[G] \tag{3-1}$$

which makes M into a $\Bbbk[G]$-comodule; see [Jantzen 2003, 2.7–2.8] or [Waterhouse 1979, 3.1–3.2] for details. We will use the Sweedler notation

$$\Delta_M(m) = \sum m_0 \otimes m_1 \qquad (m \in M)$$

as in [Montgomery 1993]. Writing $\rho_M(g)(m) = g.m$, we have

$$g.m = \sum m_0 m_1(g) \qquad (g \in G, m \in M). \tag{3-2}$$

Linear representations ρ_M as above are often called *rational*. Tensor products of rational representations of G are again rational, and similarly for sums, subrepresentations and homomorphic images of rational representations.

Example 16. If the group G is finite then G-modules are the same as (left) modules M over the group algebra $\Bbbk G$ and all linear representations of G are rational. Indeed, in this case, $\Bbbk[G]$ is the linear dual of $\Bbbk G$, that is, the $\Bbbk$-vector space of all functions $G \to \Bbbk$ with pointwise addition and multiplication. The map $\Delta_M\colon M \to M \otimes \Bbbk[G]$ is given by

$$\Delta_M(m) = \sum_{x \in G} x.m \otimes p_x,$$

where $p_x \in \Bbbk[G] = (\Bbbk G)^*$ is defined by $p_x(y) = \delta_{x,y}$ (Kronecker delta) for $x, y \in G$.

3.2. ***Some properties of G-modules.*** Let M be a G-module. The coaction Δ_M in (3-1) is injective. In fact, extending Δ_M to a map

$$\Delta_M\colon M \otimes \Bbbk[G] \longrightarrow M \otimes \Bbbk[G] \tag{3-3}$$

by $\Bbbk[G]$-linearity, we obtain an *automorphism* of $M \otimes \Bbbk[G]$: the inverse of Δ_M is the $\Bbbk[G]$-linear extension of the map $(\mathrm{Id}_M \otimes S) \circ \Delta_M\colon M \longrightarrow M \otimes \Bbbk[G]$, where $S\colon \Bbbk[G] \to \Bbbk[G]$ is the antipode of $\Bbbk[G]$: $(Sf)(g) = f(g^{-1})$ for $g \in G$.

Furthermore, G-stable cores can be computed with Δ_M as follows.

Lemma 17. *For any $\Bbbk$-subspace V of M, we have*

$$(V : G) = \Delta_M^{-1}(V \otimes \Bbbk[G]).$$

Proof. Fix a $\Bbbk$-basis $\{v_i\}$ of V and let $\{w_j\}$ be a $\Bbbk$-basis for a complement of V in M. For $m \in M$, we have

$$\Delta_M(m) = \sum_i v_i \otimes f_i + \sum_j w_j \otimes h_j$$

with uniquely determined $f_i, h_j \in \Bbbk[G]$. Moreover,

$$\begin{aligned}\Delta_M(m) \in V \otimes \Bbbk[G] &\iff \text{all the } h_j \text{ vanish}\\ &\iff g.m = \sum_i v_i f_i(g) \in V \ \text{ for all } g \in G.\end{aligned}$$

This proves the lemma. □

3.3. ***Regular representations and intertwining formulas.*** The right and left *regular representations* of G are defined by

$$\begin{aligned}\rho_r \colon G &\longrightarrow \mathrm{GL}(\Bbbk[G]), \quad (\rho_r(x)f)(y) = f(yx),\\ \rho_\ell \colon G &\longrightarrow \mathrm{GL}(\Bbbk[G]), \quad (\rho_\ell(x)f)(y) = f(x^{-1}y),\end{aligned}$$

for $x, y \in G$. Both regular representations are rational. The right regular representation comes from the comultiplication $\Delta \colon \Bbbk[G] \to \Bbbk[G] \otimes \Bbbk[G]$ of the Hopf algebra $\Bbbk[G]$; in the usual Sweedler notation, it is given by $\Delta f = \sum f_1 \otimes f_2$, where $f(xy) = \sum f_1(x) f_2(y)$ for $x, y \in G$. Similarly, the left regular representation comes from $(S \otimes \mathrm{Id}_{\Bbbk[G]}) \circ \Delta \circ S \colon \Bbbk[G] \to \Bbbk[G] \otimes \Bbbk[G]$.

Now let M be a G-module. Then the rational representations

$$1_M \otimes \rho_\ell \colon G \to \mathrm{GL}(M \otimes \Bbbk[G]) \text{ and } \rho_M \otimes \rho_\ell \colon G \to \mathrm{GL}(M \otimes \Bbbk[G])$$

are intertwined by the automorphism Δ_M of (3-3): for all $g \in G$, we have

$$\Delta_M \circ (1_M \otimes \rho_\ell)(g) = (\rho_M \otimes \rho_\ell)(g) \circ \Delta_M. \tag{3-4}$$

Similarly,

$$\Delta_M \circ (\rho_M \otimes \rho_r)(g) = (1_M \otimes \rho_r)(g) \circ \Delta_M. \tag{3-5}$$

To prove (3-5), for example, one checks that both sides of the equation send $m \otimes f \in M \otimes \Bbbk[G]$ to the function $G \to M$, $x \mapsto xg.mf(xg)$.

3.4. ***Rational group actions.*** The action of G on the $\Bbbk$-algebra R is said to be *rational* if it makes R a G-module in the sense above. The map

$$\Delta_R \colon R \to R \otimes \Bbbk[G]$$

is then a map of $\Bbbk$-algebras; equivalently, R is a right $\Bbbk[G]$-comodule algebra. Since rational actions are locally finite, they are certainly locally ideal finite in the sense of Proposition 8 (b). Therefore, the G-primes of R are exactly the ideals of R of the form $(P : G)$ for $P \in \operatorname{Spec} R$. In particular, G-prime ideals of R are semiprime; for a more precise statement, see Corollary 21 below. Moreover, the $\Bbbk[G]$-linear extension of Δ_R is an automorphism of $\Bbbk[G]$-algebras

$$\Delta_R \colon R \otimes \Bbbk[G] \xrightarrow{\sim} R \otimes \Bbbk[G]. \tag{3-6}$$

We now consider the extended G-action on the Amitsur–Martindale ring of quotients $\mathrm{Q_r}(R)$; see Section 2.3. This action is usually not rational, even if G acts rationally on R. Part (b) of the following lemma, for classical quotient rings of semiprime Goldie rings, is due to Mœglin and Rentschler [1986b, I.22].

Lemma 18. *Assume that G acts rationally on R. Then*:

(a) *The centralizer*

$$C_G(T) = \{\, g \in G \mid g.q = q \text{ for all } q \in T \,\}$$

of every subset $T \subseteq \mathrm{Q_r}(R)$ is a closed subgroup of G.

(b) *Let $V \subseteq \mathrm{Q_r}(R)$ be a G-stable* $\Bbbk$*-subspace of* $\mathrm{Q_r}(R)$. *The G-action on V is rational if and only if it is locally finite.*

Proof. (a) In view of Proposition 2(iii), the condition for an element $g \in G$ to belong to $C_G(T)$ can be stated as

$$\forall q \in T, r \in D_q : (q - g.q)g.r = 0,$$

where D_q is as in (1-1). Using the notation of (3-2), we have

$$(q - g.q)g.r = q(g.r) - g.(qr) = \sum qr_0 r_1(g) - \sum (qr)_0 (qr)_1(g).$$

Thus, putting

$$f_{r,q} = \sum qr_0 \otimes r_1 - \sum (qr)_0 \otimes (qr)_1 \in \mathrm{Q_r}(R) \otimes \Bbbk[G],$$

we see that $g \in C_G(T)$ if and only if $f_{r,q}(g) = 0$ holds for all $q \in T$ and all $r \in D_q$. Since each equation $f_{r,q}(g) = 0$ defines a closed subset of G, part (a) follows.

(b) Necessity is clear. So assume that the G-action on V is locally finite. Put $S = R \otimes \Bbbk[G]$ and consider the $\Bbbk[G]$-algebra automorphism $\Delta_R \in \mathrm{Aut}(S)$ as in (3-6) and its extension $\Delta \in \mathrm{Aut}(\mathrm{Q_r}(S))$. We must show that, under the canonical embedding $\mathrm{Q_r}(R) \hookrightarrow \mathrm{Q_r}(S)$ as in Section 1.8, we have

$$\Delta(V) \subseteq V \otimes \Bbbk[G]. \tag{3-7}$$

Since the action of G on V is locally finite, we may assume that V is finite-dimensional. Therefore, the ideal

$$D_V = \bigcap_{q \in V} D_q$$

belongs to $\mathscr{E}(R)$ and D_V is G-stable, since V is. Lemma 17 implies that

$$\Delta(D_V \otimes \Bbbk[G]) = D_V \otimes \Bbbk[G],$$

and hence

$$\Delta(V)(D_V \otimes \Bbbk[G]) = \Delta(V(D_V \otimes \Bbbk[G])) \subseteq S.$$

This shows that the subspace $\Delta(V) \subseteq \mathrm{Q_r}(S)$ actually is contained in $\mathrm{Q_r}(R) \otimes \Bbbk[G]$, and (3-7) follows from Lemma 17, since $V = (V : G)$. □

From now on, the G-action on R is understood to be rational.

3.5. ***Connected groups.*** The group G is *connected* if and only if the algebra $\Bbbk[G]$ is a domain. In this case,

$$\Bbbk(G) = \operatorname{Fract} \Bbbk[G]$$

will denote the field of rational functions on G. The group G acts on $\Bbbk(G)$ by the natural extensions of the right and left regular actions ρ_r and ρ_ℓ on $\Bbbk[G]$; see Section 3.3.

Part (a) of the following result is due to Chin [1992, Corollary 1.3]; the proof given below has been extracted from [Vonessen 1998, 3.6]. The proof of part (c) follows the outline of the arguments in [Mœglin and Rentschler 1986b, I.29, 2^e étape].

Proposition 19. *Assume that G is connected. Then*:

(a) $(P : G)$ *is prime for every* $P \in \operatorname{Spec} R$. *Therefore, the G-primes of R are exactly the G-stable primes of R.*

(b) *Assume that R is prime and every nonzero ideal I of R satisfies* $(I : G) \neq 0$. *Then G acts trivially on* $\mathscr{C}(R)$.

(c) *If R is G-rational then the field extension* $\mathscr{C}(R)/\Bbbk$ *is finitely generated. In fact, there is a G-equivariant* $\Bbbk$*-embedding of fields* $\mathscr{C}(R) \hookrightarrow \Bbbk(G)$, *with G acting on* $\Bbbk(G)$ *via the right regular representation* ρ_r.

Proof. (a) It suffices to show that $(P : G)$ is prime for each prime P; the last assertion is then a consequence of Proposition 8.

By Section 3.4, we know that the homomorphism $\Delta_R \colon R \to R \otimes \Bbbk[G]$ is centralizing. Therefore, there is a map

$$\operatorname{Spec}(R \otimes \Bbbk[G]) \to \operatorname{Spec} R, \quad Q \mapsto \Delta_R^{-1}(Q).$$

In view of Lemma 17, it therefore suffices to show that $P \otimes \Bbbk[G]$ is prime whenever P is. But the algebra $\Bbbk[G]$ is contained in some finitely generated purely transcendental field extension F of $\Bbbk$; see [Borel 1991, 18.2]. Thus, we have a centralizing extension of algebras

$$(R/P) \otimes \Bbbk[G] \subseteq (R/P) \otimes F.$$

Since $(R/P) \otimes F$ is clearly prime, $(R/P) \otimes \Bbbk[G]$ is prime as well as desired.

(b) We first prove the following special case of (b) which is well-known; see [Vonessen 1993, Prop. A.1].

Claim 20. *If R is a field then G acts trivially on R.*

Since G is the union of its Borel subgroups [Borel 1991, 11.10], we may assume that G is solvable. Arguing by induction on a composition series of G [Borel 1991, 15.1], we may further assume that G is the additive group $\mathbb{G}_{\mathrm{a}}$ or the multiplicative group $\mathbb{G}_{\mathrm{m}}$. Therefore, $R \otimes \Bbbk[G]$ is a polynomial algebra or a Laurent polynomial algebra over R. In either case, R is the unique largest subfield of $R\otimes\Bbbk[G]$, because $R \otimes \Bbbk[G]$ has only "trivial" units: the nonzero elements of R if $R \otimes \Bbbk[G] = R[t]$, and the elements of the form rt^m with $0 \neq r \in R$ and $m \in \mathbb{Z}$ if $R \otimes \Bbbk[G] = R[t^{\pm 1}]$. Consequently, the map $\Delta_R \colon R \to R \otimes \Bbbk[G]$ has image in $R \otimes 1$ which in turn says that G acts trivially on R. This proves Claim 20.

Now let R be a prime $\Bbbk$-algebra such that $(I : G)$ is nonzero for every nonzero ideal I of R. By Claim 20, it suffices to show that the G-action on $\mathscr{C}(R)$ is rational, and by Lemma 18 this amounts to showing that G-action on $\mathscr{C}(R)$ is locally finite. So let $q \in \mathscr{C}(R)$ be given and consider the ideal D_q of R as in (1-1). By hypothesis, we may pick a nonzero element $d \in (D_q : G)$. The G-orbit $G.d$ generates a finite-dimensional $\Bbbk$-subspace $V \subseteq D_q$. Moreover, qV is contained in a finite-dimensional G-stable subspace $W \subseteq R$. Therefore, for all $g, h \in G$, we have

$$(g.q)(h.d) = g.(q(g^{-1}h.d)) \in W,$$

and hence $QV \subseteq W$, where $Q \subseteq \mathscr{C}(R)$ denotes the $\Bbbk$-subspace that is generated by the orbit $G.q$. Thus, multiplication gives a linear map $Q \to \mathrm{Hom}_{\Bbbk}(V, W)$ which is injective, because $V \neq 0$ and nonzero elements of $\mathscr{C}(R)$ have zero annihilator in R. This shows that Q is finite-dimensional as desired.

(c) Put $C = \mathscr{C}(R)$ and $K = \Bbbk(G)$, the field of rational functions on G, that is, the field of fractions of the algebra $\Bbbk[G]$. The algebra $R_K = R \otimes K$ is prime by (a) and its proof, and by (1-2) there is a tower of fields

$$C \hookrightarrow \mathrm{Fract}(C \otimes K) \hookrightarrow \mathscr{C}(R_K).$$

We will first show that C is a finitely generated field extension of $\Bbbk$. Since $K/\Bbbk$ is finitely generated, the field $\mathrm{Fract}(C \otimes K)$ is certainly finitely generated over C. Thus, it will suffice to construct a C-algebra embedding $C \otimes C \hookrightarrow \mathrm{Fract}(C \otimes K)$.

To construct such an embedding, consider the natural epimorphism of $\mathscr{C}(R_K)$-algebras $RC \otimes_C \mathscr{C}(R_K) \twoheadrightarrow R_K\mathscr{C}(R_K)$. By Lemma 3(b), this map is injective, because it is clearly injective on RC. Thus,

$$RC \otimes_C \mathscr{C}(R_K) \xrightarrow{\sim} R_K\mathscr{C}(R_K). \tag{3-8}$$

Let δ be the K-algebra automorphism of R_K that is defined by K-linear extension of the G-coaction $\Delta_R \colon R \otimes \Bbbk[G] \xrightarrow{\sim} R \otimes \Bbbk[G]$ in (3-6):

$$\delta = \Delta_R \otimes_{\Bbbk[G]} \mathrm{Id}_K \colon R_K \xrightarrow{\sim} R_K. \tag{3-9}$$

Let $\widetilde{\delta}$ be the unique extension of δ to an automorphism of the central closure $R_K\mathscr{C}(R_K)$ of R_K. Clearly, $\widetilde{\delta}$ sends the $\mathscr{C}(R_K) = \mathscr{Z}(R_K\mathscr{C}(R_K))$ to itself. We claim that

$$\widetilde{\delta}(C) \subseteq \operatorname{Fract}(C \otimes K) \; ; \tag{3-10}$$

so $\widetilde{\delta}$ also sends $\operatorname{Fract}(C \otimes K)$ to itself. In order to see this, pick $q \in C$ and $d \in D_q$. Then

$$\widetilde{\delta}(q)\,\Delta_R(d) = \widetilde{\delta}(q)\widetilde{\delta}(d) = \widetilde{\delta}(qd) = \Delta_R(qd)$$

holds in $R_K\mathscr{C}(R_K)$. Here, both $\Delta_R(qd)$ and $\Delta_R(d)$ belong to

$$R_K \subseteq RC \otimes_C (C \otimes K).$$

Fixing a C-basis B for RC and writing

$$\Delta_R(qd) = \sum_{b \in B} bx_b, \quad \Delta_R(d) = \sum_{b \in B} by_b,$$

with $x_b, y_b \in C \otimes K$, the equation above becomes

$$\sum_{b \in B} b\widetilde{\delta}(q)y_b = \sum_{b \in B} bx_b.$$

Now (3-8) yields $\widetilde{\delta}(q)y_b = x_b$ for all b, which proves (3-10). For the desired embedding, consider the C-algebra map

$$\mu\colon C \otimes C \longrightarrow \operatorname{Fract}(C \otimes K)\,, \quad c \otimes c' \mapsto c\widetilde{\delta}(c'). \tag{3-11}$$

We wish to show that μ is injective. To this end, note that the G-action ρ_R on R extends uniquely to an action ρ_{RC} on the central closure RC, and the G-action $1_R \otimes \rho_r$ on R_K extends uniquely to the central closure $R_K\mathscr{C}(R_K)$. Denoting the latter action by $\widetilde{\rho_r}$, the intertwining formula (3-5) implies that

$$\widetilde{\delta} \circ \rho_{RC}(g) = \widetilde{\rho_r}(g) \circ \widetilde{\delta}\colon\, RC \to R_K\mathscr{C}(R_K)$$

for all $g \in G$. This yields

$$\mu \circ (\operatorname{Id}_C \otimes \rho_C(g)) = \widetilde{\rho_r}(g) \circ \mu \tag{3-12}$$

for all $g \in G$. Thus, the ideal $\operatorname{Ker}\mu$ of $C \otimes C$ is stable under $(1_C \otimes \rho_C)(G)$. Finally, since $C^G = \Bbbk$, we may invoke [Bourbaki 1981, Corollary to Proposition V.10.6] to conclude that $\operatorname{Ker}\mu$ is generated by its intersection with $C \otimes 1$, which is zero. This shows that μ is injective, and hence the field extension $C/\Bbbk$ is finitely generated.

It remains to construct a G-equivariant embedding $C \hookrightarrow K$, with G acting on $\Bbbk(G)$ via the right regular representation ρ_r as above. For this, we specialize (3-11) as follows. Write $C = \operatorname{Fract} A$ for some affine $\Bbbk$-subalgebra $A \subseteq C$. Then

$$\operatorname{Fract}(C \otimes K) = \operatorname{Fract}(A \otimes \Bbbk[G]),$$

and hence

$$\mu(A \otimes A) \subseteq (A \otimes \Bbbk[G])[s^{-1}]$$

for some $0 \neq s \in A \otimes \Bbbk[G]$. By generic flatness [Dixmier 1996, 2.6.3], there further exists $0 \neq f \in A \otimes A$ so that $(A \otimes \Bbbk[G])[\mu(f)^{-1}s^{-1}]$ is free over $(A \otimes A)[f^{-1}]$ via μ. Now choose some maximal ideal $\mathfrak{m}$ of A with $f \notin \mathfrak{m} \otimes A$. Let $\overline{f}$ denote the image of f in $(A \otimes A)/(\mathfrak{m} \otimes A) \cong A$, and let $\bar{s}$ denote the image of s in $(A \otimes \Bbbk[G])/(\mathfrak{m} \otimes \Bbbk[G]) \cong \Bbbk[G]$. Since $\mu(\mathfrak{m} \otimes A) = \mathfrak{m}\mu(A \otimes A)$, the map $\mu|_{A \otimes A}$ passes down to a map

$$\bar{\mu}\colon A\big[\overline{f}^{-1}\big] \longrightarrow B := \Bbbk[G]\big[\bar{\mu}(\overline{f})^{-1}\bar{s}^{-1}\big]$$

making B a free $A\big[\overline{f}^{-1}\big]$-module. Consequently, $\bar{\mu}$ extends uniquely to an embedding of the fields of fractions,

$$\operatorname{Fract} A\big[\overline{f}^{-1}\big] = C \hookrightarrow \operatorname{Fract} B = K.$$

Finally, (3-12) implies that this embedding is G-equivariant, which completes the proof of (c). □

Returning to the case of a general affine algebraic group G, we have:

Corollary 21. *Every $I \in G$-$\operatorname{Spec} R$ has the form $I = (Q : G)$ for some $Q \in \operatorname{Spec} R$ with $[G : G_Q] < \infty$. Moreover, $\mathscr{C}(I)^G \cong \mathscr{C}(Q)^{G_Q}$.*

Proof. We know that $I = (P : G)$ for some $P \in \operatorname{Spec} R$; see Section 3.4. Let G^0 be the connected component of the identity in G; this is a connected normal subgroup of finite index in G [Borel 1991, 1.2]. Put $Q = (P : G^0)$. Then Proposition 19(a) tells us that Q is prime. Furthermore, $I = (Q : G)$ and $G^0 \subseteq G_Q$; so $[G : G_Q] < \infty$. The isomorphism $\mathscr{C}(I)^G \cong \mathscr{C}(Q)^{G_Q}$ follows from Lemma 10(b). □

3.6. *The fibres of the map* (0-2). Assume that G is connected. Our next goal is to give a description of the fibres of the map $\operatorname{Rat} R \to G$-$\operatorname{Rat} R$, $P \mapsto (P : G)$ in Proposition 12. Following [Brown and Goodearl 2002] we denote the fibre over a given $I \in G$-$\operatorname{Rat} R$ by $\operatorname{Rat}_I R$:

$$\operatorname{Rat}_I R = \{P \in \operatorname{Rat} R \mid (P : G) = I\}.$$

The group G acts on $\operatorname{Rat}_I R$ via the given action ρ_R on R.

Recall that the group G acts on the rational function field $\Bbbk(G)$ by the natural extensions of the regular representations ρ_r and ρ_ℓ. We denote by

$$\operatorname{Hom}_G(\mathscr{C}(R/I), \Bbbk(G))$$

the collection of all G-equivariant $\Bbbk$-algebra homomorphisms $\mathscr{C}(R/I) \to \Bbbk(G)$ with G acting on $\Bbbk(G)$ via the right regular action ρ_r. The left regular action ρ_ℓ of G on $\Bbbk(G)$ yields a G-action on the set $\operatorname{Hom}_G(\mathscr{C}(R/I), \Bbbk(G))$.

Theorem 22. *Let $I \in G$-$\operatorname{Rat} R$ be given. There is a G-equivariant bijection*

$$\operatorname{Rat}_I R \longrightarrow \operatorname{Hom}_G(\mathscr{C}(R/I), \Bbbk(G)).$$

Proof. Replacing R by R/I, we may assume that $I = 0$. In particular, R is prime by Proposition 19. We will also put $C = \mathscr{C}(R)$ and $K = \Bbbk(G)$ for brevity. For every $P \in \operatorname{Rat} R$ with $(P : G) = 0$, we will construct an embedding of fields

$$\psi_P : C \hookrightarrow K$$

such that the following hold:

(a) $\psi_P(g.c) = \rho_r(g)(\psi_P(c))$ and $\psi_{g.P} = \rho_\ell(g) \circ \psi_P$ holds for all $g \in G$, $c \in C$;

(b) if $P, Q \in \operatorname{Rat} R$ are such that $(Q : G) = (P : G) = 0$ but $Q \neq P$ then $\psi_Q \neq \psi_P$;

(c) given a G-equivariant embedding $\psi : C \hookrightarrow K$, with G acting on K via ρ_r, we have $\psi = \psi_P$ for some $P \in \operatorname{Rat} R$ with $(P : G) = 0$.

This will prove the theorem.

In order to construct ψ_P, consider the K-algebra $(R/P)_K = (R/P) \otimes K$. This algebra is rational by Lemma 7. We have a centralizing $\Bbbk$-algebra homomorphism

$$\varphi_P : R \xrightarrow{\Delta_R} R \otimes \Bbbk[G] \xrightarrow{\text{can.}} (R/P)_K, \tag{3-13}$$

where the canonical map

$$R \otimes \Bbbk[G] \to (R/P)_K$$

comes from the embedding $\Bbbk[G] \hookrightarrow K$ and the epimorphism $R \twoheadrightarrow R/P$. Since $(P : G) = 0$, Lemma 17 implies that φ_P is injective. Since $(R/P)_K$ is prime, it follows that $\mathscr{C}_{\varphi_P} = C$ holds in Lemma 4. Hence φ_P extends uniquely to a centralizing $\Bbbk$-algebra monomorphism

$$\widetilde{\varphi}_P : RC \hookrightarrow (R/P)_K \mathscr{C}((R/P)_K) = (R/P)_K \tag{3-14}$$

sending C to $\mathscr{C}((R/P)_K) = K$. Thus we may define $\psi_P := \widetilde{\varphi}_P|_C : C \hookrightarrow K$. It remains to verify properties (a)–(c).

Part (a) is a consequence of the intertwining formulas (3-4) and (3-5). Indeed, (3-5) implies that $\varphi_P(g.r) = \rho_r(g)(\varphi_P(r))$ holds for all $g \in G$ and $r \in R$. In view of Proposition 2(ii), this identity is in fact valid for $\widetilde{\varphi}_P$ and all $r \in RC$, which proves the first of the asserted formulas for ψ_P in (a). For the second formula, consider the map $(\varphi_P)_K$ that is defined by K-linear extension of (3-13) to $R_K = R \otimes K$; this is the composite

$$(\varphi_P)_K : R_K \xrightarrow{\delta} R_K \overset{\text{can.}}{\twoheadrightarrow} (R/P)_K, \tag{3-15}$$

where δ is as in (3-9). The map $(\rho_R \otimes \rho_\ell)(g)$ gives ring isomorphisms $R_K \xrightarrow{\sim} R_K$ and $(R/P)_K \xrightarrow{\sim} (R/g.P)_K$ such that the following diagram

$$\begin{tikzcd} R_K \arrow[r, "\sim"] \arrow[d, "\text{can.}"'] & R_K \arrow[d, "\text{can.}"] \\ (R/P)_K \arrow[r, "\sim"] & (R/g.P)_K \end{tikzcd}$$

commutes. The intertwining formula (3-4) implies that, for all $g \in G$,

$$(\varphi_{g.P})_K \circ (1_R \otimes \rho_\ell)(g) = (\rho_R \otimes \rho_\ell)(g) \circ (\varphi_P)_K.$$

Restricting to R we obtain

$$\varphi_{g.P} = (\rho_R \otimes \rho_\ell)(g) \circ \varphi_P,$$

and this becomes $\psi_{g.P} = \rho_\ell(g) \circ \psi_P$ on C. This finishes the proof of (a).

For (b), let

$$(\widetilde{\varphi}_P)_K \colon (RC)_K = RC \otimes K \twoheadrightarrow (R/P)_K$$

be defined by K-linear extension of (3-14) and put $\widetilde{P} = \operatorname{Ker}(\widetilde{\varphi}_P)_K$. Let $Q \in \operatorname{Rat} R$ be given such that $(Q : G) = 0$ and let $\widetilde{Q} = \operatorname{Ker}(\widetilde{\varphi}_Q)_K$ be defined analogously. If $Q \neq P$ then $\widetilde{Q}$ and $\widetilde{P}$ are distinct primes of $(RC)_K$; in fact,

$$\widetilde{Q} \cap R_K \neq \widetilde{P} \cap R_K,$$

because the restriction of $(\widetilde{\varphi}_P)_K$ to R_K is given by (3-15). Since both $\widetilde{Q}$ and $\widetilde{P}$ are disjoint from RC, Lemma 3(c) gives $\widetilde{P} \cap C_K \neq \widetilde{Q} \cap C_K$. This shows that $(\psi_P)_K$ and $(\psi_Q)_K$ have distinct kernels, and so $\psi_P \neq \psi_Q$ proving (b).

Finally, for (c), let $\psi \colon C \hookrightarrow K$ be some G-equivariant embedding. Define a K-algebra map

$$\Psi \colon R_K \longrightarrow S = RC \otimes_C K$$

by K-linear extension of the canonical embedding $R \hookrightarrow RC$. Note that, for $c \in C$,

$$c \otimes 1 = 1 \otimes \psi(c) \tag{3-16}$$

holds in S. Put

$$P = \delta(\operatorname{Ker} \Psi) \cap R,$$

with δ as in (3-9). We will show that P is the desired rational ideal.

The algebra S is K-rational, by Lemma 7, and G acts on S via $\rho_{RC} \otimes_C \rho_r$, where ρ_{RC} is the unique extension of the G-action ρ_R from R to the central closure RC. The map Ψ is G-equivariant for this action and the diagonal G-action $\rho_R \otimes \rho_r$ on R_K. Furthermore, by (3-5), the automorphism

$$\delta^{-1} \colon R_K \xrightarrow{\sim} R_K$$

is equivariant with respect to the G-actions $1_R \otimes \rho_r$ on the first copy of R_K and $\rho_R \otimes \rho_r$ on the second R_K. Therefore, the composite $\Psi \circ \delta^{-1} \colon R_K \to S$ is equivariant for the G-actions $1_R \otimes \rho_r$ on R_K and $\rho_{RC} \otimes_C \rho_r$ on S. Now consider the centralizing monomorphism of $\Bbbk$-algebras

$$\mu \colon R/P \hookrightarrow R_K/\delta(\operatorname{Ker}\Psi) \xrightarrow[\delta^{-1}]{\sim} R_K/\operatorname{Ker}\Psi \underset{\Psi}{\hookrightarrow} S.$$

By the foregoing, we have $\mu(R/P) \subseteq S^G$, the $\Bbbk$-subalgebra of G-invariants in S. Since S is prime, we have $\mathscr{C}_\mu = \mathscr{C}(R/P)$ in Lemma 4. Hence, μ extends uniquely to a monomorphism $\widetilde{\mu} \colon R/P\mathscr{C}(R/P) \hookrightarrow S\mathscr{C}(S) = S$ sending $\mathscr{C}(R/P)$ to $\mathscr{C}(S) = K$. Therefore, $\widetilde{\mu}(\mathscr{C}(R/P)) \subseteq K^G = \Bbbk$, which proves that P is rational. Furthermore, by Lemma 17, we have

$$(P : G) = \Delta_R^{-1}(P \otimes \Bbbk[G]) \subseteq \delta^{-1}(\delta(\operatorname{Ker}\Psi)) = \operatorname{Ker}\Psi.$$

Since Ψ is mono on R, we conclude that $(P : G) = 0$. It remains to show that $\psi = \psi_P$. For this, consider the map $\widetilde{\varphi}_P$ of (3-14); so $\psi_P = \widetilde{\varphi}_P|_C$. For $q \in C$, $d \in D_q$ we have

$$\delta(qd) \bmod P \otimes K = \widetilde{\varphi}_P(qd) = \widetilde{\varphi}_P(q)\widetilde{\varphi}_P(d) = \delta(\psi_P(q)d) \bmod P \otimes K$$

because $\psi_P(q) \in K$ and δ is K-linear. It follows that $\psi_P(q)d - qd \in \operatorname{Ker}\Psi$; so

$$0 = \psi_P(q)\Psi(d) - \Psi(qd) = qd \otimes_C 1 = \psi(q)\Psi(d),$$

where the last equality holds by (3-16). This shows that $\psi_P(q) = \psi(q)$, thereby completing the proof of the theorem. □

3.7. ***Proof of Theorem 1.*** We have to prove

(1) given $I \in G\text{-}\operatorname{Rat} R$, there is a $P \in \operatorname{Rat} R$ such that $I = (P : G)$;

(2) if $P, P' \in \operatorname{Rat} R$ satisfy $(P : G) = (P' : G)$ then $P' = g.P$ for some $g \in G$.

3.7.1. We first show that it suffices to deal with the case of connected groups. Let G^0 denote the connected component of the identity in G, as before, and assume that both (1) and (2) hold for G^0.

In order to prove (1) for G, let $I \in G\text{-}\operatorname{Rat} R$ be given. By Corollary 21, there exists $Q \in \operatorname{Spec} R$ with $I = (Q : G)$, $G^0 \subseteq G_Q$ and $\mathscr{C}(R/Q)^{G_Q} = \Bbbk$. Since G_Q/G^0 is finite, it follows that Q is in fact G^0-rational. Inasmuch as (1) holds for G^0, there exists $P \in \operatorname{Rat} R$ with $Q = (P : G^0)$. It follows that $(P : G) = (Q : G) = I$, proving (1).

Now suppose that $(P : G) = (P' : G)$ for $P, P' \in \operatorname{Rat} R$. Putting $P^0 = (P : G^0)$ we have

$$(P : G) = \bigcap_{x \in G/G^0} x.P^0 = \bigcap_{x \in G/G^0} (x.P : G^0),$$

a finite intersection of G^0-prime ideals of R. Similarly for $P'^0 = (P' : G^0)$. The equality $(P : G) = (P' : G)$ implies that $(P' : G^0) = (x.P : G^0)$ for some $x \in G$. (Note that if $V \subseteq g.V$ holds for some $\Bbbk$-subspace $V \subseteq R$ and some $g \in G$ then we must have $V = g.V$, because the G-action on R is locally finite.) Invoking (2) for G^0, we see that $P' = yx.P$ for some $y \in G^0$, which proves (2) for G.

3.7.2. Now assume that G is connected. In view of Theorem 22, proving (1) amounts to showing that there is a G-equivariant $\Bbbk$-algebra homomorphism

$$\mathscr{C}(R/I) \to \Bbbk(G)$$

with G acting on $\Bbbk(G)$ via the right regular action ρ_r. But this has been done in Proposition 19(c). For part (2), it suffices to invoke Theorem 22 in conjunction with the following result which is the special case of [Vonessen 1998, Theorem 4.7] for connected G.

Proposition 23. *Let G act on $\Bbbk(G)$ via ρ_r and let F be a G-stable subfield of $\Bbbk(G)$ containing $\Bbbk$. Let $\operatorname{Hom}_G(F, \Bbbk(G))$ denote the collection of all G-equivariant $\Bbbk$-algebra homomorphisms $\varphi \colon F \to \Bbbk(G)$. Then the G-action on $\operatorname{Hom}_G(F, \Bbbk(G))$ that is given by $g.\varphi = \rho_\ell(g) \circ \varphi$ is transitive.*

This completes the proof of Theorem 1. □

3.7.3. It is tempting to try and prove (1) above in the following more direct fashion. Assume that R is G-prime and choose an ideal P of R that is maximal subject to the condition $(P : G) = 0$. This is possible by the proof of Proposition 8(b) and we have also seen that P is prime. I don't know if the ideal P is actually rational. This would follow if the field extension $\mathscr{C}(R)^G \hookrightarrow \mathscr{C}(R/P)^{G_P}$ in Lemma 10 were algebraic in the present situation. Indeed, every ideal I of R with $I \supsetneqq P$ satisfies $(I : G) \neq 0$, and hence $(I : H) \supsetneqq P$. Therefore, Proposition 19(b) tells us that the connected component of the identity of G_P acts trivially on $\mathscr{C}(R/P)$ and so $\mathscr{C}(R/P)$ is finite over $\mathscr{C}(R/P)^{G_P}$.

Acknowledgement

It is a pleasure to thank Rudolf Rentschler for his comments, questions, and guidance to the literature on enveloping algebras. The author also thanks Ken Goodearl, Jens Carsten Jantzen, Peter Linnell, and Lance Small for helpful comments at various stages of this work, and the referee for a careful reading of the article and valuable suggestions.

References

[Amitsur 1972] S. A. Amitsur, "On rings of quotients", pp. 149–164 in *Symposia Mathematica* (Rome, 1970), vol. VIII, Academic Press, London, 1972. MR 48 #11180 Zbl 0263.16003

[Baxter and Martindale 1979] W. E. Baxter and W. S. Martindale, III, “Jordan homomorphisms of semiprime rings”, *J. Algebra* **56**:2 (1979), 457–471. MR 80f:16008 Zbl 0427.16006

[Borel 1991] A. Borel, *Linear algebraic groups*, 2nd ed., Graduate Texts in Mathematics **126**, Springer, New York, 1991. MR 92d:20001 Zbl 0726.20030

[Borho et al. 1973] W. Borho, P. Gabriel, and R. Rentschler, *Primideale in Einhüllenden auflösbarer Lie-Algebren (Beschreibung durch Bahnenräume)*, Lecture Notes in Mathematics **357**, Springer, Berlin, 1973. MR 51 #12965 Zbl 0293.17005

[Bourbaki 1981] N. Bourbaki, *Éléments de mathématique*, Lecture Notes in Mathematics **864**, Masson, Paris, 1981. MR 84d:00002 Zbl 0498.12001

[Brown and Goodearl 2002] K. A. Brown and K. R. Goodearl, *Lectures on algebraic quantum groups*, Advanced Courses in Mathematics. CRM Barcelona, Birkhäuser Verlag, Basel, 2002. MR 2003f:16067 Zbl 1027.17010

[Brown and Lorenz 1996] K. A. Brown and M. Lorenz, “Grothendieck groups of invariant rings: linear actions of finite groups”, *Math. Z.* **221**:1 (1996), 113–137. MR 96m:19005 Zbl 0905.19001

[Chin 1992] W. Chin, “Actions of solvable algebraic groups on noncommutative rings”, pp. 29–38 in *Azumaya algebras, actions, and modules*, edited by D. Haile and J. Osterburg, Contemp. Math. **124**, Amer. Math. Soc., Providence, RI, 1992. MR 93d:16032 Zbl 0759.16012

[Dixmier 1972] J. Dixmier, “Sur les idéaux génériques dans les algèbres enveloppantes”, *Bull. Sci. Math.* (2) **96** (1972), 17–26. MR 47 #1895 Zbl 0235.17008

[Dixmier 1977] J. Dixmier, “Idéaux primitifs dans les algèbres enveloppantes”, *J. Algebra* **48**:1 (1977), 96–112. MR 56 #5673 Zbl 0366.17007

[Dixmier 1996] J. Dixmier, *Enveloping algebras*, Graduate Studies in Mathematics **11**, American Mathematical Society, Providence, RI, 1996. Revised reprint of the 1977 translation. MR 97c:17010 Zbl 0867.17001

[Duflo 1982] M. Duflo, “Théorie de Mackey pour les groupes de Lie algébriques”, *Acta Math.* **149**:3-4 (1982), 153–213. MR 85h:22022 Zbl 0529.22011

[Erickson et al. 1975] T. S. Erickson, W. S. Martindale, 3rd, and J. M. Osborn, “Prime nonassociative algebras”, *Pacific J. Math.* **60**:1 (1975), 49–63. MR 52 #3264 Zbl 0355.17005

[Gabriel 1971] P. Gabriel, *Représentations des algèbres de Lie résolubles (d’après J. Dixmier).*, pp. 1–22, Lecture Notes in Mathematics **179**, Springer, New York, 1971. Zbl 0225.17004

[Irving and Small 1980] R. S. Irving and L. W. Small, “On the characterization of primitive ideals in enveloping algebras”, *Math. Z.* **173**:3 (1980), 217–221. MR 82j:17015 Zbl 0437.17002

[Jantzen 2003] J. C. Jantzen, *Representations of algebraic groups*, 2nd ed., Mathematical Surveys and Monographs **107**, American Mathematical Society, Providence, RI, 2003. MR 2004h:20061 Zbl 1034.20041

[Lambek 1976] J. Lambek, *Lectures on rings and modules*, 2nd ed., Chelsea, New York, 1976. MR 54 #7514 Zbl 0365.16001

[Lang 2002] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics **211**, Springer, New York, 2002. MR 2003e:00003 Zbl 0984.00001

[Lorenz and Passman 1979] M. Lorenz and D. S. Passman, “Centers and prime ideals in group algebras of polycyclic-by-finite groups”, *J. Algebra* **57**:2 (1979), 355–386. MR 80f:20005 Zbl 0415.16008

[Martindale 1969a] W. S. Martindale, III, “Lie isomorphisms of prime rings”, *Trans. Amer. Math. Soc.* **142** (1969), 437–455. MR 40 #4308 Zbl 0192.37802

[Martindale 1969b] W. S. Martindale, III, "Prime rings satisfying a generalized polynomial identity", *J. Algebra* **12** (1969), 576–584. MR 39 #257 Zbl 0175.03102

[Martindale et al. 1990] W. S. Martindale, M. P. Rosen, and J. D. Rosen, "Extended centroids of power series rings", *Glasgow Math. J.* **32**:3 (1990), 371–375. MR 91i:16062 Zbl 0711.16024

[McConnell and Robson 2001] J. C. McConnell and J. C. Robson, *Noncommutative Noetherian rings*, Graduate Studies in Mathematics **30**, American Mathematical Society, Providence, RI, 2001. MR 2001i:16039 Zbl 0980.16019

[Mœglin 1980] C. Mœglin, "Idéaux primitifs des algèbres enveloppantes", *J. Math. Pures Appl.* (9) **59**:3 (1980), 265–336. MR 83i:17008 Zbl 0454.17006

[Mœglin and Rentschler 1981] C. Mœglin and R. Rentschler, "Orbites d'un groupe algébrique dans l'espace des idéaux rationnels d'une algèbre enveloppante", *Bull. Soc. Math. France* **109**:4 (1981), 403–426. MR 83i:17009 Zbl 0495.17006

[Mœglin and Rentschler 1984] C. Mœglin and R. Rentschler, "Sur la classification des idéaux primitifs des algèbres enveloppantes", *Bull. Soc. Math. France* **112**:1 (1984), 3–40. MR 86e:17006 Zbl 0549.17007

[Mœglin and Rentschler 1986a] C. Mœglin and R. Rentschler, "Idéaux G-rationnels, rang de Goldie", 1986. Preprint.

[Mœglin and Rentschler 1986b] C. Mœglin and R. Rentschler, "Sous-corps commutatifs ad-stables des anneaux de fractions des quotients des algèbres enveloppantes; espaces homogènes et induction de Mackey", *J. Funct. Anal.* **69**:3 (1986), 307–396. MR 88h:17011 Zbl 0618.17007

[Montgomery 1980] S. Montgomery, *Fixed rings of finite automorphism groups of associative rings*, Lecture Notes in Mathematics **818**, Springer, Berlin, 1980. MR 81j:16041 Zbl 0449.16001

[Montgomery 1993] S. Montgomery, *Hopf algebras and their actions on rings*, CBMS Regional Conference Series in Mathematics **82**, 1993. MR 94i:16019 Zbl 0793.16029

[Nouazé and Gabriel 1967] Y. Nouazé and P. Gabriel, "Idéaux premiers de l'algèbre enveloppante d'une algèbre de Lie nilpotente", *J. Algebra* **6** (1967), 77–99. MR 34 #5889 Zbl 0159.04101

[Passman 1989] D. S. Passman, *Infinite crossed products*, Pure and Applied Mathematics **135**, Academic Press, Boston, 1989. MR 90g:16002 Zbl 0662.16001

[Passman 1991] D. S. Passman, *A course in ring theory*, The Wadsworth & Brooks/Cole Mathematics Series, Wadsworth & Brooks/Cole Advanced Books & Software, Pacific Grove, CA, 1991. MR 91m:16001 Zbl 0783.16001

[Procesi 1973] C. Procesi, *Rings with polynomial identities*, Pure and Applied Mathematics **17**, Marcel Dekker, New York, 1973. MR 51 #3214 Zbl 0262.16018

[Rentschler 1974] R. Rentschler, "L'injectivité de l'application de Dixmier pour les algèbres de Lie résolubles", *Invent. Math.* **23** (1974), 49–71. MR 49 #10748 Zbl 0299.17003

[Rentschler 1979] R. Rentschler, "Orbites dans le spectre primitif de l'algèbre enveloppante d'une algèbre de Lie", pp. 88–98 in *Séminaire d'Algèbre Paul Dubreil 31ème année*, edited by M.-P. Malliavin, Lecture Notes in Math. **740**, Springer, Berlin, 1979. MR 82b:17012 Zbl 0429.17008

[Rentschler 1987] R. Rentschler, "Primitive ideals in enveloping algebras (general case)", pp. 37–57 in *Noetherian rings and their applications* (Oberwolfach, 1983), edited by L. W. Small, Math. Surveys Monogr. **24**, Amer. Math. Soc., Providence, RI, 1987. MR 89d:17014 Zbl 0651.17005

[Vonessen 1993] N. Vonessen, "Actions of linearly reductive groups on PI-algebras", *Trans. Amer. Math. Soc.* **335**:1 (1993), 425–442. MR 93c:16034 Zbl 0789.16025

[Vonessen 1996] N. Vonessen, "Actions of algebraic groups on the spectrum of rational ideals", *J. Algebra* **182**:2 (1996), 383–400. MR 97c:16044 Zbl 0867.16020

[Vonessen 1998] N. Vonessen, "Actions of algebraic groups on the spectrum of rational ideals, II", *J. Algebra* **208**:1 (1998), 216–261. MR 99k:16073 Zbl 0914.16013

[Waterhouse 1979] W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics **66**, Springer, New York, 1979. MR 82e:14003 Zbl 0442.14017

Communicated by J. Toby Stafford
Received 2008-01-24 Accepted 2008-04-28

lorenz@temple.edu
Department of Mathematics, Temple University,
Philadelphia, PA 19122-6094, United States
http://www.math.temple.edu/~lorenz/

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in ANT are usually in English, but articles written in other languages are welcome.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@mathscipub.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 2 No. 4 2008

1937-0652(2008)2:4;1-C